Development of Scalable Coding of Encrypted Images Using Modified Absolute Moment Block Truncation Code

Pankiraj Jeya Bright (jeyabright@gmail.com)
Kalasalingam Academy of Research and Education https://orcid.org/0000-0002-9246-5301
Vishnuvarthanan Govindaraj
Kalasalingam University: Kalasalingam Academy of Research and Education
Yu-Dong Zhang
University of Leicester
Pallikonda Rajasekaran
Kalasalingam University: Kalasalingam Academy of Research and Education
Anisha Milton
Kalasalingam University: Kalasalingam Academy of Research and Education
Arunprasath Thiagarajan
Kalasalingam University: Kalasalingam Academy of Research and Education

Research

Keywords: Scalable Coding on Encrypted Image, Image Decryption, Image Reconstruction, Secured Signal Processing, Modified Absolute Moment Block Truncation Code, Image Encryption

Posted Date: January 3rd, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1205275/v1

Development of Scalable Coding of Encrypted Images Using Modified Absolute Moment Block Truncation Code

Jeya Bright Pankiraj[1*], Vishnuvarthanan Govindaraj[2], Yudong Zhang[3], Pallikonda Rajasekaran Murugan[4], Anisha Milton[5], Arunprasath Thiagarajan[6]
[1,4]Department of ECE, Kalasalingam Academy of Research and Education, Srivilliputhur,India
[2,5,6]Department of BME, Kalasalingam Academy of Research and Education, Srivilliputhur, India
[3]F26, Informatics Building, School of Informatics, University of Leicester, University Road, Leicester, UK
[*]Correspondence: jeyabright@gmail.com

Abstract—Many researchers worked on scalable coding for unencrypted images, and there is more space for research in scalable coding for encrypted images. This paper proposes a novel method of scalable coding for encrypted images, especially for lossy compression images using the Modified Absolute Moment Block Truncation Code (MAMBTC) technique. The given input image is compressed using MAMBTC and then encrypted using a Pseudo-Random Number (PRNG) at the encryption phase. The PRNG is shared between the encoder and the decoder. At the decryption phase, the compressed pixel value is obtained by decryption using the PRNG and then reconstructed using MAMBTC, scaled by scaling factor 2 and Bilinear Interpolation Technique to obtain the original image. MAMBTC gives better image quality than Block Truncation Code (BTC), a higher PSNR of 36.32 dB, and a Compression ratio of 1.09, which makes the proposed system ready for the signal processing community/applications.

Keywords— Scalable Coding on Encrypted Image, Image Decryption, Image Reconstruction, Secured Signal Processing, Modified Absolute Moment Block Truncation Code, Image Encryption

1. Introduction

In today's technology, scalability is essentially required for transmission and reception of data, especially in the signal processing community, and therefore it is an essential area of

research. The Secured Signal Processing (SSP) for encrypted signals is performed on [1], and Discrete Fourier Transform is implemented on [2] by using homomorphic properties. In [3], the privacy problem is studied for adaptive filtering, and the same was analyzed for the reduction of expansion factor in [4] for SSP in the encrypted domain. In [5], the digital watermarking technique is proposed, and the enciphering rate is low, which is overcome by using the fingerprinting technique in [6].

Nowadays, the usage of image data is larger, which has increased storage space and bandwidth. It makes the transmission process costlier. Therefore, reducing storage space, bandwidth and transmission costs are essential for the SSP on the encrypted domain. The signals are first compressed and then encrypted, which is the traditional way of transmitting data, but it is reversed in [7],[8],[9],[10] and [11].

Scalability is mostly preferred for many applications. Rate Scalability occurs when the bit-stream is extracted at the desired rate from the decoder for lossy image, and higher bit rates can be decoded until a perfect image is reconstructed. Resolution Scalability can be improvised when a lower resolution of the lossy image is extracted from the decoder, and higher resolution is achieved until the original image is reconstructed without loss. In [12] and [13], scalable coding is carried out on unencrypted signals. The first work to report on scalable coding for encrypted images is [14], where Hadamard transform is used for image compression, the pseudo-random number is used for image encryption and image decryption, and scaling is done by scaling factor 2. Later, bilinear interpolation technique is used for image reconstruction.

In this paper, the authors propose a novel method of scalable coding on encrypted images using Modified Absolute Moment Block Truncation Code (MAMBTC) Technique. In [15], the BTC technique was introduced in 1979. BTC works with two-level quantizers in which the mean is used as a threshold value, and the original content is reconstructed using the

mean and variance value. In [16], the Absolute Moment Block Truncation Code (AMBTC) technique was introduced in the year 1984, and AMBTC works with two-level quantizers in which the mean is used as a threshold value. The original image is reconstructed using high range and low range values. AMBTC technique is very attractive to many applications, such as internet video with software-only codecs, digital cameras and printers that require only moderate data rates. The advantage of the AMBTC technique was, the demand for storage space is decreased and also it lends itself very nicely to parallel processing. In [17], scalable coding is carried out by BTC for encrypted images. The principal content is compressed by BTC, encrypted by PRNG and transmitted. It is further decrypted at the decoder, and the principal content is reconstructed by applying techniques, such as BTC, scaled by scaling factor 2 and Bilinear Interpolation Technique. In this paper, the principal content is compressed by MAMBTC and then encrypted using the PRNG, and finally, it is transmitted. The PRNG is shared between encoder and decoder. The transmitted value is decrypted by PRNG on the decoder, and the original image is reconstructed using the MAMBTC, scaled by scaling factor 2 and Bilinear Interpolation technique. The MAMBTC gives higher Peak Signal to Noise Ratio (PSNR), better Compression Ratio (CR), and reduced Mean Squared Error (MSE), Bit Rate (BR) than the existing techniques.

2. Related Works

2.1.1 Scalable Coding of Encrypted Images using Hadamard Transform

In [14], the raw image is encrypted by adding a pseudo-random number generated value (PRNG), where the PRNG acts as a secret key. Then the encrypted image is divided into rough content and detailed content. The rough content is rounded and quantized while detailed content is taken Hadamard transform, and both encoded bits are transmitted by the encoder as bit-streams. The bit-stream and secret key are shared with the decoder. At the decoder, rough

content is decrypted by subtracting it with the secret key, and the obtained value is kept separately. The rough content value is taken bilinear transform to the original image size, and after rounding and quantization, Hadamard transform is applied and resized to the detailed content matrix size. Finally, the input image size is reconstructed by combining rough and detailed content. However, the reconstructed image quality is with lower PSNR, lower CR, and increased BR.

2.1.2 Scalable Coding using BTC

In [17], the authors have introduced the scalable coding of encrypted images using BTC. In this, the principal content is compressed by BTC. It is then encrypted by PRNG, and the same will be shared between encoder and decoder. The encoded bit-stream is transmitted. In the decoding process, they first decrypt the transmitted image, and they reconstruct the principal content by using techniques, such as BTC, scaling factor as 2, and bilinear interpolation technique. This technique gives lower PSNR, lower CR, and higher MSE, and a higher BR. We can achieve improved PSNR and CR values, and reduced MSE and BR by using the developed MAMBTC technique.

3. Proposed Method

Fig.1 shows the proposed system. MAMBTC technique is used to compress the input gray level pixel value. Then pseudo-random numbers (PRNG) are generated and added with compressed pixel values to get the encrypted output. The PRNG is shared between encoder and decoder. The transmitted bit stream is decrypted at the receiver side using the PRNG. Then the principal content is reconstructed by MAMBTC and scaling technique. The reconstructed content has better image quality, higher resolution, higher CR, lesser MSE, reduced BR, and higher PSNR than the conventional BTC.

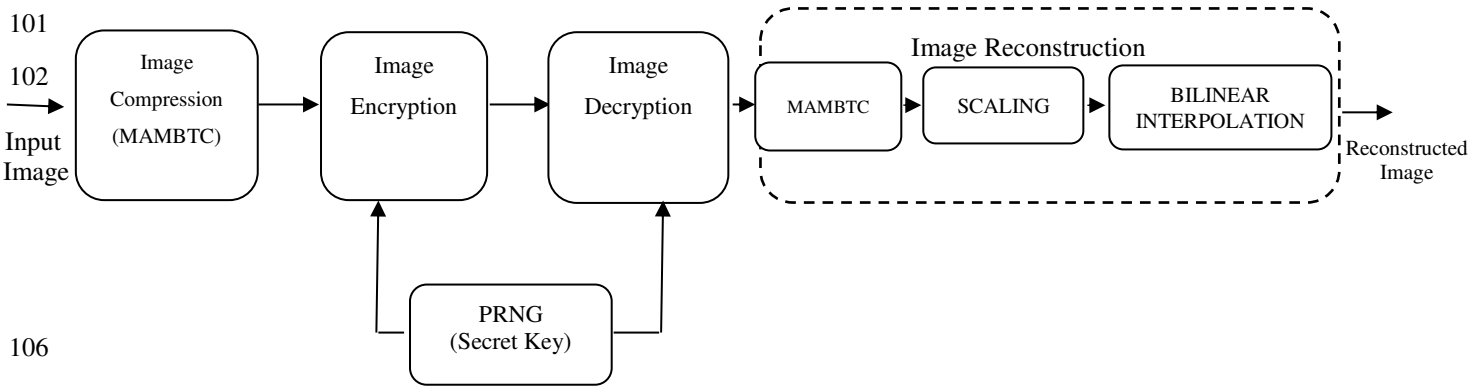


Fig.1 Proposed System

3.1 Image Encoding Process

3.1.1 Image Compression

The first novelty introduced is the threshold value (T_{th}). The uncompressed input image is gray in color. The input pixel values are within [0, 255], and it will be in the form of a B1*B2 matrix, where B1 is the row size, and B2 is the column size. The MAMBTC technique is applied to the input image to get a compressed pixel value. It is then encrypted by adding the compressed pixel value with the PRNG. The proposed MAMBTC algorithm steps are as follow,

Step1: - The uncompressed input gray level image of size 512*512 is divided into non-overlapping blocks having size B1*B2, where B1 and B2 values are taken as 4.

Step 2: - Each block is quantized to obtain the mean value. The mean ($\bar{x}$) is calculated using equation (1), and these values are different for each block.

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

Step 3: - The higher range and lower range values of each non-overlapping block are calculated, which are termed as quantizers of MAMBTC. The higher range (x_{HV}) value is calculated by taking the gray level value, which is greater than or equal to the mean value ($\bar{x}$) of the block as given in equation (2), where K represents the pixels whose gray level value is greater or equal than mean value ($\bar{x}$). The lower range (X_L) value is calculated by taking the gray level value whose values are lesser than the mean value ($\bar{x}$) of the block as given by equation (3), which is expressed in scalar form.

$$x_{HV} = \frac{1}{K}\sum_{x_i \geq \bar{x}}^{n} x_i \tag{2}$$

$$x_{LV} = \frac{1}{16-K}\sum_{x_i<\bar{x}}^{n} x_i \tag{3}$$

Step 4:- The threshold value (T_{th}) is calculated by adding mean ($\bar{x}$)**,** higher range (x_{HV}) value and lower range (x_{LV}) value and then divided by 3 for each non-overlapping block. It is given in equation (4) as:

$$T_{th} = \frac{\bar{x} + x_{HV} + x_{LV}}{3} \tag{4}$$

Step 5:- The binary block ($c(i,j)$) is constructed by comparing each gray level value with the threshold value (T_{th}). The gray level values in the block having greater or equal than the threshold value is replaced by value "1" in the binary block, and those gray level having less than the threshold value is replaced by value "0" in the binary block. It is given by equation (5) as:

$$c(i,j) = \begin{cases} 1 & x_i \geq T_{th} \\ 0 & x_i < T_{th} \end{cases} \tag{5}$$

This process reduces each block to a bit plane. Each non-overlapping block has a higher range value and lower range value meant to be shared to the receiver side, and they will be the same as higher range and lower range values for that block during reconstruction. Thus, the input image is compressed using MAMBTC.

3.1.2 Image Encryption

The second novelty is introduced in this by encrypting the MAMBTC compressed image. The bit amount for the compressed image is 8N. The pseudo-random number (PRNG) of values between 0 and 255 for the size B1*B2 are produced by the pseudo-random number generator, and the pseudo-random bit sequence length is 8N. Let $pr(i,j)$ be the PRNG value. The PRNG is shared with the decoder too. The encrypted pixel value is obtained by adding a compressed pixel value of size B1*B2 with the PRNG of size B1*B2, and then masked by modulo 256. It is given as:

$$en(i,j) = mod\left[\left(c(i,j) + pr(i,j)\right), 256\right] \quad (6)$$

$$1 \leq i \leq B_1,\ 1 \leq j \leq B_2$$

Where, $c(i,j)$ is the compressed image value, $pr(i,j)$ is the secret key, and $en(i,j)$ is the encrypted pixel value. The original image is shown in Fig. 2, and its encrypted image is shown in Fig.3. The image encryption algorithm used is semantically secure against any Probability Polynomial Time (PPT) adversary. The block is sent along with the secret key (PRNG) and also with values of higher range (X_{HV}) and lower range (X_{LV}).

Fig. 2 Original Image

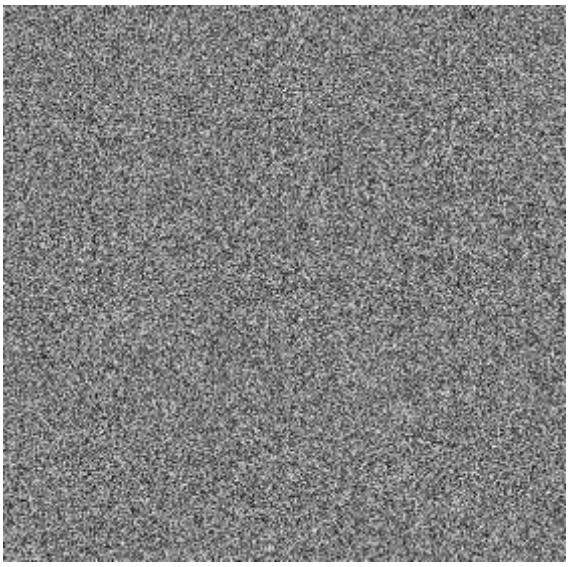


Fig. 3 Encrypted Image

3.2 Image Decoding Process

3.2.1 Image Decryption

The secret key (PRNG) is received at the receiver. The decrypted image is obtained by subtracting the transmitted encoded image with a secret key masked with the modulo-256 operation. The formula used is:

$$de(i,j) = mod[(en(i,j) - pr(i,j)),256] \quad (7)$$

Where $en(i,j)$ represents the transmitted encrypted image, $pr(i,j)$ represents the PRNG, and $de(i,j)$ represents the compressed bit plane transmitted. The $de(i,j)$ contains two quantized values, namely "0" and "1". The decrypted image is shown in Fig. 4.

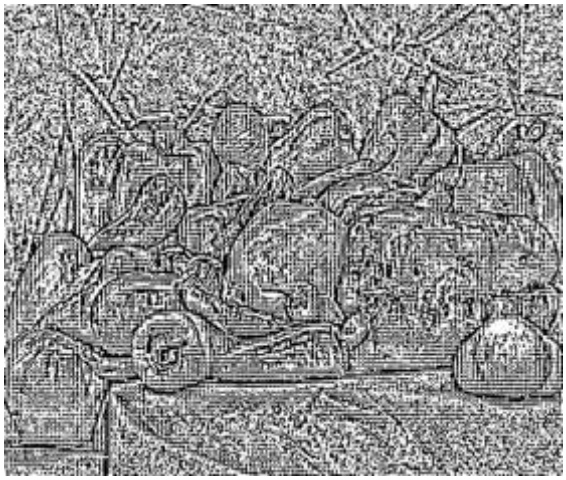


Fig. 4 Decrypted Image

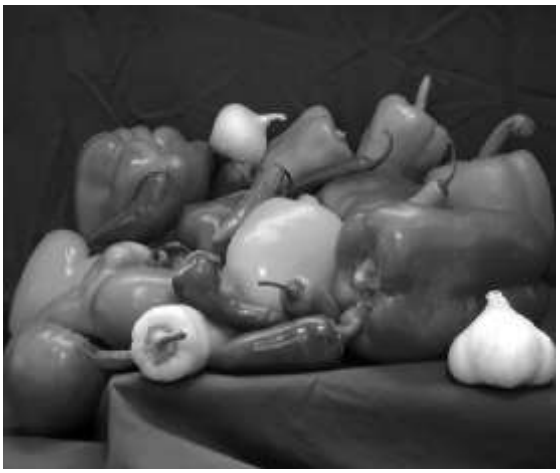


Fig. 5 Reconstructed Image

3.2.2 Image Reconstruction

The third novelty introduced in this paper is by having to scale on the MAMBTC reconstructed image first, and then the original content is reconstructed by using the popular scaling technique, namely Bilinear Interpolation Technique. The image reconstruction process is in three stages. Firstly, by using the MAMBTC technique, the receiver side receives the high range value and low range value transmitted by the encoder. The original content is reconstructed by replacing the quantized value "1" in the decrypted compress bit plane by higher range (X_{HV}) value and "0" by lower range (X_{LV}) value. It is given as:

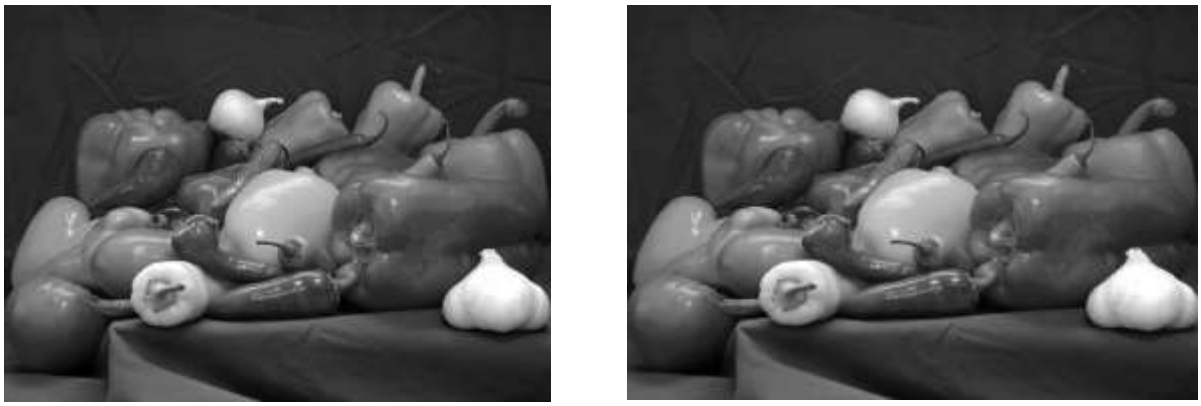
$$re(i,j) = \begin{cases} X_{HV}\,, & de(i,j) = 1 \\ X_{LV}\,, & de(i,j) = 0 \end{cases} \tag{8}$$

Accordingly, $re(i,j)$ gives the reconstructed image using MAMBTC. Secondly, it is scaled by scaling factor 2, and finally, the original image size is reconstructed using Bilinear Interpolation Technique. The reconstructed image is shown in Fig. 5.

4. Experimental Results and Discussion

4.1 Reconstructed Image

The comparison between the original and reconstructed images is shown in Fig.6. The reconstructed image obtained has higher quality, and it reflects equivalent to the original image. The comparison between the reconstructed images using MAMBTC, BTC and Hadamard transform techniques is shown in Fig.7. It clearly shows that the quality of the reconstructed image using MAMBTC is much better than BTC and Hadamard transform in terms of PSNR, wPSNR, MSE, wMSE and compression ratio.



(a) (b)

Fig. 6 Comparison between the original image and the reconstructed image (a). Original Image (b). Reconstructed Image

(a) (b) (c)

Fig. 7 Comparison between reconstructed images using MAMBTC, BTC and Hadamard Transform techniques (a) Hadamard (b) BTC (c) MAMBTC

4.2 Compression Ratio (CR)

The CR is used to determine the compression algorithm performance [17]. Here, the CR ratio is used to evaluate the MAMBTC compression algorithm. It is the ratio of the uncompressed image (or) original image file size to the compressed image file size.

The compression ratio can be computed by using the formula as:

$$Compression\ Ratio = \frac{file\ size\ of\ the\ uncompressed\ image}{file\ size\ of\ compressed\ image} \quad (9)$$

The comparison values of compression ratio among MAMBTC, BTC, and Hadamard transform techniques are shown in Fig.8 for various input images.

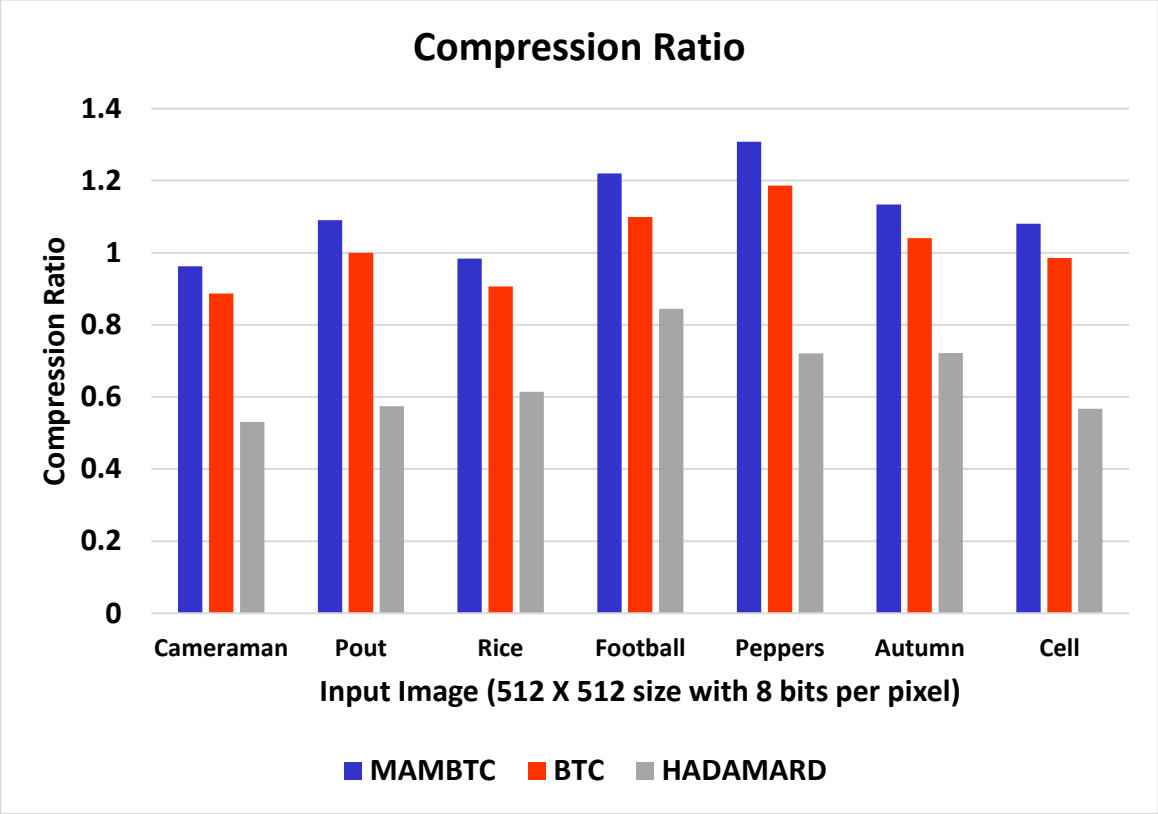


Fig. 8 Comparison of Compression ratio between MAMBTC, BTC, and Hadamard transform techniques for different Images

4.3 Bit Rate (BR)

Bit rate [17] is also used to determine the compression algorithm performance. The lower bit rate represents better compression algorithm performance.

The bit rate can be computed by using the formula as:

$$bit\ rate = \frac{b}{compression\ ratio} \quad (10)$$

Where b is the number of bits per pixel of the uncompressed image. The comparison values of bit rates among MAMBTC, BTC and Hadamard transform techniques are shown in Fig.9 for various input images.

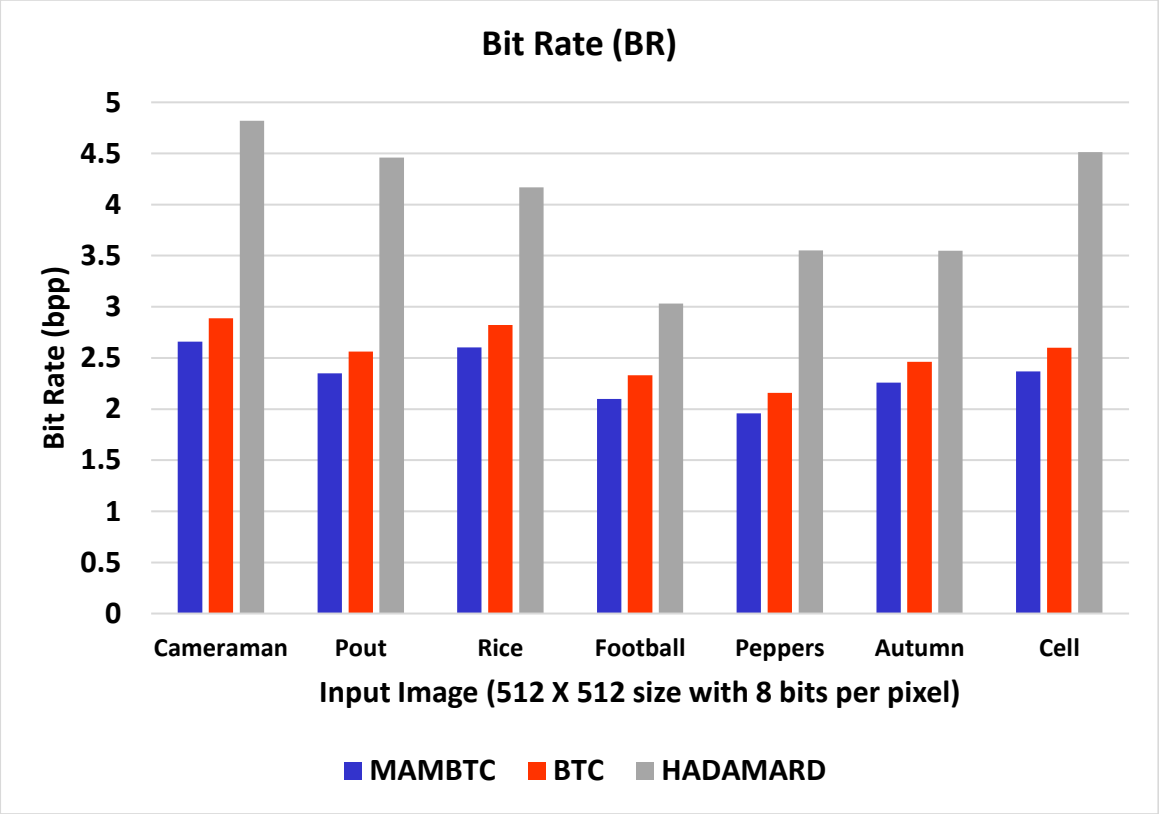


Fig. 9 Comparison of Bit Rates between MAMBTC, BTC, and Hadamard transform techniques for different Images

4.4 Mean Squared Error (MSE)

The MSE is used to determine the loss of energy value in lossy compression of the original value [17]. It is measured by differences in individual pixel's gray values. If the mean squared error is small, it means that the reconstructed image will be equivalent to the original image.

Mean Squared Error (MSE) can be computed by using the formula as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[out(i,j) - inp(i,j)]^2 \quad (11)$$

Where $out(i,j)$ is the compressed image, $inp(i,j)$ is the original image, m and n are the sizes of rows and columns in the compressed image and original image, respectively.

The comparison values of Mean Squared Error (MSE) among MAMBTC, BTC, and Hadamard transform techniques are shown in Fig.10 for various input images.

T

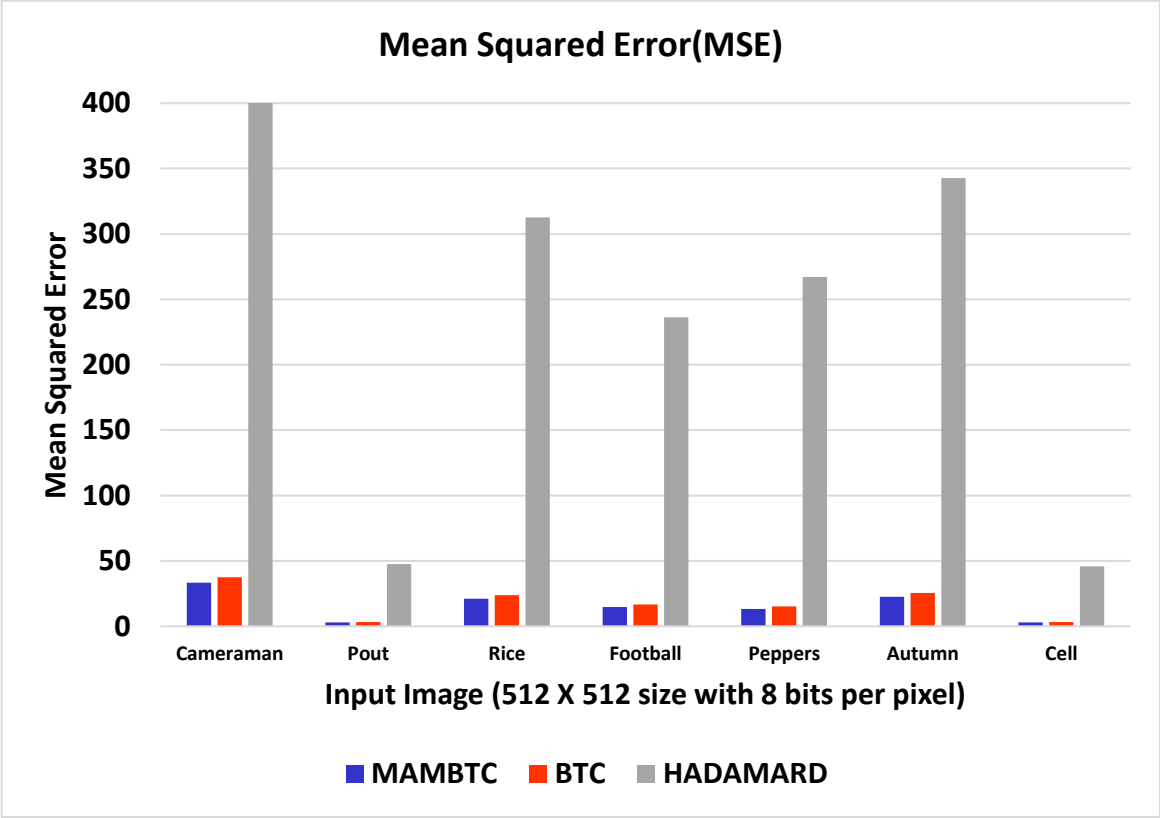


Fig. 10 Comparison of MSE between MAMBTC, BTC, and Hadamard transform techniques for different Images

4.5 Weighted Mean Squared Error (wMSE)

wMSE determines the distortion level in the image. wMSE is based on a correlation between neighboring pixels since it has different effects on the human visual system when pixels are at different positions in an image [17].

Weighted Mean Squared Error (wMSE) can be computed by using the formula as:

$$wMSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(2\left|\frac{out(i,j)-inp(i,j)}{out(i,j)+inp(i,j)}\right|\right)^2 \quad (12)$$

Where, $out(i,j)$ is the compressed image, $inp(i,j)$ is the original image, m and n are the sizes of rows and columns in the compressed image and original image, respectively.

The comparison values of wMSE among MAMBTC, BTC, and Hadamard transform techniques are shown in Fig.11 for various input images.

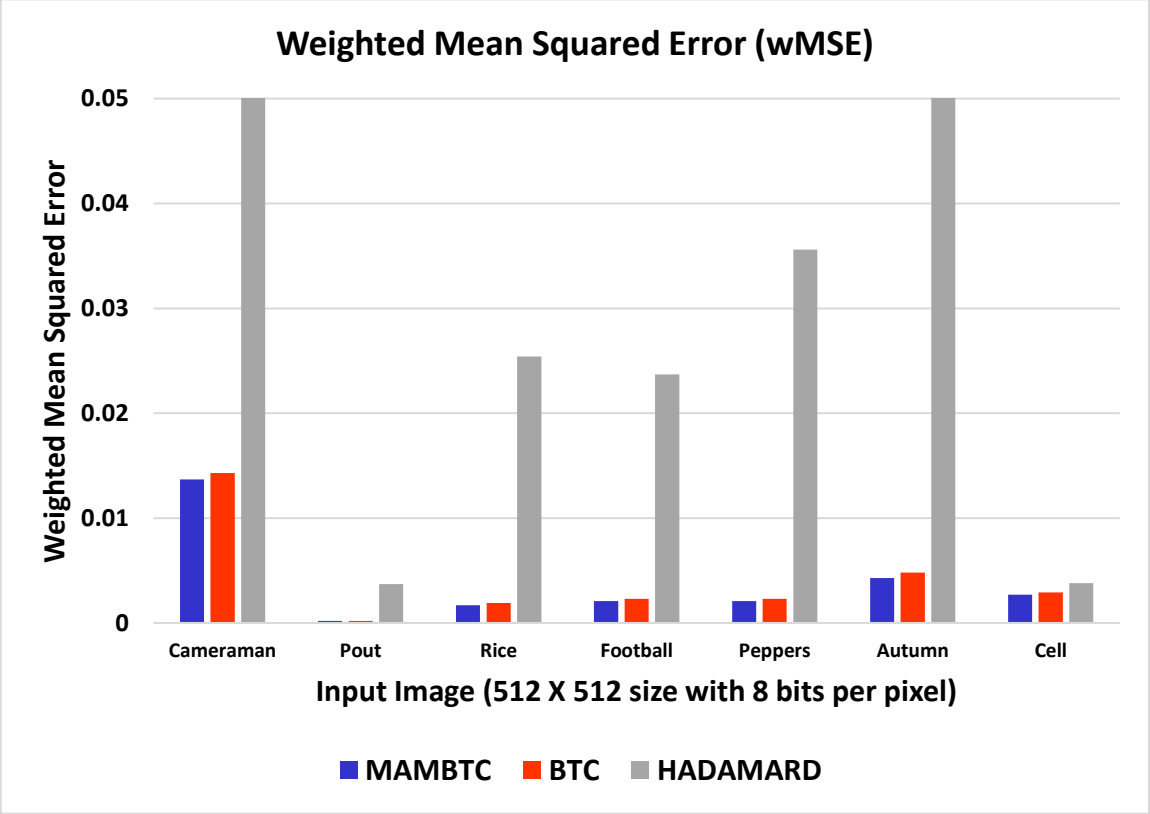


Fig. 11 Comparison of wMSE between MAMBTC, BTC, and Hadamard transform techniques for different Images

4.6 Peak Signal to Noise Ratio (PSNR)

The PSNR is a metric used for qualitative measurement of reconstructed image for lossy compression [22], [23]. The reconstructed image quality will be better if a higher PSNR value is obtained.

PSNR can be computed by using the formula as:

$$PSNR = 10\, log_{10} \frac{255^2}{MSE} \quad (13)$$

Where MSE is the mean squared error.

The comparison values of PSNR among MAMBTC, BTC and Hadamard transform techniques are shown in Fig.12 for various input images.

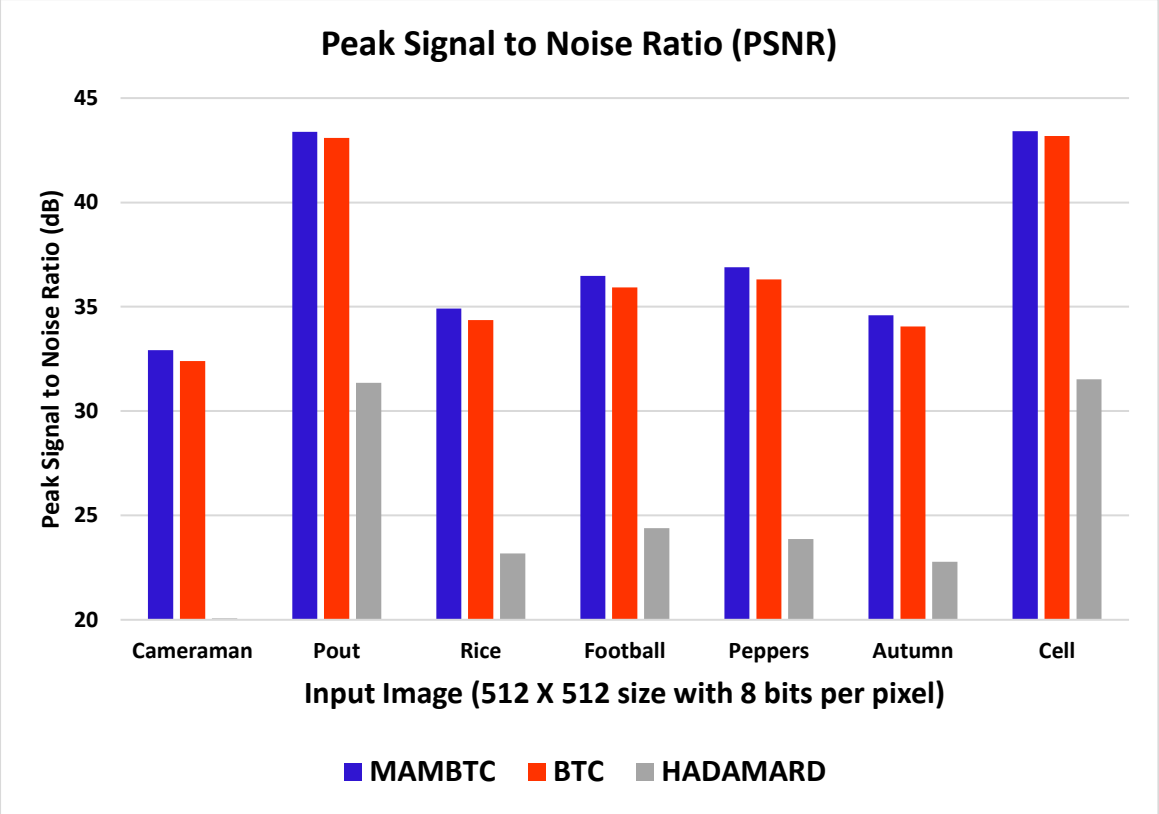


Fig. 12 Comparison of PSNR between MAMBTC, BTC and Hadamard transform techniques for different Images

4.7 Weighted Peak Signal to Noise Ratio (wPSNR)

The wPSNR [17] is an extension of PSNR. The measurement of wPSNR is based on neighboring pixels and the human visual system. The wPSNR gives the image quality and is calculated between original and compressed content.

wPSNR can be computed by using the formula:

$$wPSNR = 10\ \log_{10}\left(\frac{255^2}{wMSE}\right) \quad (14)$$

Where wMSE is a weighted mean squared error.

The comparison values of wPSNR between MAMBTC, BTC and Hadamard transform techniques are shown in Fig.13 for various input images.

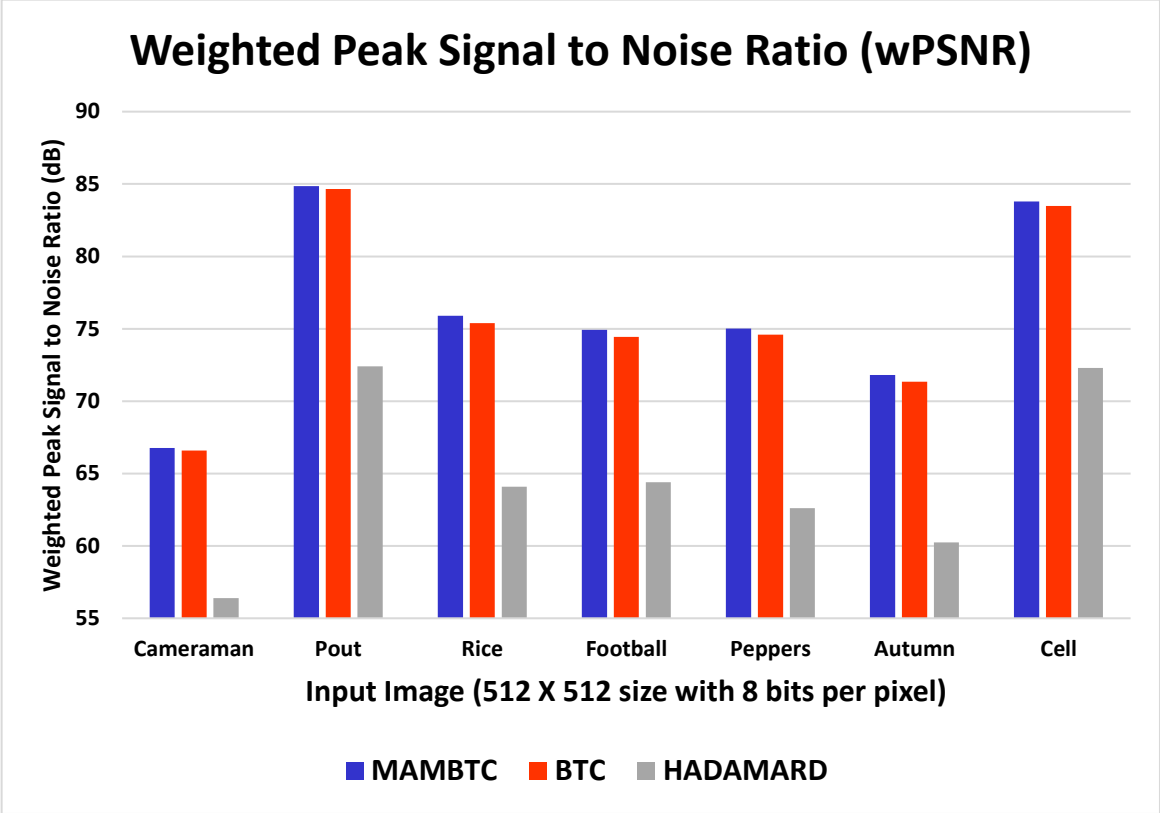


Fig. 13 Comparison of wPSNR between MAMBTC, BTC and Hadamard transform techniques for different Images

4.8 Computational Time

The comparison values of computational time [24] among MAMBTC, BTC and Hadamard transform techniques are shown in Fig.14 for various input images. Even though MAMBTC has higher computational complexity than BTC, but the compression ratio of MAMBTC is better than BTC.

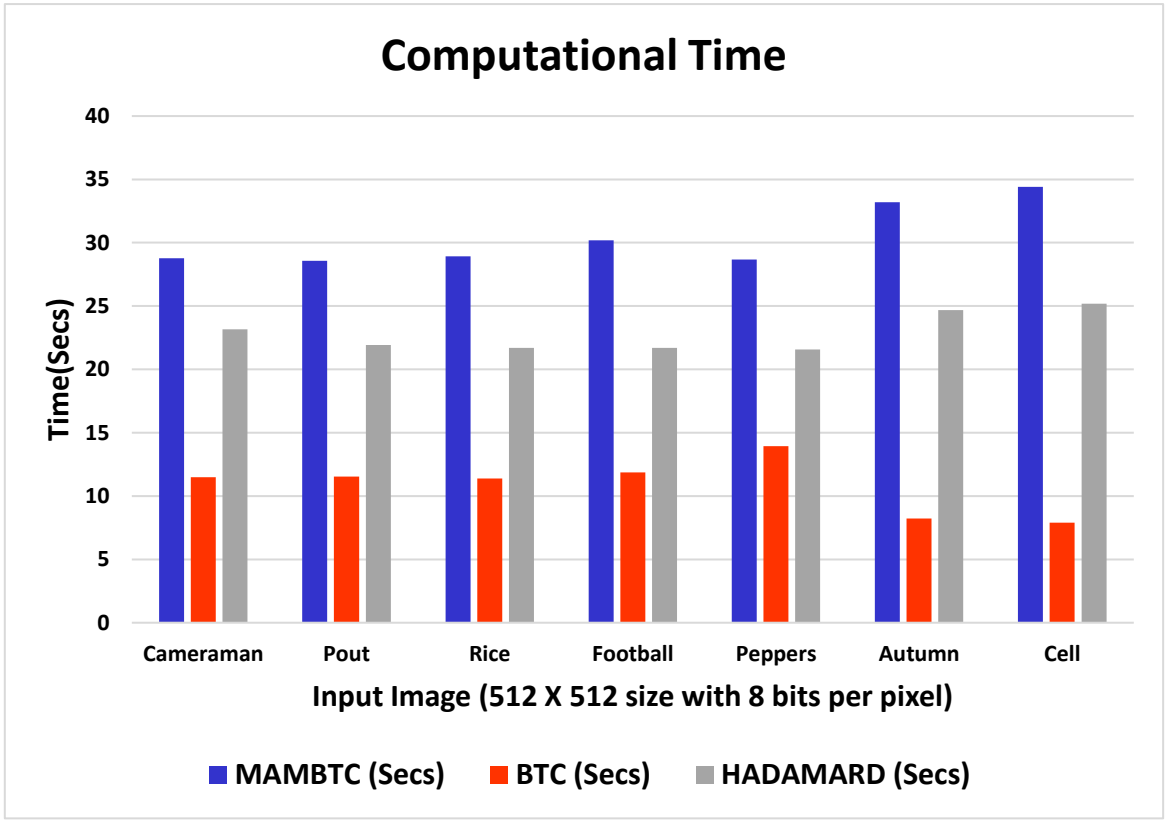


Fig. 14 Comparison of Computation Time between MAMBTC, BTC and Hadamard transform techniques for different Images

4.9 Memory Size

The comparison values of memory size [24] among MAMBTC, BTC and Hadamard transform techniques are shown in Fig.15 for various input images. Fig. 15 infers that the MAMBTC requires lesser memory than the BTC and Hadamard techniques for compressing the different standard input images.

Table 1 lists the performance evaluation of proposed system values such as Compression Ratio, Bit Rate, MSE, wMSE, PSNR, wPSNR, Computational Time and Memory Size.

Table 1 Performance Evaluation of Proposed System

Input Image	Compression Ratio	Bit Rate	MSE	wMSE	PSNR (dB)	wPSNR (dB)	Computational Time (Secs)	Memory Size (MB)
Cameraman	**0.9623**	**2.6603**	**33.2453**	**0.0137**	**32.9135**	**66.7728**	**28.772**	**1371**
Pout	**1.0901**	**2.3483**	**2.9861**	**0.0002**	**43.3797**	**84.8556**	**28.5758**	**1380**
Rice	**0.9839**	**2.6019**	**20.9969**	**0.0017**	**34.9093**	**75.898**	**28.9336**	**1367**
Football	**1.2201**	**2.0981**	**14.624**	**0.0021**	**36.4801**	**74.9267**	**30.199**	**1364**
Peppers	**1.3077**	**1.9576**	**13.2815**	**0.0021**	**36.8983**	**75.0046**	**28.6825**	**1363**
Autumn	**1.1342**	**2.2571**	**22.5541**	**0.0043**	**34.6005**	**71.8069**	**33.1961**	**1280**
Cell	**1.0808**	**2.3686**	**2.9595**	**0.0027**	**43.4187**	**83.7846**	**34.4036**	**1278**

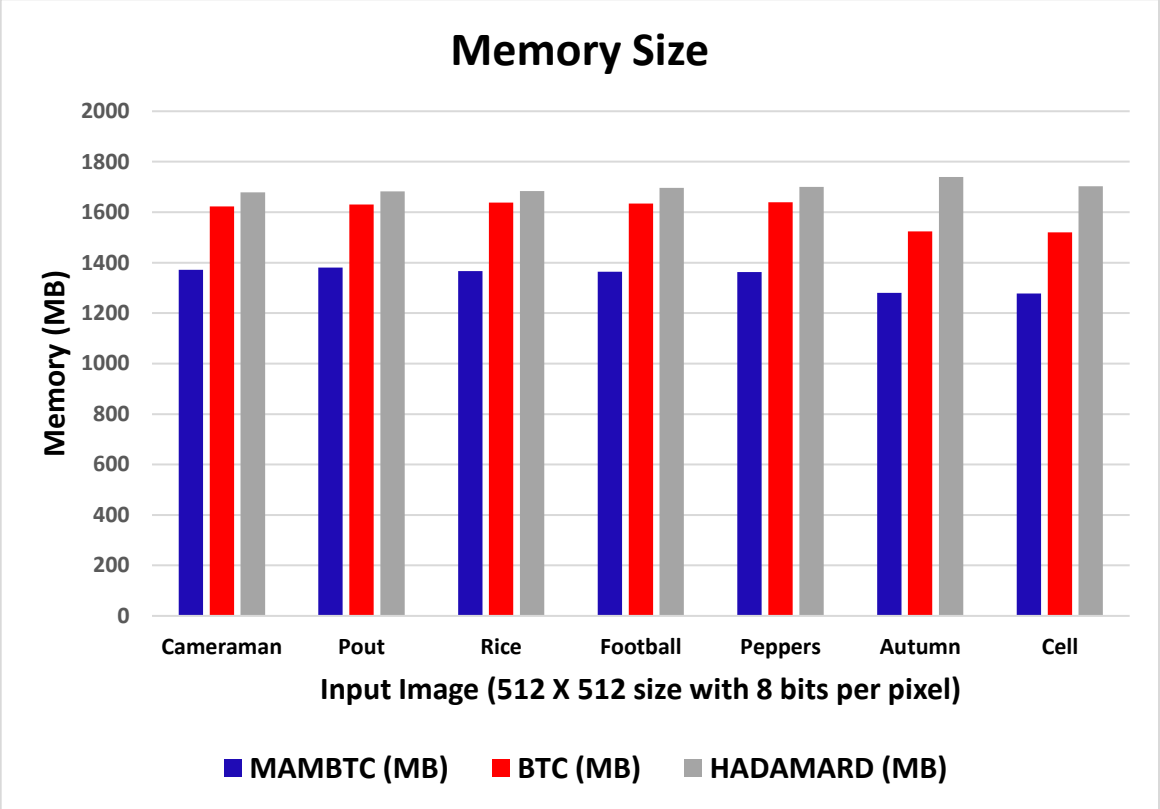


Fig. 15 Comparison of Memory Size between MAMBTC, BTC and Hadamard transform techniques for different Images

Figure 16 compares the various state of the art techniques with the present proposed system by comparing the PSNR values with Pepper image. The resultant graph shows that the proposed system of this study is much better than the various state of the art techniques.

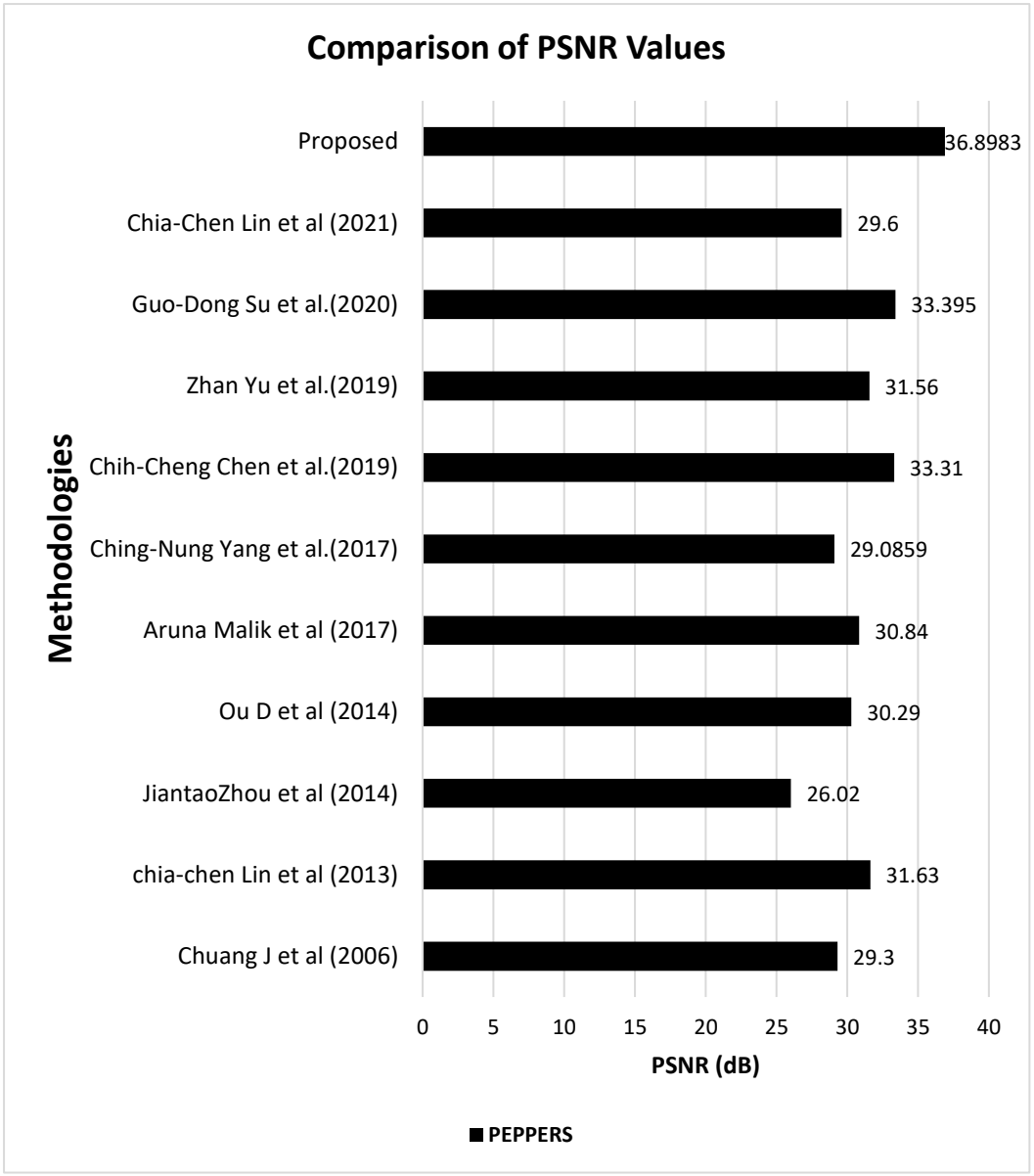


Fig. 16 Comparison between various state of art techniques with the proposed system

5. Conclusion

In this paper, the researchers have presented a novel scheme of scalable coding of encryption of images using the MAMBTC. The original input image is compressed by using the MAMBTC. Then using PRNG, it is encrypted, and the encoded bit-stream is transmitted. The original image is reconstructed by the MAMBTC, which is further scaled by scaling factor 2 and bilinear interpolation technique at the decoder. It requires low storage, and coding and decoding techniques of MAMBTC are simpler. The requirement for computational complexity is higher for MAMBTC since it needs both the high range and low range values of each non-

overlapping block, but the compression ratio is higher than BTC, and the requirement for storage space is decreased when compared to BTC. The experiment results show that it has improved performance than BTC with increased PSNR, increased compression ratio, increased wPSNR, decreased MSE, decreased wMSE, and decreased bit rate. As a result, the proposed method is very robust and effective for Signal Processing Community to transmit signals on encrypted domains than the existing techniques available.

List of abbreviations

Table 2 shows the various abbreviations used in this paper

Table 2 Utilized parameter and their functionality

S.No	Parameters	Working outcomes of the parameters
1	X_{HV}	Higher range value of the non-overlapping block
2	X_{LV}	Lower range value of the non-overlapping block
3	$\bar{x}$	Mean value of the non-overlapping block
4	$c(i,j)$	Binary Block of the non-overlapping block of an encoder
5	$pr(i,j)$	The pseudo-random generated value
6	$en(i,j)$	Encrypted Pixel Value
7	$de(i,j)$	Decrypted Pixel Value
8	$re(i,j)$	Reconstructed Pixel Value
9	MSE	Mean Squared Error Value
10	wMSE	Weighted Mean Squared Error Value
11	PSNR	Peak Signal to Noise Ratio
12	wPSNR	Weighted Peak Signal to Noise Ratio
13	CR	Compression Ratio
14	BR	Bit Rate
15	PRNG	Pseudo-random number generated value
16	SSP	Secured Signal Processing

Declarations

Availability of data and materials

The conclusion and comparison data of this article are included within the article

Competing Interests

The authors declare that they have no competing interests

Funding

Not Applicable

Author's Contributions

JBP proposed the framework of this work and carried out the whole experiments and drafted the manuscript. VG greatly helped in articulating the manuscript. YZ helped in finalizing the manuscript. MPR, AM and AT have helped in technical writing. All authors read and approved the final manuscript.

Acknowledgements

Not Applicable

References

1. Z.Erkin et al.,Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing. EURASIP Journal on Information Security. **2007**, 1-20 (2007). doi:10.1155/2007/78943.

2. T.Bianchi et al., On the implementation of the discrete Fourier transform in the encrypted domain. IEEE Transformation on Information Forensics and Security. **4**(1), 86–97 (2009). doi:10.1109/tifs.2008.2011087.

3. J.R.Troncoso Pastoriza, F.Pérez-González, Secure adaptive filtering. IEEE Transformation on Information Forensics and Security. **6**(2),469–485(2011). doi:10.1109/tifs.2011.2109385.

4. T.Bianchi et al., Composite signal representation for fast and storage-efficient processing of encrypted signals. IEEE Transformation on Information Forensics and Security. **5**(1),180–187 (2010). doi:10.1109/tifs.2009.2036230.

5 N.Memon, P.W.Wong, A buyer-seller watermarking protocol. IEEE Transactions on Image Processing. **10**(4), 643–649 (2001). doi:10.1109/83.913598.

362 6. M.Kuribayashi, H.Tanaka, Fingerprinting protocol for images based on an additive
363 homomorphic property. IEEE Transactions on Image Processing. **14**(12), 2129–2139
364 (2005). doi:10.1109/tip.2005.859383.

365 7. M.Johnson et al., On compressing encrypted data. IEEE Transactions on Signal Processing.
366 **52**(10), 2992–3006 (2004). doi:10.1109/tsp.2004.833860.

367 8. D.Schonberg et al., On blind compression of encrypted correlated data approaching the
368 source entropy rate. in 43rd Annual Allerton Conference, Allerton, IL, USA (2005).

369 9. R.Lazzeretti, M.Barni, Lossless compression of encrypted grey level and color images. in
370 16th European Signal Processing Conference, pp. 1-5, Lausanne, Switzerland (2008)

371 10. A.Kumar, A.Makur,Lossy compression of encrypted image by Compressing sensing
372 technique. in IEEE Region 10 Conference (TENCON2009), pp.1–6 (2009).
373 doi:10.1109/TENCON.2009.5395999.

374 11. X.Zhang, Lossy compression and iterative reconstruction for encrypted image. IEEE
375 Transformation on Information Forensics and Security. **6**(1), 53–58 (2011).
376 doi:10.1109/tifs.2010.2099114.

377 12. A.Bilgin et al., Scalable image coding using reversible integer wavelet transforms. IEEE
378 Transactions on Image Processing. **9**(11), 1972–1977 (2000). doi:org/10.1109/83.877218.

379 13. D.Taubman, High performance scalable image compression with EBCOT. IEEE
380 Transactions on Image Processing. **9**(7),1158–1170 (2000). doi:org/10.1109/83.847830.

381 14. Zhang Xinpeng et al., Scalable Coding of Encrypted Images. IEEE Transactions on Image
382 Processing. **21**(6),3108-3114. doi:org/10.1109/TIP.2012.2187671.

383 15. Edward J. Delp, O. Robert Mitchell, Image Coding Using Block Truncation Coding. IEEE
384 Transactions on Communications, 27, 1335-1342, (1979).
385 doi:org/10.1109/TCOM.1979.1094560.

16. M.D.Lema, O.R.Mitchell, Absolute Moment Block Truncation Coding and its Application to color images. IEEE Transactions on Communications. **32**(10),1148-1157, (1984). doi:org/10.1109/TCOM.1984.1095973.

17. P.Jeya Bright, G.Vishnuvarthanan, Development of a scalable coding for the encryption of Images using Block Truncation Code, in 3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019), pp.934-938, Tirunelveli, India, (2019). doi:org/10.1109/ICOEI.2019.8862525.

18. Ching-Nung Yang et al., Constructions of general (k,n) reversible AMBTC based visual cryptography with two decryption options. Journal of Visual Communication and Image Representation. **48**,182-194, (2017). doi:org/10.1016/j.jvcir.2017.06.012.

19. Guo-Dong Su, Chin-Chin Chang, A High Capacity Reversible Data Hiding in Encrypted AMBTC-Compressed Images. IEEE Access. **8**, 26984–27000, (2020). doi:org/10.1109/ACCESS.2020.2966234.

20. Chih-Cheng Chen et al., TSIA: A Novel Image Authentication Scheme for AMBTC-Based Compressed Images Using Turtle Shell Based Reference Matrix. IEEE Access. **7**,149515-149526, (2019). doi:org/10.1109/ ACCESS.2019.2944833.

21. Zhan Yu et al., HBF-DH: An Enhanced Payload Hybrid Data Hiding Method Based on a Hybrid Strategy and Block Features. IEEE Access. **7**, 148439–148452, (2019). doi:org/10.1109/ACCESS.2019. 2943505.

22. Stephen.T.Welstead, Fractal and Wavelet Image Compression Techniques, pp.155-156, SPIE Publication, Washington (1999)

23. Raouf Hamzaoui and Dietmar Saupe, Fractal Image Compression-Document and Image Compression, pp.168-169, CRC Press (2006)

24. Saravanan Alagarsamy et al., Multi-channeled MR brain image segmentation: A new automated approach combining BAT and clustering technique for better identification of

411 heterogeneous tumors. Biocybernetics and Biomedical Engineering. **39**(4), 1005-1035,
412 (2019). doi:org/10.1016/j.bbe.2019.05.007.

413 25. J.C.Chuang, C.C Chang, Using a simple and fast image compression algorithm to hide
414 secret information. International Journal of Computers and Applications. **28**(4),329–333,
415 (2006). doi:org/10.1080/1206212X.2006.11441818.

416 26. Duanhao Ou, Wei Sun., High payload image steganography with minimum distortion based
417 on absolute moment block truncation coding. Multimedia Tools Appl. **74**, 9117–9139,
418 (2014). doi:org/10.1007/s11042-014-2059-2.

419 27. Aruna Malik et al., A high payload data hiding scheme based on modified AMBTC
420 technique. Multimedia Tools Appl. **76**,14151–14167, (2017). doi:org/10.1007/s11042-
421 016-3815-2.

422 28. Jiantao Zhou et al., Scalable Compression of Stream Cipher Encrypted Images Through
423 Context-Adaptive Sampling. IEEE Transactions on Information Forensics and Security.
424 **9**(11),1857–1868, (2014). doi.org/10.1109/TIFS.2014.2352455.

425 29. Chia-Chen Lin et al., A Novel Reversible Data Hiding Scheme Based on AMBTC
426 Compression Technique. Multimedia Tools Appl, **74,** 3823–3842,(2013).
427 doi:org/10.1007/s11042-013-1801-5.

428 30. Chia-Chen Lin et al., Reversible Data Hiding for AMBTC Compressed Images Based on
429 Matrix and Hamming Coding. MDPI-Electronics. **10**(281), 1-20, (2021).
430 doi:org/10.3390/electronics10030281.