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

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

Abstract: ***In today's world, security of data from intruders and hackers during transmission and reception needs image encryption, and to reduce space requirement and faster transmission needs image compression, which tend to be the emerging research arenas. Especially for lossy compression, rebuilding of image equivalent to the transmitted original image is highly unachievable. So far many papers are reported for scalable coding on unencrypted images. We propose a scalable coding for encrypted images by Min-Max Block Truncation Coding Technique(MMBTC). The Min-Max Block Truncation Coding Technique compress the raw image and later encrypted by pseudorandom number, and the encoded bit streams are transmitted. The secret key is encryption key and communicated between encoder and decoder. In the decoding process, the compressed image is recovered with secret key and the raw image is rebuilded by using Min-Max Block Truncation Coding Technique.***

Keywords: Block Truncation Coding, Image Encryption, Min-Max Block Truncation Coding, Scalable Coding.

I. INTRODUCTION

In transmission and reception image encryption and image Compression have a vital role. The image encryption purpose is to secure/preserve the leakage of statistical information from attacker or hacker or intruder and there are many cryptographic techniques available for it, say for example, the study about signal processing in encrypted signals [1], Encrypted samples using homomorphic properties [2] and the problems in privacy protection [3]. In [4], the encrypted signals are represented as composite signals, which increase the speed for linear operations. The problem faced by the insertion of watermark copy in the original content by the seller is addressed by having an invisible watermarking technique, and if an unauthorized copy is sold by the buyer it can be proved [5], and a new method of encryption was introduced to identify the illegal copy by embedding a value before the finger-print [6].

There is large amount of image data are used in today's world which requires enormous amount of storage space. Also, it requires large bandwidth which makes the transmission costlier. For reduced storage space and to decrease the bandwidth size, it requires image compression. Image compression techniques will remove the irrelevant data and thereby reduces the data size requirement of digital image. Redundant Data either contain absence of relevant information or duplication of already known data. The image compression on images will give images with reduced data size, storage costs and transmission time. Without compression the file size is bigger usually megabytes and by doing compression nearly 10 percent of original file size is reduced without compensating the quality due to this loss. Lossy compression is used to remove some details with the help of techniques such that our eye can't identify it. Digital images contain pixels which are nothing but color information. The pixel values vary slightly from its neighborhood, it is replaced by theirs. This may cause some information to be lost but if the algorithm is good it can't be noticed by our eye. In [7], they proposed that in an insecure communication path, transmission of redundant data is done not in the traditional way but by reversing the order. In [8], a memory less source redundancy is achieved, which is inversely proportional to the square root of block length and it is implemented by using low density parity check codes for both memory and memory less sources.

In [9], compression is done for grey and color images by splitting as bit planes and the lower bit planes of the encrypted are erased without compromising the reconstructed image quality. The efficient pursuit algorithm is proposed [10] than the existing greedy algorithm, such as matching pursuit, orthogonal matching pursuit, and in these, image is encrypted first and then compressed using compressive sensing technique, and then decoded using basis pursuit algorithm. This paper [11] proposes image encryption by pseudorandom permutation and excessive rough coefficients are removed during image compression and original content is reconstructed by using iterative reconstruction method.

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

Scalability means manipulation of bit stream or file. Scalability is especially useful for previewing images while downloading them from web browser. Various scalability techniques are available and some of them are rate scalability and resolution scalability. Scalability is reported for unencrypted images such as in [12] a new scalable image coder is used, in which reversible integer wavelet transform and bit plane coder are there; such that desired scalability is achieved. In [13], SNR scalability is achieved by using a new algorithm namely EBCOT, and up to this, scalable coding is done on only unencrypted images. In [14], reported first for encrypted images using scalable coding, in which image compression is done by Hadamard Transform, image encryption by pseudorandom number technique and original principal content, and is reconstructed by means of iterative updating procedure. It has higher computational complexity, lower PSNR, lower wPSNR, lower compression ratio and the bit error rate, MSE and wMSE are poor. In [16], the scalable coding on encrypted images is done by using BTC, where the raw image is compressed using BTC and then encryption is done by adding the compressed pixel value with the generated pseudorandom number value between the range 0 to 255, and the encoded bit stream is transmitted. The encrypted key is communicated between encoder and original principal content is rebuilded at decoder by decrypting the transmitted content with encrypted key and then rebuilded using BTC technique.

We propose a new method for scalable coding in encrypted images by using an improved version of BTC namely Min-Max Block Truncation Coding (MMBTC). In this, the raw image is compressed by using MMBTC technique and then the image encryption is performed by pseudorandom number technique, and the encoded bit streams are transmitted. The encrypted key is communicated between encoder and decoder. The original principal content is reconstructed by decrypting the transmitted encoded bit stream with encrypted key and then reconstructed using MMBTC Technique. Our proposed method has lower computational complexity, since it lends to parallel processing and each block is independent. Also, it has improved PSNR, wPSNR, compression ratio, bit error rate, MSE and wMSE.

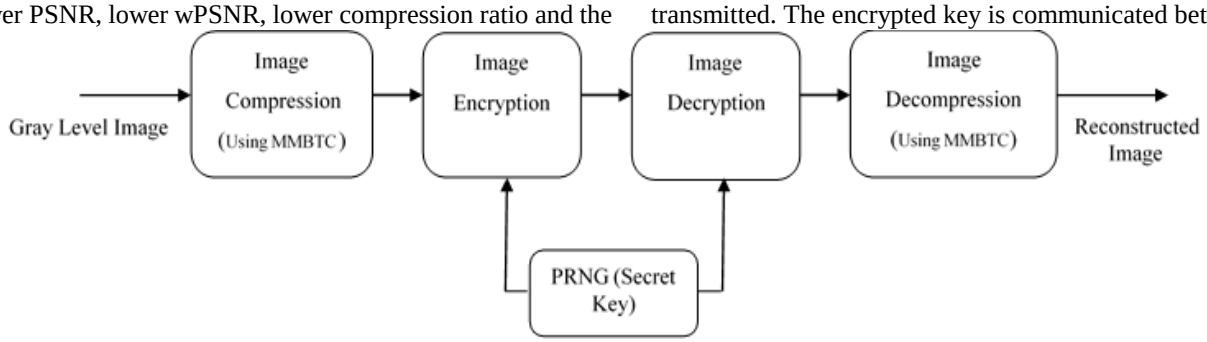

Fig. 1. Proposed System

II. PROPOSED METHOD

Fig.1 is the proposed method, in which raw pixel value is compressed with MMBTC Technique. The compressed pixel will be in binary form with values "0" and "1". Image encryption is done by combining the compressed pixel value with the encrypted key that is attained by generating pseudorandom numbers between the range 0-255, and the encoded bit streams are transmitted. The encrypted key is communicated at both ends. At the decoder side, the transmitted encoded bit streams are decoded by first decrypting with the secret key, and the original principal content is rebuilded by using MMBTC Technique. The rebuilded image shows higher resolution and improved compression ratio, PSNR, wPSNR, MSE, wMSE and bit error rate.

A. Image Encoding

Image Compression

The raw gray image will be uncompressed and the pixel values are within 0 and 255, which can be shown in a matrix format of size D1*D2, where D1 is size of row and D2 is size of columns. The raw image is compressed by using MMBTC Technique. MMBTC steps are given below: -

Step1: - Divide the input image of size 512*512 into non overlapping blocks of size D*D, where D is taken as 4, typically.

Step 2:- Calculate the mean ($\bar{x}$) value, diagonal maximum(dh) and minimum value(dl) for each non-overlapping blocks and their values vary from each block to block. The diagonal minimum value and the diagonal maximum value will act as two quantizer values of MMBTC.

Step 3: - The mean ($\bar{x}$) is chosen as threshold value. In the Non-overlapping blocks, whose pixel values greater than or equal threshold value is represented as "1", and remaining is represented as "0" in the binary block and it is denoted as m_i and the bit amount value is 8N which is given as

$$m_i(i,j) = \begin{cases} 1, & GraylevelPixelvalue \geq \bar{x} \\ 0, & GraylevelPixelvalue < \bar{x} \end{cases} \quad (1)$$

Image Encryption

The gray level pixel values are in the range between 0 and 255. The pseudorandom number generator is used to generate the values between 0 and 255 of size D1*D2 having length 8N. This secret key is communicated between encoder and decoder. The encryption process is done by adding the compressed pixel value and secret key where both having size D1*D2 and then modulo 256 operations is taken, which is given as:

$$em(i,j) = mod[m(i,j) + rm(i,j), 256] \quad (2)$$

$$1 \le i \le D_1 , \quad 1 \le j \le D_2$$

Where $m(i,j)$ is the compressed value $rm(i,j)$ is the secret key and $em(i,j)$ 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. The Fig. 2(a) and Fig.2(b) shows the input gray image and its encrypted image.

Fig.2(a). Original Image

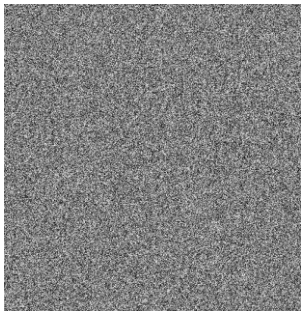

Fig.2(b). Encrypted Image

A. Image Decoding

Image Decryption

The decrypted output is extracted from the encoded bit stream by subtracting the encoded bit stream with the secret key and then taking modulo-256 operations which is given as

$$dm(i,j) = mod[em(i,j) - rm(i,j), 256] \quad (3)$$

Where $em(i,j)$ represents the transmitted encoded pixel value and $rm(i,j)$ represents the secret key which is shared by the encoder and $dm(i,j)$ is the decrypted pixel value. The decrypted pixel value contains the binary values "0" and "1".

Image Reconstruction

The original principal content is rebuilded in the Image Reconstruction process by using Min-Max Block Truncation Coding. The diagonal maximum value and the diagonal minimum value are communicated by the encoder to the decoder. The decrypted pixel values in the non-overlapping block are replaced by diagonal maximum and diagonal minimum values, respectively, which are shared by the encoder. The binary value "1" in the decrypted block is replaced by diagonal maximum value (dh) and the binary value "0" is replaced by diagonal minimum value (dl). Thus the original principal content of the image is reconstructed, which is given as:

$$mout(i,j) = \begin{cases} dh, & dm(i,j) = 1 \\ dl, & dm(i,j) = 0 \end{cases} \quad (4)$$

Where dh is the diagonal maximum value of each non-overlapping block and dl 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 Min-Max Block Truncation Coding Technique. This paper proposes the resolution scalability such that from lower resolution of lossy image is reconstructed with higher resolution. On comparing the reconstructed image with the original image, both images look similar.

Fig.4(a). Original Image

Fig.4(b). Reconstructed Image

ii. Comparison Parameters

Compression Ratio:

The formula for compression ratio is given as:

$$Compression\ Ratio = \frac{file\ size\ of\ uncompressed\ image}{file\ size\ of\ compressed\ image} \quad (5)$$

Bit Rate:

The formula for bit rate is given as:

$$bit\ rate = \frac{b}{compression\ ratio} \quad (6)$$

Where b is uncompressed image bits per pixel.

MSE

The MSE is given as:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[mout(i,j) - min(i,j)]^2 \quad (7)$$

Where, $mout(i,j)$ is the reconstructed principal content, and $min(i,j)$ is the original principal content and m and n are size of rows and columns..

wMSE:

The wMSE is given as:

$$wMSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(2\left|\frac{mout(i,j)-min(i,j)}{mout(i,j)+min(i,j)}\right|\right)^2 \quad (8)$$

Where, $mout(i,j)$ is the reconstructed principal content and $min(i,j)$ is the original principal content and m and n are size of rows and columns

PSNR:

The PSNR ratio is a metrics about quality of rebuilded image. If the MSE is less, then PSNR value will be more and vice-versa. If the PSNR value obtained is higher than the reconstructed image, quality is better and also nearer to original principal content.

The formula for PSNR is given as:

$$PSNR = 10\ log_{10}\frac{255^2}{MSE} \quad (9)$$

Where, MSE represents Mean Square Error.

wPSNR

The wPSNR is given as:

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

Where wMSE is the weighted Mean Square Error.

Table I list the experimental values for all parameter for various input images using MMBTC.

Table- I: Comparison Parameter values for Input Images

INPUT IMAGE	CR	BR	MSE	wMSE	PSNR	wPSNR
Lena	0.81	3.17	77.7	0.0091	29.22	68.5
Cameraman	0.84	3.06	89.5	-	28.61	-
Pout	0.91	2.79	6.97	0.0004	39.69	81.3
Rice	0.85	3.00	57.3	0.0045	30.54	71.6
Football	1.02	2.51	37.8	0.0052	32.35	70.9
Peppers	1.06	2.41	35.4	0.0049	32.63	71.2

IV. CONCLUSION

In this, we presented a new method for scalable coding on encrypted images namely MMBTC. We have chosen diagonal minimum value and diagonal maximum value of each non-overlapping block as quantizers, which shows the reconstructed image has better quality. We have implemented this by compressing the input image by Min-Max Block Truncation Coding Technique and then image encryption by pseudorandom number technique. The encoded bit stream is transmitted along with secret key, where the secret key is communicated between encoder and decoder. In decoder, the transmitted encoded bit stream is decrypted using encrypted key to extract the compressed pixel value, and then the original principal content is rebuilded by using MMBTC Technique. We have experimented on various images using this Min-Max Block Truncation Coding technique and we measured parameters such as Compression ratio, Bit rate, PSNR, Wpsnr, MSE and wMSE. Our method has less computational complexity since only diagonal maximum values and diagonal minimum values are used in reconstruction and also support parallel processing. Our experimental results show better compression ratio, Bit rate, PSNR, wPSNR, MSE and wMSE. Also, the reconstructed image quality is better and shows equivalent to original image.

This paper has chosen mean value as the threshold to construct the binary block, and it 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' Industry experience in Mainframes with 3 years worked in USA.He has more than 15 years of teaching experience and has his affilation as Associate Professor and Head with the Department of Electronics and Communication Engineering, in the DMI Engineering college, Aralvoimozhi, Kanyakumari District, Tamilnadu, India. 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.