Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFECTIVE APPROACH OF IMAGE RETRIEVAL USING SCALABLE IMAGE ENCRYPTION

K.SRILATHA
Assistant Professor.
Department of Electronics and Communication Engineering,
Sathyabama University, Chennai, Tamilnadu, India.
E-mail: srilatha169@gmail.com,

ABSTRACT

The encryption has a comprehensive scheme for providing confidentiality of security such as privacy, reliability and authentication of information. This paper proposes a unique scheme of scalable coding of transmitting and receiving images in an extreme protected way using Absolute Moment block truncation coding (AMBTC). The gray level pixel of image has compressed by AMBTC then encrypted image is acquired by adding compressed AMBTC pixel value that has masked by a modulo-256 addition with PRNG (Pseudo Random Number Generator) that has derived from a secret key Subsequently encrypted image data into a down sampled sub image and some data groups using a multiple-resolution creation, an encoder gives the quantized sub image and the Harr coefficients of all data set to reduce the data. Then, the data of quantized sub image and coefficients are held as a set of bit streams transmitted. At the receiver side, although a sub image is decrypted to give the rough information of the original image, the quantized coefficients are used to reconstruct the original image with an iterative procedure. Due to the hierarchical mechanism, the original image with higher resolution reconstructed by decompressing the decrypted pixel value using AMBTC.

Keywords: *Scalable Coding, Harr Transform, Image Compression, Image Encryption/Decryption, Absolute Moment Block Truncation Coding (AMBTC)*

1. INTRODUCTION

Now a day, encrypted signal processing is involved significant research interests. The frequency domain and adaptive filtering can be engaged in the encrypted area based on the homomorphic properties of a cryptography [3], [4], and a complex signal representation method can be used to decrease the size of encrypted information and computation difficulty [2]. In both encryption and information hiding, a part of important data signal is encrypted for content security, and the residual data are used to bring the additional message for rights protection. With several buyer–seller code of behaviour [1], [9], the some secrete data such as balm print, finger print are embedded into an encrypted form of digital multimedia to make sure that the seller cannot know the buyer's watermarked version while the buyer cannot obtain the original product.

The quantity of image data develops progressively. Large storage and bandwidth are required to store and transmit the images which are quite costly. Therefore methods to compress the image data are important nowadays. In [8] first compressing and then encrypting a data stream it without negotiating either the compression efficiency or the information security and the encrypted data are compressed using source coding principles, since the key will be obtainable at the decoder. The blind communication of an encrypted basis [8] has used not only memory less sources but also sources with hidden Markov correlation using LDPC codes, taking benefit of their decoding error discovery capability. In [10] in place of compressing bi-level images specifically sparse black and white images, In [7]a basis detection algorithm is used to allow joint decryption and decompression. But the rate of error performance is low. The original image of compressed gray level is encrypted by pseudo random pixel permutation in [7] and fine information coefficients in the transform area and then reconstructed with the content of the original image by iterative updating the coefficient values with the assistance of spatial correlation in usual image. In [13] this technique the pixel places are shuffled only so as to the enemy without the knowledge of the secret key can take the information from an encrypted image. Besides, several techniques for loss compressing encrypted

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

images are developed. In [13], a compressive identifying tool is bring together to achieve the loss compression of encrypted images, and a basis detection algorithm has used to allow joint decryption and decompression. While having the compressed data and the permutation way, a receiver can be reconstructed the content of the original image by retrieving the coefficient values. Yet, the error distortion performance is low, and there is a leakage of statistical data in [14] then only the pixel positions were shuffled and the pixel values were not masked in the encryption phase.

This proposed scheme presents a scalable coding of encrypted gray level images and compression using AMBTC. Scalable coding of unencrypted images [1], [10] and for encrypted images have been reported. In this method, better compression is done by using AMBTC and also the attacker cannot take any statistical data. AMBTC is a recent technique used for compression of monochrome image data. It is to execute moment preservative quantization for blocks of pixels so as to quality of image will endure satisfactory and simultaneously the demand for memory storage will be decreased.AMBTC has grown popularity because of its real-world usefulness. At the receiver using secret key and decompression the original content is reconstructed.

2. PROPOSED LOSSY COMPRESSION AND SCALABLE CODING OF ENCRYPTED GRAY LEVEL IMAGES

The block diagram of the proposed system is shown in Fig.No.1.In the proposed system, the input gray level pixel value has compressed by using Absolute Moment Block Truncation Coding. It is a recent technique used for compression of Gray level image data. The compressed pixel values are encrypted by generating a series of (PRN) pseudorandom numbers which doing as a secret key and then transmitted. At the receiver, decryption has done by using secret key and the compressed pixel value is acquired. The original gray image has reconstructed by decompressing using Absolute Moment Block Truncation Coding. The reconstructed image shows higher resolution, higher BR, WPSNR, SSIM, CR and improved entropy.

A. Image Compression

The input gray level image has uncompressed format and that the pixel values are having within [0,255] denoted in a matrix format N1 * N2 where N1 is the number of rows and N2 as the number of columns. The input image has been compressed by using Absolute Moment BTC (AMBTC) [8] that conserves the higher mean and lower mean of an each block. The AMBTC algorithm consists of the following steps:

•S1: An image is divided into non overlapping blocks. The dimensions of a block can be (4 * 4) or (8 * 8), etc.

•S2: Compute the average gray level of the block (4x4) as equations (1)

•S3: Pixels in the image block has categorized into two ranges of values. The upper range is those gray levels which are larger than the block average gray level (x) and the residual carried into the lower range. The mean of higher range H_{range} and the lower range L_{range} are calculated as:

$$H_{range}=\frac{1}{M}\sum_{Ki>K1}^{n} Ki$$

$$L_{range}= \frac{1}{16-M}\sum_{Ki<K1}^{n} Ki \qquad (1)$$

Here M is the number of pixels whose gray level is more than *K.*

•S4: Binary block, represented by R_b, is used to represent the pixels and also use “1” to represent a pixel as equation (2) whose gray level is larger than or equal to *x* and “0” to denote a pixel whose gray level is less than K_1.

$$R_b = \begin{cases} 1 & Ki \geq K1 \\ 0 & Ki < K1 \end{cases} \qquad (2)$$

By this method each block has reduced to a bit plane. Whole blocks of the AMBTC compressed image will have the same mean and standard deviation of the original image. The thresholding procedure makes it possible to make a replica a sharp edge with high fidelity, taking improvement of the human visual system’s ability to do local spatial integration and mask errors. Thus input gray level image is compressed using AMBTC as in Fig.No.2

B. Image Encryption

The compressed image bit quantity is 8N. Pseudo random number is made between the values [0,255] for the dimension N1 * N2.The length of pseudorandom bit order is 8N.The pseudorandom number generator (PRNG) performance as a secret key and shared between encoder and decoder. The encrypted image is acquired by adding both compressed image of size N1 * N2 and pseudo

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

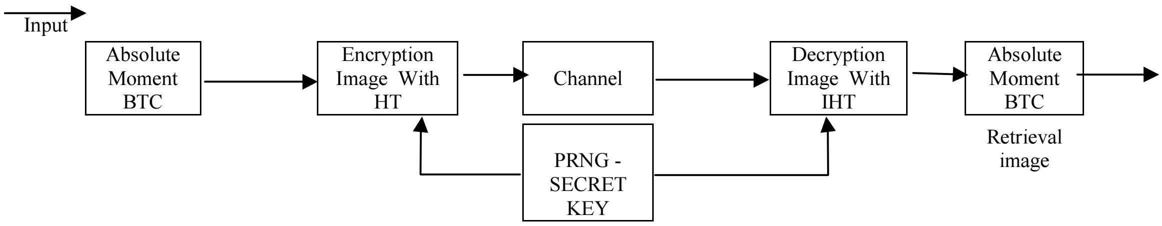
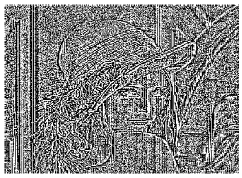


Fig.No.1 Block Diagram of Proposed System

Image

(a).Original Image-I

(b).Gray Image-I



(c) AMBTC Compressed Image I

Fig.No.2.Image Compression

random number of dimensions N1*N2 and then taking modulo-256 operations. It is specified as equation (3):

$$ep^{(T+1)}(i,j)=mod[s(i,j)+k(i,j),256] \quad 1\le i\le N_1,\ 1\le j\le N_2, \qquad (3)$$

Where P (i, j) represents the compressed image values of pixels at locations (i, j), k (i, j) represents the pseudorandom numbers within [0,255] produced by PRNG and ep(T+1)(i,j) represents the encrypted pixel values. Fig. 3 gives an original image and its encrypted form. It has well known that is no probability polynomial time (PPT) algorithm to discriminate a pseudo random number sequence up till now. Consequently, any PPT adversary cannot discriminate an encrypted pixel sequence and a random number(PN) sequence. Specifically image encryption

Image algorithm that proposed scheme is semantically protected compared to any PPT adversary. The block has transmitted along with PRNG (pseudorandom numbers generator) and Mean and Standard Deviation values.

C. Encrypted Image Encoding

Even though an encoder has not known the secret key and the unique content, it compress the encrypted data as a set of bit streams. The comprehensive encoding process is as follows and scalable encoding output shows in Fig.No.3.First, the encoder decomposes the encrypted image into a series of sub images and data sets with a multiple-resolution construction. The sub image at the (t+1)th level is produced by down sampling the sub image at the ep(T+1)th level as follows (4):

$$ep^{(T+1)}(i,j)= ep^{(T)}(2i,2j),\ T=0,1,\ldots,t-1 \qquad (4)$$

Where $ep^{(T)}$ is just the encrypted image and T is the number of decomposition levels. In addition, the encrypted pixels that belong to (t+1) but do not belong to $ep^{(T)}$ form data set $W^{(t+1)}$ as follows (5):

$$W^{(t+1)}=\{ep^{(T)}(i,j)|mod(i.2)=1 \quad Mod(j,2)=1\},$$
$$T=0.1\ldots\ldots t-1. \qquad (5)$$

For each data set W(t) (t= 0,1,…..T) the encoder permutes and divides encrypted pixels in it into $A^{(t)}$ groups, each of which containing $B^{(t)}$ pixels $A^{(t)} * B^{(t)}=3N/4^t$ .In this manner, the $A^{(t)}$ pixels in the same set scatter in the whole image. The permutation technique is public by the encoder and the decoder, and the values of $B^{(t)}$ will be conferred later. Represent the encrypted pixels of the A^{th} set as $ep_k^{(T)}(1)$, $ep_k^{(T)}(2)$,…. $ep_k^{(T)}(B^{(t)})$ and perform the Harr transform in each group as equation (6):

$$[D_K^{(T)}(A^{(t)}]_{1*k}=H*[ep_k^{(T)}(A^{(t)})]_{1*k} \qquad (6)$$

Where $A^{(t)}* A^{(t)}$ is a Harr matrix equation (7) made up of +1 or -1. That involves the matrix H meets $H'*H=H*H'=B^{(t)} * I$

Where

$$H=\frac{1}{\sqrt{N}}\begin{cases} 2^{P/2} & ,\frac{q-1}{2^P}\le x<\frac{q-0.5}{2^P} \\ -2^{P/2}, & \frac{q-0.5}{2^P}\le x<\frac{q}{2^P} \\ 0 & otherwise \end{cases} \qquad (7)$$

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

where H' is a transpose of H,I is an $B^{(t)} * B^{(t)}$ identity matrix, and $B^{(t)}$ must be a multiplied by 4. For each coefficient $D_K^{(T)}$ (l) calculate equation (8)

$$dk(t)(l) = \left\lceil \frac{mod[Dk(t)(l),256]}{256/H(t)} \right\rceil \quad (8)$$

Where H(t)=round (H/sqr $B^{(T)}$)
H- is an integer shared by the encoder and the decoder, If the channel bandwidth is limited, the later bit streams can be abandoned. A higher resolution image can reconstruct when more bit streams are acquired at the receiver. Now, the total C_R compression ratio equation (9) which is a ratio between the quantity of the encoded data and the encrypted image data, is

$$CR = \frac{Log2H}{8.4\,L} + \frac{3}{8} * \sum_{t=1}^{T} Log2.H(t)/4t \ldots \quad (9)$$


(a).Original Image-I

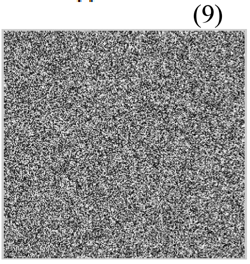

(b).Encrypted Image-I

Fig.No.3.Scalable Coding Encryption

D. Image Reconstruction

With the bit streams and the secret key, a receiver can be reconstructed the main content of the original image, and the resolution of the restored image is dependent on the number of received bit streams. Although BG offers the rough information of the original content, $BS^{(t)}$ may be used to reconstruct the complete content with an iterative technique. The image reconstruction process is as follows.

Hence, the receiver may be used an iterative procedure to increasingly improve the quality of the reconstructed image by updating the pixel values along with $D_K^{(t)}$(l).The complete procedure is as follows.

1) For each group $[P_k^{(t)}(1), P_k^{(t)}(2),\ldots P_k^{(t)}(B^{(t)})]$ calculate $P'^{(t)}_k(l)$ from equation (10)

$$P'^{(t)}_k(l)=mod[P_k^{(t)}(B^{(t)})+e_k^{(t)}(B^{(t)}),256]$$
$$1\leq b^{(t)}\leq k,\ 1\leq a^{(t)}\leq l, \quad (10)$$

$e_k^{(t)}$ PN derived from secret key

2) Calculate Decryption from equation (11) and (12)

$$D_{cry}(t)(l))=mod\,[D_K^{(T)}]*\Delta(t)+\Delta(t)/2- D'^{(T)}_K(l),256] \quad (11)$$

where

$$D'^{(T)}_K(l)=\begin{cases} Dcry(t)(l), & if\ dk(l) < 128 \\ Dcry(t)(l)) - 256 & if\ dk(l) \geq 128 \end{cases}$$

$$[P'_K(t)*B(T)]=[\,P_K(t)*B(T)]+H'/B(T)[D'_{cryt}(B(T)] \quad (12)$$

D. Image Decompression

The original image has been reconstructed by means of Absolute Moment Block Truncation Coding. To reconstruct the original image shown in Fig.No.4 and Fig.No.5, elements assigned as "0" are substituted with the value A' and elements assigned as "1" are substituted with the value A .The original image can be reconstructed by using equation (13) and (14),

In the decoder, an image block is reconstructed by replacing the `1' s with H and the '0''s by L In the AMBTC,if need 16 bits to code the bit plane which is similar as in the BTC. But, AMBTC involves less computation than BTC.

$$K = \begin{cases} Lrange & Rb = 0 \\ Hrange & Rb = 1 \end{cases} \quad (13)$$

$$P(i,j)=\begin{cases} A, Dcryt(t+1)(i,j) = 1 \\ A', Dcryt(t+1)(i,j) - 0 \end{cases} \quad (14)$$

AMBTC has a number of advantages over BTC some advantage is in the case that the quantizer is used to transmit an image from source to a destination, it is essential to compute at the transmitter the two quantities, the sample mean and sample standard deviation for BTC and example first absolute central moment for AMBTC.

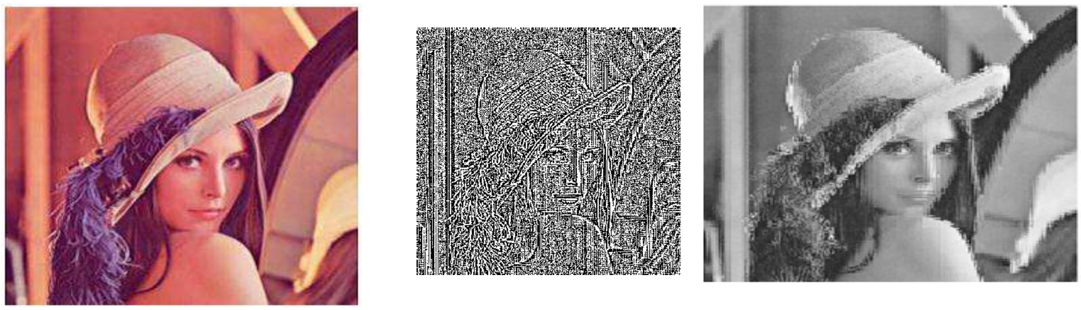
When compare the computation for deviated information, in case of standard BTC it is computed a sum of m values and every one of them will be squared however AMBTC is only essential to compute the sum of these m values. Meanwhile the multiplication time is numerous times larger than the addition time in most digital processors, thus using AMBTC the entire calculation time at the transmitter is considerably reduced.

3. IMAGE QUALITY MEASUREMENTS

It plays important roles in several images processing application .When image compression system is designed and implemented; it is significant to be capable to estimate its performance. This estimation should be done in such a way to be able to comparing results with other image compression methods. The image

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

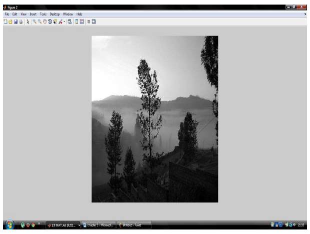
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



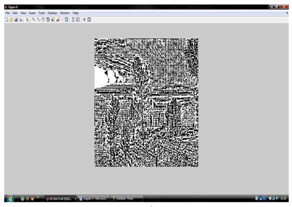
(a).Original Image-I *(b).Decrypted Image-I* *(b).Decompressed Image-I*

Fig.No.4.Scalable Coding Decryption and Decompressed Image

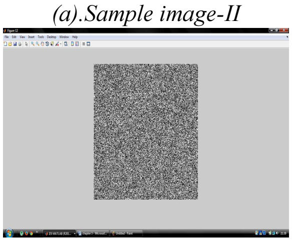
(a).Sample image-II



(b).The input image has been converted to a gray image

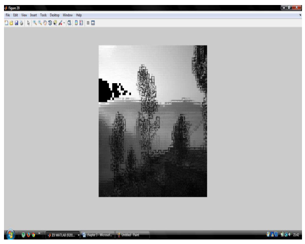


(c).Compressed image

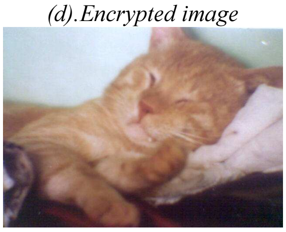


(d).Encrypted image

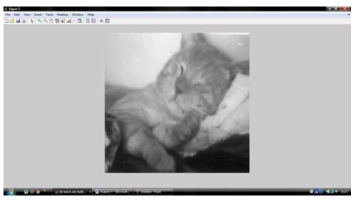
(e).Decrypted image



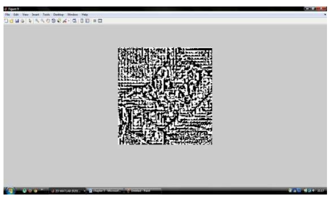
((f).Decompressed Image



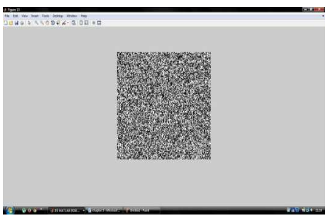
(g).Sample image-III



(h).The input image has been converted to a gray image

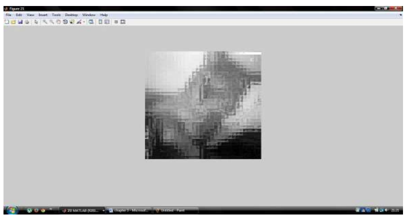


(i).Compressed image



(j).Encrypted image

(k).Decrypted image



(l).Decompressed Image

Fig.No.5.Scalable Coding Encryption and Decryption results of different Image

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

quality metrics can generally classified into two classifications, subjective and objective. subjective image quality is a technique of estimation of images by the observer's read images directly to decide their feature. in objective procedures of image quality metrics, certain statistical indices are calculated to show the image quality. In the proposed work will focus in objective[9]-[10] measures such as 1.Peak Signal to Noise Ratio (PSNR),2.Weighted Peak Signal to Noise Ratio (WPSNR), 3.Bit Rate (BR) and 4.Structural Similarity Index (SSIM).

1.Peak Signal to Noise Ratio (PSNR)

$$PSNR=10*Log_{10}(L^2/MSE) \quad (15)$$

Where $MSE=\frac{1}{kl}*\sum_{i=1}^{k}*\sum_{j=1}^{l}[y(i,j)-x(i,j)]^{\wedge 2}$

2. Weighted Peak Signal to Noise Ratio (WPSNR)

$$WPSNR=10Log\left[\frac{L^{\wedge}2}{|(Y-X)/(1+\theta\sigma^{\wedge}2(i,j))|}\right] \quad (16)$$

Where

$$\sigma^2(i,j)=\frac{D}{(2L+1)}*\sum_{i=1}^{k}*\sum_{j=1}^{l}[x(i+k,j+l)-x'(i,j)]^{\wedge 2}$$

3. Bit Rate (BR)

$$B_R = (B/CR) \quad (17)$$

Where B- bits per pixel of the uncompressed image, CR the Compression Ratio

4. Structural Similarity Index (SSIM).

$$SSIM(x,y)=\frac{(2\mu x\mu y+C1)(2\sigma xy+c2)}{(\mu x^2+\mu y^2+c1)(\sigma x^2\,\sigma y^2+c2)} \quad (18)$$

Where c1=(M1 L)2,M1⋘1 and c2==(M2 L)2,M2⋘1

Fig.No.5. Performance of the proposed scheme with BTC BTC

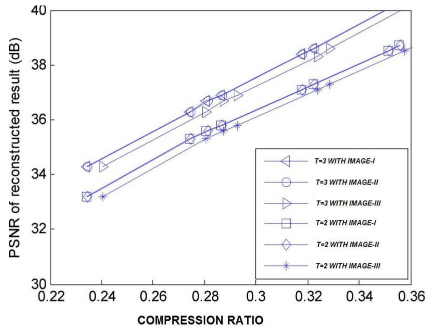


Fig.No.6. Performance of the proposed scheme with different T value

4. RESULTS AND DISCUSSION

Three testing Images-I,II,III that are sized 512 * 512 had used as the original images in the experiment. Let T=3 and encoded the encrypted images are using H=24,$B^3(t)$= 4, $B^2(t)$= 8 and $B^1(t)$=24 to generate the bit streams BG, BS^3, BS^2 and BS^1. In this occasion, the total compression ratio CR=0.326 and provides the reconstructed Images-I using {BG},{BG BS^3},{BG BS^3 BS^2}and {BG BS^3BS^2BS}correspondingly. Reconstructed results with greater resolution have gotten while extra bit streams were used. The PSNR is generally used as a degree of quality of restoration of lossy compression. It is an smart measure for the loss of image quality because of its ease and mathematical accessibility. Peak Signal to Noise Ratio (PSNR) is a qualitative measure based on the Mean Square Error (MSE) of the reconstructed image. If the reconstructed image is proximate to the original image, then Mean Square Error (MSE) is small and PSNR taking a large value.PSNR is dimensionless and is stated in decibel. The values of PSNR in restored results are represented as PSNR1, PSNR2, Although the PSNR values of Images-I are 15.1064 and 39.2590 dB, those of Images-II are 16.8595 and 49.2314dB. Images-III are 14.2389 and 28.1718 dB Moreover, the iterative updating technique expressively enriched the reconstruction quality. Compared with the results in Table II, the new CR-PSNR1 performance of Images-III is better, whereas that of Images-I is poorer. The reason is that Images-III is smoother than Images-I. For Images-I, the larger B(t) was supportive to evenly distribute the errors on pixels into the Harr coefficients, When an encrypted image is decomposed within further levels, more data are convoluted in quantization and compression; consequently, the CR-PSNR1 performance is better, and more iterations for image reconstruction are

Journal of Theoretical and Applied Information Technology
20th February 2015. Vol.72 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

necessary. It is presented that the performance upgrading is not important as soon as using a higher T above 3. To compare among the used compression methods, three parameters were calculated. These are BR, WPSNR, and SSIM while a block dimensions is 8*8. These values are enumerated in Table.1.that the image compression using AMBTC offers improved image quality than image compression using BTC at the similar bit rate. Besides, the AMBTC is reasonably faster compared to BTC. But, a decoder with greater computation complexity and the decoder's feedback for transfer rate of each bit plane required in the method extended. The proposed system is more suitable for real-time decompression without feedback channel

Table.1.AMBTC and BTC Parameters

Image		BR	WPSNR	SSIM
I	BTC	1.25899	34.65	0.874
	AMBTC	1.25899	34.98	0.882
II	BTC	1.25899	33.07	0.826
	AMBTC	1.25899	33.89	0.828
III	BTC	1.25899	33.71	0.861
	AMBTC	1.25899	34.66	0.868

Table 2: Simulation results on the given sample images

Image	PSNR1	PSNR2	MSE1	MSE2	Entropy
I	15.1064	39.2590	1.1422e+04	708.1606	7.7452
II	16.8595	49.2314	9.3348e+03	224.6511	7.7254
III	14.2389	28.1718	1.2622e+04	2.5380e+03	7.7143

5. CONCLUSION

This proposed scheme has a novel approach of scalable coding for encrypted images and image compression using Absolute Moment block truncation coding has been examined The original image is encrypted by a modulo 256 addition with (PN) pseudorandom numbers, and the encoded bit streams are made a quantized encrypted sub image and the quantized remains of Harr coefficients. At the receiver, whereas the sub image is decrypted to create an approximate image, the quantized data of Harr coefficients can be offered more exhaustive data for image reconstruction. Meanwhile the bit streams are made with a multiple-resolution construction, the principal content with higher resolution obtained while more bit streams are received. The lossy compression AMBTC and scalable coding for encrypted image with better performance merits more analysis in the future.

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, pp. 1–20, Jan. 2007.

[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, pp. 86–97, Mar. 2009

[3]. Xinpeng Zhang, Member, IEEE, Guorui Feng, Yanli Ren, and Zhenxing Qian*"Scalable Coding of Encrypted Images"* IEEE transactions on image processing, vol. 21, no. 6, june 2012.

[4] Rafael C. Gonzalez, Richard Eugene; *"Digital image processing",* Edition 3, 2008, page 466

[5]M. Ghanbari *"Standard Codecs: Image Compression to AdvancedVideo Coding"* Institution Electrical Engineers , ISBN: 0852967101,2003 , CHM , 430 pages.

[6] Delp, E. J., Saenz, M., and Salama, P., 2000, *Block Truncation Coding (BTC), Handbook of Image and Video Processing,* edited by Bovik A. C., Academic Press, pp. 176-181.

[7] Franti P, Nevalainen O, Kaukoranta T. *Compression of Digital Images by Block Truncation Coding: A Survey,* The Computer Journal, Vol. 37, No. 4, 1994.

[8] C. C. Tsou, S. H. Wu, Y. C. Hu, *"Fast Pixel Grouping Technique for Block Truncation Coding,"* 2005 Workshop on *"Consumer*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Electronics and Signal Processing (WCEsp 2005)", Yunlin, Nov. 17-18, 2005

[9] M.D.Lema, O.R.Mitchell, *"Absolute Moment Block Truncation Coding and its Application to Color Image",* IEEE Trans. Coomun., Vol. COM-32, No. 10, pp. 1148-1157, Oct. 1984.

[10] Somasundaram, K.and I. Kaspar Raj. *"Low Computational Image Compression Scheme based on Absolute Moment Block Truncation Coding".* May 2006. Vol. 13.

[11] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, *"Toward compression of encrypted images and video sequences,"* IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[12] A. Kumar and A. Makur, *"Lossy compression of encrypted image by compressing sensing technique,"* in Proc. IEEE TENCON, 2009, pp.1–6.

[13] X. Zhang, *"Lossy compression and iterative reconstruction for en- crypted image,"* IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[14] 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, pp. 1972–1977, Nov. 2000.

[15] D. Taubman, *"High performance scalable image compression with EBCOT,"* IEEE Trans. Image Process., vol. 9, no. 7, pp. 1158–1170,
Jul. 2000.

[16] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, *"A commutative digital image watermarking and encryption method in the tree structured Haar transform domain,"* Signal Process. Image Commun., vol. 26, no. 1, pp. 1–12, Jan. 2011.

[17] N. Memon and P. W. Wong, *"A buyer-seller watermarking protocol,"* IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr.2001.

[18]M.Kuribayashi and H. Tanaka, *"Finger printing protocol for images based on additive homomorphic property,"* IEEE Trans. Image Process., vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

[19] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, *"On compressing encrypted data,"* IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[20]D.Schonberg, S. C. Draper, and K. Ramchandran, *"On blind compres- sion of encrypted correlated data approaching the source entropy rate,"* in Proc. 43rd Annu. Allerton Conf., Allerton, IL, 2005.