ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9797-9803

A Novel Combination of Encryption and Compression for Privacy Protection by Using BTC

[1] Kancharla Murali, [2] Mr.B.Vishnu Vardhan

[1]M.Tech Student, Dept of CSE, PVP Siddhartha Institute of technology, Kanuru (V), Penamaluru (M), Krishna(Dist), A.P, India
murali.kancharla1228@gmail.com

[2] Assistant Professor, Dept of CSE, PVP Siddhartha Institute of technology, Kanuru (V), Penamaluru (M), Krishna(Dist), A.P, India
vishnu.pvpsit@gmail.com

ABSTRACT

The privacy protection between the buyer and the respective seller is a area of concern in the area of digital image procession security domain. From last few decades it has been an area of research for many researchers due to its high equipped prominence protection of information between buyer and seller. The Proposed work presents new approach to transmitting the digital images using a framework named block truncation coding. The proposed block truncation coding framework main approach is to compress the images according to original gray level pixel value in high equipped manner. Addition of BTC pixel value along with the pseudo random number to obtain the encrypted image in an efficient way and then transmits the obtained encrypted image. Finally at the receiver side the compressed pixel value is obtained by using cryptographic key which is done in well equipped manner and latter the original image is obtained successfully by decompressing the decrypted signal using the BTC approach.

Keywords: Image compression; Image encryption; Lossy compression; Image reconstruction; Block Truncation Coding

INTRODUCTION

The quantity of image information grows day by day. Massive storage and information measure are required to store and transmit the photographs that are kind of expensive. Therefore strategies to compress the image information are basically now-a-days. The compression techniques are classified into 2 main classifications specifically lossy compression techniques and lossless compression techniques [1]. Lossless compression quantitative relation provides smart quality of compressed pictures however yields solely less compression whereas the lossy compression techniques [2] result in loss of information with higher compression quantitative relation. JPEG [1] and Block Truncation secret writing [3] may be a lossy image compression techniques .It is an easy technique that involves less procedure complexness. BTC may be a recent technique used for compression of monochrome image

information. it\'s one-bit reconciling moment-preserving quantize that preserves sure applied mathematics moments of little blocks of the input image within the quantity output. The first formula of BTC preserves the quality mean and also the variance [9]. The applied mathematics overheads Mean and also the variance are to be coded as a part of the block. The truncated block of the BTC is that the one-bit output of the quantize for each component within the block .Various strategies are planned throughout last twenty years for compression such BTC and Absolute Moment Block Truncation secret writing AMBTC [6].AMBTC preserves the upper mean and lower mean of the blocks and use this amount to quantize output. AMBTC provides higher image quality than compression mistreatment BTC.

In recent years, encrypted signal process has attracted sizable analysis interests [1]. The distinct Fourier rework and reconciling filtering are often enforced within the encrypted domain supported the homomorphism properties of a cryptosystem [2], [3], and a composite signal illustration methodology are often wont to cut back the scale of encrypted information and computation complexness [4]. In joint encoding and information activity, a vicinity of serious information of a visible signal is encrypted for content protection, and also the remaining information are wont to carry the extra message for copyright protection [5], [6]. With some buyer–seller protocols [7], [8], the fingerprint information are embedded into associate encrypted version of digital transmission to make sure that the vendor cannot understand vendee the customer the client's watermarked version whereas the buyer cannot get the first product.

This paper presents an ascendible secret writing of encrypted colour pictures and compression mistreatment block truncation secret writing. Ascendible secret writing of unencrypted pictures [12], [13] and for encrypted pictures [14] are been according. within the planned methodology, higher compression is achieved by mistreatment BTC and additionally the aggressor cannot get any applied mathematics info.BTC may be a recent technique used for compression of monochrome image information.BTC may be a renowned compression theme planned in 1979 for the colour scale pictures by Delp and Mitchell [15]. BTC is to perform moment conserving quantization for blocks of pixels so quality of image can stay acceptable and at a similar time the demand for space for storing can decrease.BTC has gained quality thanks to its sensible utility. At the receiver facet mistreatment cryptanalytic key and decompression the first content is reconstructed.

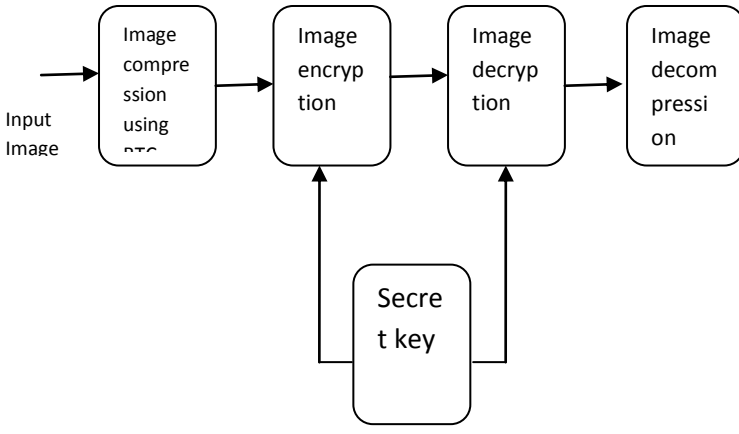


FIG 1: PROPOSED SYSTEM

A Novel Combination of Encryption and Compression for Privacy Protection by Using BTC

The diagram of the planned system is shown in Fig 1.In the planned system, the input colour pel worth is compressed by victimization Block Truncation cryptography.BTC may be a recent technique used for compression of monochrome image knowledge. The compressed pel worth is encrypted by generating a series of pseudorandom numbers that act as a secret key so transmitted. At the receiver aspect, coding is finished by victimization secret key and therefore the compressed pel worth is obtained. the first image is reconstructed by pressing victimization Block Truncation cryptography. The reconstructed image exhibits higher resolution, higher compression magnitude relation and improved PSNR.

A. compression

The input colour image is in uncompressed format which the pel values are inside [0,255] are portrayed in an exceedingly matrix format N1 X N2 wherever N1 is that the variety of rows and N2 because the variety of columns. The input image is compressed by victimization Block Truncation cryptography.BTC algorithmic rule involves the subsequent steps:-

Step 1:- 512 X 512 pel image is split into non overlapping rectangular regions. For the sake of simplicity the blocks we have a tendency to let the Blocks be sq. regions of size n x n wherever n is often four.

Step 2:- The mean x and variance σ values are calculated. These values amendment from block to dam.

Step 3:- the 2 values x and σ are termed as quantizes of BTC. Taking x because the threshold worth a 2 level bit plane is obtained by comparison every pel worth with the edge x. The binary block is denoted by .In the binary block the worth "1" is employed to represent a pel whose colour is larger than or adequate threshold x and "0" is to represent a pel whose colour is a smaller amount than threshold x. it\'s given as By this method every block is reduced to a small degree plane.

$$d_i(i,j) = \begin{cases} 1, & pixel\ value \geq \bar{x} \\ 0, & pixel\ value < \bar{x} \end{cases} \qquad (1)$$

The blocks of the BTC compressed image can all have an equivalent mean and variance of the first image? The thresholding method makes it doable to breed a pointy edge with hi-fi, taking advantage of the human visual system's capability to perform native spacial integration and mask errors. Therefore input colour image is compressed victimization BTC.

cover image

Compressed Immage

B. Image Encryption

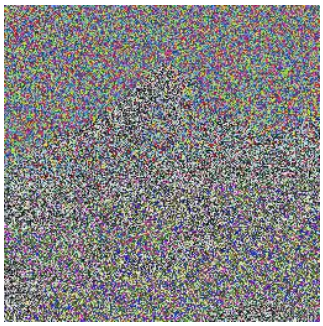
The compressed image bit quantity is 8N. Pseudo random variety is generated between the values [0,255] for the dimensions N1 X N2.The length of pseudorandom bit sequence is 8N.The pseudorandom number generator (PRNG) act as a secret key and shared between encoder and decoder. The encrypted image is obtained by adding each compressed image of size N1 X N2 and pseudo random variety of size N1 X N2 so

taking modulo 256 operations. It is givenasfoll0ws:

$$pp^{(t+1)}(i,j) = mod[oo(i,j) + e(i,j), 256] \quad (2)$$
$$1 \le i \le N_1, 1 \le j \le N_2$$

Where of (i, j) represents the compressed image values of pixels at positions (i, j), e (i, j) represents the pseudorandom numbers inside [0,255] generated by PRNG and represents the encrypted pel values. Fig. a pair of provides a clever image and its encrypted version. it\'s acknowledge that there is no chance polynomial time (PPT) algorithm to tell apart a pseudo random variety sequence and a random variety sequence hitherto. that\'s to mention image secret writing Image algorithm that we\'vet planned is semantically secure against any PPT opponent. The block is transmitted beside PRNG and values of Mean and variance.

Encrypted Immage



C. Image Reconstruction

Image coding at the receiver aspect, the encrypted image is decrypted with the assistance of secret key specifically PRNG. The formula used is

$$hh^{(T+1)}(i,j) = mod[pp^{(t+1)}(i,j) - e(i,j), 256] \quad (3)$$

Where is that the transmitted encrypted image and e (i, j) is that the secret key shared by the encoder and is that the compressed bit obtained by taking the distinction between the encrypted image and pseudo random variety disguised with modulo-256 operations. Here quantity worth "1" represents the pixels with colour worth is greater than or adequate threshold and quantity worth "0" represents the pixels with colour worth is a smaller amount than or adequate threshold. Image Decompression The original image is reconstructed by means that of Block Truncation cryptography. To reconstruct the first image, parts allotted as "0" are replaced with the value "a" and parts allotted as "1" are replaced with the worth "b".It is given as

$$x(i,j) = \begin{cases} a & hh^{(T+1)}(i,j) = 1 \\ b & hh^{(T+1)}(i,j) = 0 \end{cases}$$

(4)

The original image is reconstructed by exchange "1" with the values of "a" and "0" with values of "b". The "a" and "b" values are calculated by victimization this formula,

$$a = \bar{x} + \sqrt[\sigma]{p/q} \quad (5)$$

$$b = \bar{x} + \sqrt[\sigma]{\frac{q}{p}} \quad (6)$$

Where is mean, σ is variance, p is the number of 0's and letter is that the variety of 1's within the compressed bit plane severally. Therefore original image is reconstructed. Fig three shows the reconstructed image and decrypted version.

Decrypted Immage

DeCompressed Immage

Experimental results:

The human vision cannot distinguish so many colors (of the number of) generated by the use of 8 b for each color component. Therefore, we may extend the proposed method to obtain better compression ratios with reasonable SNR values by employing a simple technique [8] to reduce the representative bits of each color component from 8 to 5 b. Besides, the resulting 16-b bit maps still occupy over 35% of the output codes. In order to reduce redundancy in the bit map, we may employ the method of [9] to use 6-b indices to represent 64 predefined standard bit maps [9], which are designed according to the observation of the human visual system's sensitivity to edge and line patterns in small image blocks, and to represent the bit map of each image block by one of the 64 indices after matching the bit map with the 64 standard ones.

The Following shows the Compression results wirh different block sizes

Table 1: Compression results with different block sizes.

Block size	**2*2**	**3*3**	**4*4**	**5*5**	**6*6**	**7*7**	**8*8**
MSE	7.69	23.56	35.54	46.44	56.17	64.62	72.36
bpp	5.00	2.79	2.00	1.66	1.47	1.36	1.25

Table-2 The comparative SNR values and compression ratios of conventional btc, single-bit-map btc, and proposed algorithms cicmpbtc

	conventional BTC	single bit map BTC	CICMPBTC with 4×4 block size	CICMPBTC with 5×5 block size	*CICMPBTC** with 4×4 block size
Lena	32.85/4.0	29.03/6.0	31.55/7.03	30.95/9.27	29.14/12.29
pepper	32.46/4.0	27.43/6.0	30.93/6.60	30.12/8.80	28.54/11.47
house	39.93/4.0	31.16/6.0	36.77/7.75	33.32/9.81	33.47/13.67
jet	32.10/4.0	28.45/6.0	31.03/7.71	30.53/10.04	28.63/13.59
candy	39.60/4.0	31.04/6.0	37.52/8.20	33.87/10.51	33.20/14.57
balloon	34.93/4.0	28.32/6.0	33.53/7.36	32.26/9.55	31.16/12.92
average	**35.31/4.0**	**29.23/6.0**	**33.56/7.44**	**31.84/9.66**	**30.69/13.09**

SIMULATION RESULTS

FIG 2: ORIGINAL AIRPLANE AND ITS RECONSTRUCTED IMAGE

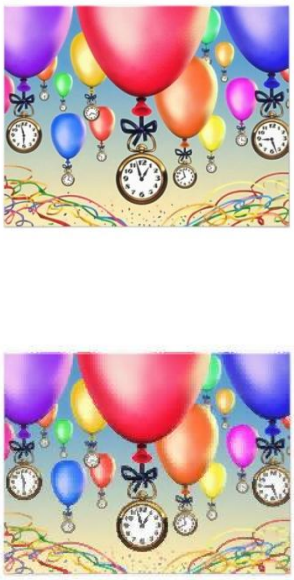


FIGURE 3: ORIGINAL BALLOON AND ITS RECONSTRUCTED IMAGE

CONCLUSION

The block truncation coding framework is dated so old that it is first applied in the year 1977 and although so many research works proposed on the video compression standard still BTC is favorable to apply in many image processing applications. The proposed work presents the novel approach to improve the compressed image consistency and the proposed block truncation coding framework main approach is to compress the images according to original gray level pixel value in high equipped manner. Addition of BTC pixel value along with the pseudo random number to obtain the encrypted image in an efficient way and then transmits the obtained encrypted image

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] J. R. Troncoso-Pastoriza and F. Perez Gonzalez, "Secure adaptive filtering," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 469–485, Jun. 2011.

[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, pp. 180–187, Mar. 2010.

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

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