ORIGINAL RESEARCH PAPER
Volume-7 | Issue-9 | September-2018 | PRINT ISSN No 2277 - 8179
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

# ENCRYPTED IMAGE RECONSTRUCTION BY DECODING THE BITSTREAM

Engineering

**Mohitha M Rao** Department of Telecommunication Engineering VKIT, Bengaluru

## ABSTRACT

In this paper, we propose a novel scheme of scalable coding for encrypted images. In the encryption phase, the original pixel values are masked by a modulo-256 addition with pseudorandom numbers that are derived from a secret key. After decomposing the encrypted data into a down-sampled sub image and several data sets with a multiple-resolution construction, an encoder quantizes the sub image and the hadamard coefficients of each data set to reduce the data amount. Then, the data of quantized sub image and coefficients are regarded as a set of bit streams. At the receiver side, while a sub image is decrypted to provide the rough information of the original content, the quantized coefficients can be used to reconstruct the detailed content with an iteratively updating procedure. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bit streams are received. The image quality is analyzed by comparing the decrypted image with the original image by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE).

## KEYWORDS

## I. INTRODUCTION

Idea of reversible data hiding in encrypted images (RDH-EI) originates from reversible data hiding (RDH) in plaintext images [1][6]. It is feasible in the applications like cloud storage and medical systems. In cloud storage, a content owner can encrypt an image to preserve his/her privacy, and upload the encrypted data onto cloud [3][4]. The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display [5] [7].

Watermarking has been widely used for proof of ownership and copyright protection; however, it has also been applied to applications such as broadcast monitoring, data integrity verification, and image indexing and labeling. Digital watermarking has

been investigated for the last several decades and is a mature field of research. However, current efforts try to improve its performance, as new requirements and challenges posed by new applications motivate the need for continued research in this area [10].

## II. LITERATURE REVIEW

In [1] an analytical strategy combining fractal geometry and grey-level co-occurrence matrix (GLCM) statistics was devised to investigate ultrastructural changes in oestrogen-insensitive SK-BR3 human breast cancer cells undergoing apoptosis in vitro. Apoptosis was induced and assessed by measuring conventional cellular parameters during the culture period. In many popular texture analysis methods, second or higher order statistics on the relation between pixel gray level values are stored in matrices. A high dimensional vector of predefined, non-adaptive features is then extracted from these matrices [2]. A generalized statistical texture analysis technique for characterizing and recognizing typical, diagnostically most important, vascular patterns relating to cervical lesions from colposcopic images[3]. Chromatin distribution reflects the organization of the DNA of a nucleus and contains important cellular diagnostic and prognostic information. Feulgen staining of breast tissue enables the chromatin distribution of the nucleus to be visualized in the form of texture[4]. A novel reversible data hiding algorithm, which can recover the original image without any distortion from the marked image after the hidden data have been extracted, is presented in this paper. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image [5].

## III. PROPOSED SYSTEM

In this work, we propose a novel scheme of scalable coding for encrypted images. Then decomposition of the original image into a downsampled subimage in three or four levels takes place. This process is called as downsampling. The input and downsampled images are compressed using Block Truncation Coding (BTC). The compressed images at different levels are encrypted using modulo-256 addition process and the encrypted images at different levels are obtained. In the encryption phase, the original pixel values are masked by a modulo-256 addition with pseudorandom numbers that are derived from asecret key. Then the modulo-256 subtraction process is done as an initialization stage of decryption process. Then the decompression is done to decompress the decrypted image. Finally the decrypted image is obtained at multiple levels. At the receiver side, while a subimage is decrypted to provide the rough information of the original content, the quantized coefficients can be used to reconstruct the detailed content with an iteratively updating procedure. The image quality of the decrypted image is analyzed by comparing with the input image by using statistical parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE).

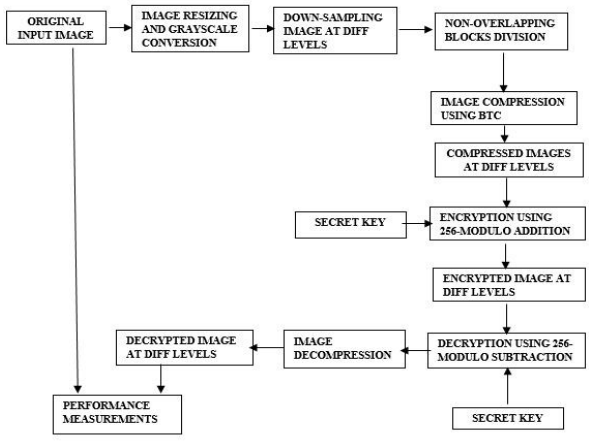



**Fig.1.block diagram of proposed system**

### A. Downsampling

First, the input image decomposes into a seriesof subimages. The subimage at the $(t+1)$thlevel$G^{(t+1)}$ is generated by down sampling thesubimage at the t thlevel as follows:

$$g^{(\tau+1)}(i,j)=\gamma^{(t)}(2i,2j),t=0,1, \ ,T-1 \qquad (1)$$

T is is the number of decomposition levels.
g(t) is the input grayscale image.

The decomposition of the original image into a downsampled subimage in three or four levels takes place. This process is called as downsampling.

### B. Image Compression

The images at different levels are compressed using Block Truncation Coding (BTC) and the compressed image for the different levels of downsampled images is obtained.

In this scheme, the image is divided into non overlapping blocks of pixels. For each block, threshold and reconstruction values are determined. The threshold is usually the mean of the pixel values in the block. Then a bitmap of the block is derived by replacing all pixels whose values are greater than or equal (less than) to the threshold by a 1 (0). Then for each segment (group of 1s and 0s) in the bitmap, the reconstruction value is determined. This is the average of the values of the corresponding pixels in the original block.

### C. Image Encryption

The image is in compressed format and that the pixel values are within [0, 255], and denote the numbers of rows and columns as N1 and N2 and the pixel number as ($N=N_1 \times N_2$). Therefore, the bit amount of the original image is 8N. The content owner generates a pseudorandom bit sequence with a length of 8N. Here, we assume the content owner and the decoder has the same pseudorandom number generator (PRNG) and a shared secret key used as the seed of the PRNG. Then, the content owner divides the pseudorandom bit sequence into N pieces, each of which containing 8 bits, and converts each piece as an integer number within [0, 255]. An encrypted image is produced by a one-by-one addition modulo 256 as follows:

$$g^{(0)}(i,j)=\mathrm{mod}\,[p(i,j)+e(i,j),256],\ 1<i<N_1,1<i<N_2$$

Where p (i, j) represents the gray values of pixels at positions (I, j), e (I, j) represents the pseudorandom numbers within [0, 255] generated by the PRNG, and $g^{(0)}(i,j)$ represents the encrypted pixel values. Clearly, the encrypted pixel values $g^{(0)}(I,j)$ are pseudorandom numbers since $e(i,j)$ values are pseudorandom numbers. It is well known that there is no probability polynomial time (PPT) algorithm to distinguish a pseudorandom number sequence and a random number sequence until now. Therefore, any PPT adversary cannot distinguish an encrypted pixel sequence and a random number sequence. That is to say, the image encryption algorithm that we have proposed is semantically secure against any PPT adversary.

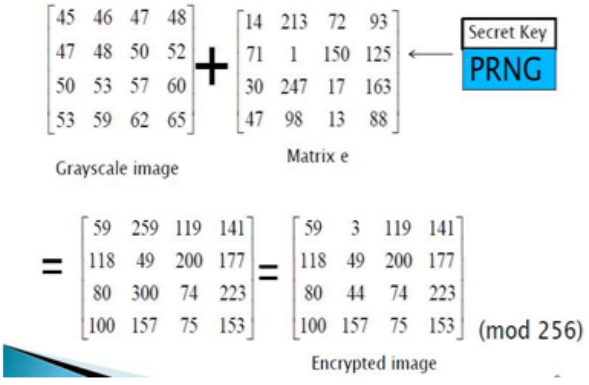


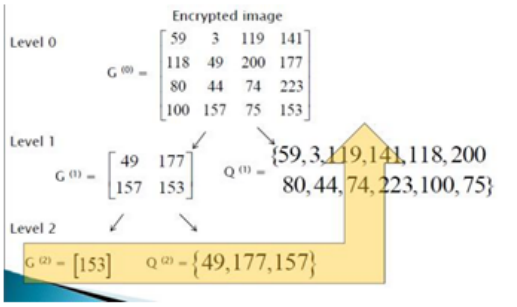

**Fig.2.Image Encryption**

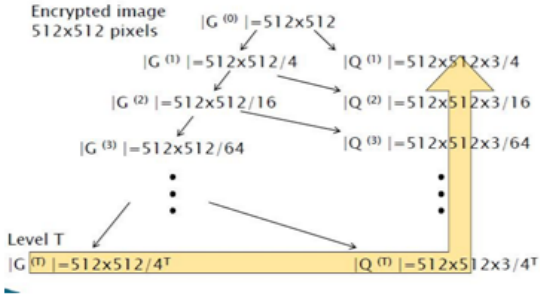
Although an encoder does not know the secret key and the original content, he can still compress the encrypted data as a set of bitstreams. The detailed encoding procedure is as follows. First, the encoder decomposes the encrypted image into a series of subimages and data sets with a multiple-resolution construction. The subimage at the (t +1)th level $G^{(t+1)}$ is generated by downsampling the subimage at the t th level as follows:

$$g^{(t+1)}(i,j)=g^{(t)}(2i,2j),\ t=0,1,\ ,T-1 \qquad (3)$$

Where $G^{(0)}$ just the encrypted image and T is is the number of decomposition levels. In addition, the encrypted pixels that belongs to G ( t +1) but do not belong to form data set $Q^{(t+1)}$ as follows:
$Q^{(t+1)}=\{g^{(t)}(i,j)\mathrm{mod}\,(i,2)=1\ \mathrm{or}\ \mathrm{mod}(j,2)=1\}$,

That means each $G^{(t)}$ is decomposed into $G^{(t+1)}$ and $Q^{(t+1)}$, and the data amount of $Q^{(t+1)}$ is three times of that of $G^{(t+1)}$. After the multiple-level decomposition, the encrypted image is reorganized as $G^{(T)}$, $Q^{(T)}$, $Q^{(T-1)}$, and $Q^{(t)}$




### D. Image Decryption and Decomposition

Then the modulo-256 subtraction process is done as an initialization stage of decryption process. Then the decompression is done to decompress the decrypted image. Finally the decrypted image is obtained at multiple levels. At the receiver side, while a subimage is decrypted to provide the rough information of the original content, the quantized coefficients can be used to reconstruct the detailed content with an iteratively updating procedure.

### E. Performance Evaluation

1. Experiments were made by comparing original input images and decrypted images.
2. The performance factor for the proposed algorithm is evaluated by PSNR and MSE PSNR-Peak Signal to Noise Ratio
3. MSE-Mean Squared Error

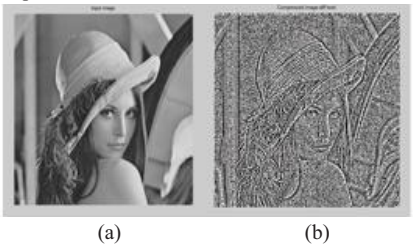
## IV. SOFTWARE SPECIFICATION

This paper proposes a novel nonrigid inter- t = 0,1 , T -1. subject multichannel image registration method which combines information from different modalities/channels to produce a unified joint registration. Multichannel images are created using co-registered multimodality images of the same subject to utilize information across modalities comprehensively. Contrary to the existing methods which combine the information at the image/intensity level, the proposed method uses feature-level information fusion method to spatio-adaptively combine the complementary information from different modalities that characterize different tissue types, through Gabor wavelets transformation and Independent Component Analysis (ICA), to produce a robust inter-subject registration.

MATLAB 8.3 Version R2014a. This MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

## V. EXPERIMENTAL RESULTS

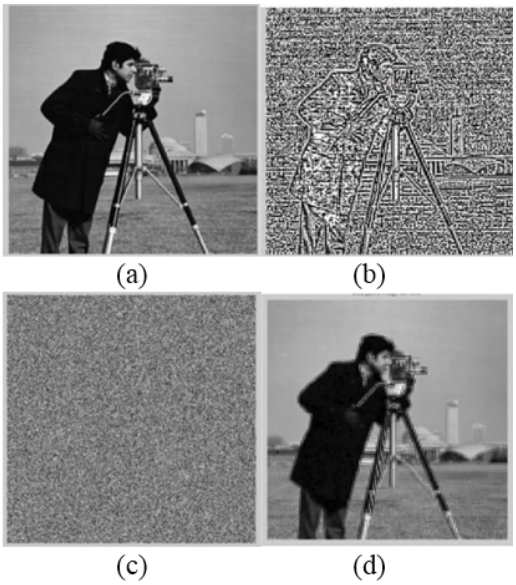
A group of experimental results are shown in



(a) (b)

(c) (d)

**Fig.3, in which (a) is the original images sized 512×512., (b) the compressed image, (c) the encrypted image, and,(d) the decrepted image**



(a) (b)

(c) (d)

**Fig.4, For cameraman image (a) is the original images sized 512×512. (b) the compressed image, (c) the encrypted image, and (d) the decrepted image**

The proposed method is compared with the separable RDH-EI method in [10]. Both methods embed message into three LSB-layers of the encrypted image. And the above results are of 512×512. Above mention methods are done to all different levels of images which will get after downsampling of original image size 512×512.

## VI.CONCLUSION AND FUTURE WORK

This work proposed an approach of combining and encrypting the secret key into the compressed input image using modulo 256 addition process. The encrypted image is obtained. At starting the image is decomposed into different levels. Then we need to decrypt/extract the original image from the decompressed encrypted image using modulo-256 subtraction. We demonstrate that the watermarks generated with the proposed algorithm are invisible and can be visible sometimes and the quality of adulterated image and the recovered image are improved. The proposed method is compared with the existing watermarking methods by using statistical parameters such as peak-signal-to-noise-ratio (PSNR), Mean Square Error (MSE) and Normalized Cross Correlation (NCC).

In the future work experiments with more images were carried out and tested by considering various phenomenon's such as exclusion of low resolution images and including the calculation of some more statistical parameters.

## REFERENCES


[1] W. Zhang, X. Hu, N. Yu, et al. "Recursive histogram modification: establishing equivalency between reversible data hiding and lossless data compression," IEEE Trans. on Image Processing, vol. 22, no. 7, pp. 2775-2785, Jul. 2013.

[2] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. on Circuits and Systems for Video Technology, vol.19, no.7, pp. 989-999, Jul. 2009.

[3] B.ou, X. Li, Y. Zhao, R. Ni, Y. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Trans. on Image Processing, vol. 22, no.12, pp. 5010-5021, Dec. 2013.

[4] Ioan-Catalin Dragoi, Dinu Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Trans. on Image Processing, vol. 23, no. 4, pp. 1779-1790, Apr. 2014.

[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362, Mar. 2006.

[6] 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.

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

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

[9] 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.

[10] 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.

[11] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in Proc. 16th EUSIPCO, Lausanne, Switzerland, Aug. 2008 .

[12] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Signal Process., vol. 19, no. 4,pp. 1097–1102, Apr. 2010.

[13] 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.

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

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

[16] A. Bilgin, P. J. Sementilli, F. Sheng, and M. W. Marcellin, "Scalable image coding using reversible integerwavelet transforms," IEEE Trans.Image Process., vol. 9, no. 11, pp. 1972–1977, Nov. 2000.

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