An Efficient Method for Secure Image Compression

Priya C, Ramya C, Agashthiya R V, Hema R, Mythily G, Preethi V P

Abstract: ***In this modern world with developing technology there exist demand for data and information transmission in a safe and rapid manner. There exists a need for compressing these images for storage and communication purposes. Image compression is to compress the image to produce good quality image and to reduce the storage space. This algorithm will provide efficient image compression without reducing the quality of image. To retain the secrecy of the image RSA encryption algorithm is used for encrypting and decrypting the image in a secured manner followed by SPIHT algorithm for decomposition and encoding. Here in this paper ETC and CTE methods are adopted and compared. The Lossless image Encryption then Compression (ETC) system yields high compression ratio, high PSNR when compared with CTE system. The performance parameters like Compression Ratio, PSNR (in dB), MSSIM are tabulated.***

Keywords: Image Compression, SPIHT, DWT, RSA, PSNR.

I. INTRODUCTION

In this digitized world with fast exchange of data in electronic way, data security is playing a major role in data storage and transmission. Due to the usage of images in industrial applications, it is important to protect the confidential data from third-party access. Digital image processing is necessary because day to day activities like satellite remote sensing, fax transmission, high definition television, multimedia are growing rapidly. There involved inherent complexity of JPEG images lower than that of grey level images. Hence a large amount of space is required for storing and time for transmission. The only solution to this problem is to compress the image so that the storage space and time taken for transmission will be reduced.

Image compression techniques

There are basically two methods for image compression:

1. Lossless Compression Techniques
2. Lossy Compression Techniques

In Lossless Compression technique, the result after compression, is identical to the original image.

In Lossy Compression technique, the compressed image is not identical to the original image and it also has reduction in image quality when compared to reconstructed image.

Set partitioning in hierarchical trees (SPIHT) is a wavelet based computational algorithm which is very fast among all the image compression techniques based transmission algorithm which offers high compression ratios, high image quality, fast execution time etc, A new hybrid compression method [2] to reduce the file size of JPEG coded images without any fidelity loss. It can reduce the storage cost for backup and hide the JPEG coded images for both personal and cloud applications. Encryption then Compression (ETC) system [4] using a combination of prediction error clustering and random permutation. Highly effective compression of the encrypted data has been obtained by a context-adaptive arithmetic coding approach. The theoretical and experimental results have high level of security. The paper [5] compares the generalization of SPIHT with Set Partition Coding System (SPACS). The SPIHT algorithm was firstly introduced by Said and W. A Pearlman [6] and using this algorithm, compression ratio high PSNR values are obtained for different types of grey-scale images are obtained. In [8], the author has used content-dependent compression noise level estimation and reduction framework through similar patch clustering and low-rank constraint. This method improves the quality of compressed images. In this paper section II relates proposed method.

II. PROPOSED METHOD

A. Block Diagram

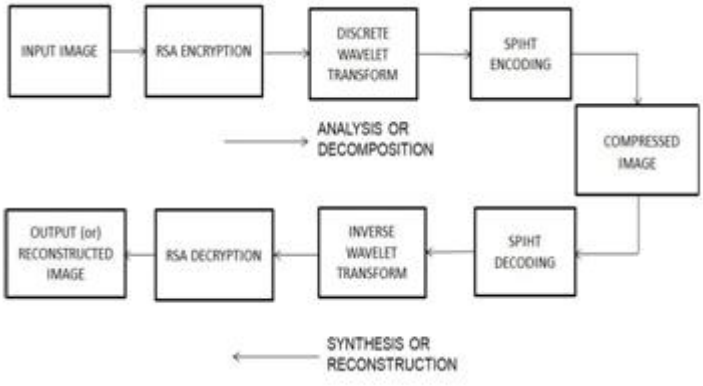


Fig. 2.1 Proposed block diagram of Encryption then Compression system

Revised Manuscript Received on April 15, 2019.

Priya C, Associate professor, Department of Electronics and Communication Engineering, Karpagam college of Engineering, Coimbatore

Ramya C, Associate professor, Department of Electronics and Communication Engineering, PSG College of Technology

Agashthiya R V, Student, Department of Electronics and Communication Engineering, Karpagam college of Engineering, Coimbatore

Hema R, Student, Department of Electronics and Communication Engineering, Karpagam college of Engineering, Coimbatore

Mythily G, Student, Department of Electronics and Communication Engineering, Karpagam college of Engineering, Coimbatore

Preethi V P, Student, Department of Electronics and Communication Engineering, Karpagam college of Engineering, Coimbatore

In the proposed method block diagram shown in Fig.2.1, the upper block represents analysis (or) decomposition while the lower block performs synthesis (or) reconstruction. Firstly, the image is encrypted using RSA algorithm and the encrypted image is passed to DWT block which outputs wavelet coefficients of the original image. Then these coefficients are passed to the SPIHT encoder which encodes the output and gives data in bit stream manner, thus providing compressed image. Now this compressed image is sent to the SPIHT decoder which decodes the bit stream and passes to the IDWT block to get the output (or) reconstructed image. This reconstructed image is then decrypted using RSA algorithm and then the original image is obtained.

B. RSA

To encrypt the original image RSA algorithm is used. which is an irregular cryptographic algorithm. RSA algorithm has two different keys, which can also be called as public key cryptography algorithm, because anyone of the keys can be allocated to any other. The supplementary key should remain private.

1. The RSA (Rivest-Shamir-Adelman) cryptosystem is the almost broadly-utilized public key cryptography algorithm world-wide. It is mainly used to encrypt a text or image lacking the requirement to interchange a secret key individually.
2. The RSA algorithm can be utilized for either public key encryption or digital signatures. Its safety is depends on the complications of separating large integers.

C. Image Encryption and Decryption

In the ever-enlarging growth of multimedia implementations, safety is a dominant problem in communication. Encryption is an usual method for image security process. This process translates the actual image to any-other image which cannot be interpret, The image privileges among users is maintained , which is also necessary where no-one can acquire to notice the content lacking a key for decryption. The technique of encoding basic messages into cipher messages is called **Encryption**, and the backward process of changing cipher text back to plain text is known as **Decryption**. Video and image encryption have implementation in different domains containing internet circulation, multimedia structures, medical imaging, Tele-care and radiotelegraph. In modern years, sufficient of color image encryption reaches have been preferred. Up-to now, different data encryption algorithms have been suggested and popularly utilized, such like AES, RSA, or IDEA virtually of which are used in text or binary data. It is hard to apply the same in multimedia and ineffective for color image encryption since intense correlation exists between pixels.

D. Discrete Wavelet Transform (DWT)

The initial step in image compression to exploit redundancy by means of wavelet transform. In fig 2.2, the sub-band decomposition of two-dimensional signal is done by using separable transforms which can be implemented using 1-D filters on the rows first and second on the columns.

The original image is decomposed using sub-band decomposition of N ×M image. Then each and every row is filtered and down-sampled to obtain two N × $\frac{M}{2}$ images. Similarly each column is filtered and sub-sampled to obtain 4 $\frac{N}{2}$ x $\frac{M}{2}$ images. Since the rows and columns are low-pass filtered and high-pass filtered respectively, the first sub-image is obtained (LL image); Similarly by low-pass filtering the rows and high-pass filtering the columns, second sub-image is obtained (LH image);In the same way by high-pass filtering the rows and low-pass filtering the columns, the third sub-image is obtained(HL image); and the fourth sub-image is obtained by high-pass filtering the rows and columns (HH image). The second decomposition level is shown in Fig.2.3 (b). Each and every sub-image obtained in this manner can be filtered and sub-sampled to get four more sub-images resulting in a total of 10 sub-images as shown in Fig 2.3(c).

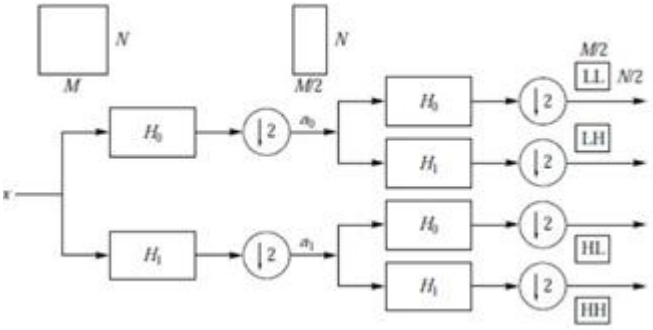


Fig. 2.2 Sub-band decomposition

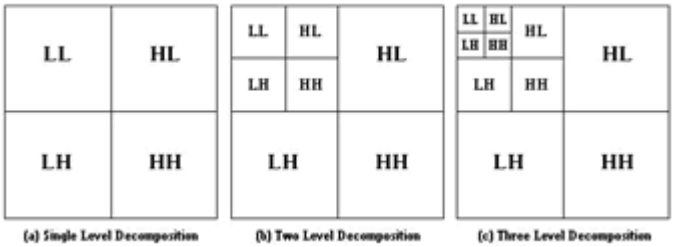


Fig. 2.3 Three levels of decomposition

E. SPIHT Algorithm

SPIHT (Set partitioning in hierarchical trees) algorithm is used for compressing the original image, it utilizes the intrinsic resemblance over the sub-bands in a wavelet decomposition of an image. This algorithm first codes the wavelet transform coefficients first, and transfer the bits so that a progressively pure duplication of the actual image can be obtained growingly.

Flow Chart of SPIHT

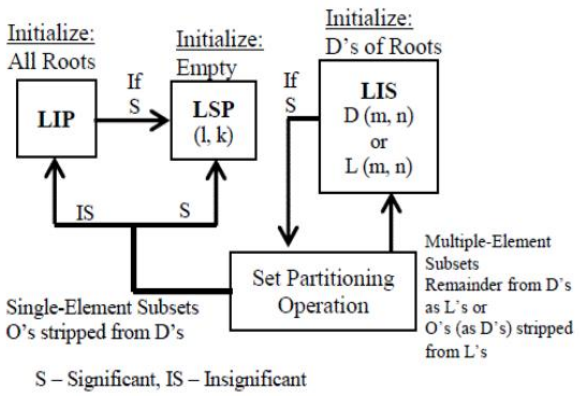


Fig. 2.4 Flow chart of SPIHT

SPIHT has three lists of wavelet coefficients

1. LIP: It contains the individual coefficients which has magnitudes smaller than the thresholds.
2. LSP: It involves the list of pixels having magnitudes larger than the threshold value.
3. LIS: It has the list of wavelet coefficients which is defined by tree structures and it has magnitudes smaller than the threshold.

where LIP = List of Insignificant Pixels,
LSP = List of Significant Pixels,
LIS = List of Insignificant Sets.

Steps involved in SPHIT algorithm:

STEP 1: The threshold value is initialized, the value in trees are allocated to LSP and LIP is initialized to an empty set in tree.

STEP 2: After initialization, coefficient of current bit in the sorting pass is encoded.

To check whether the wavelet coefficients in LIP are important coefficients:

1) If the coefficients are important then the output is "1" and depends upon the sign bit whether it is positive or negative sign bits and it is represented by "1" and "0" respectively then the coefficients are removed from LIP and added to the end of LSP.

2) In case the coefficients are unimportant, then it is assigned to a direct output of "0".

STEP 3: In the refinement pass, the contents of LSP from the previous pass are examined.

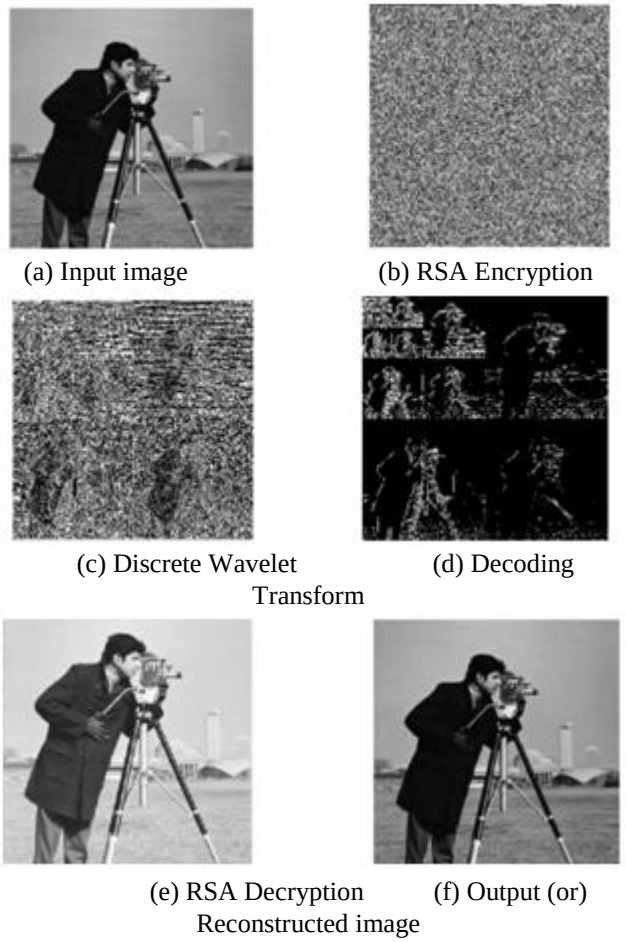
STEP 4: Then the threshold value will be updated (back to step 2).

F. Image Compression

By reducing the un-relatedness of an image is the basic focus of image compression process and to deliver provision for saving and transferring the data in an essential aspect. The beginning step in this process is to transform the image from the description of their spatial field into offprint case of the description by the work of few previously well-known translations and then encodes the translated values (i.e. coefficients). This process permits enormous compression of data as differentiated to the prophetic processes, however at the value of the enormous computational requirements. In this paper section III relates proposed method.

III. RESULTS AND DISCUSSION

The Encryption Then Compression algorithm has been executed in MATLAB r2013a and it is verified or tested for 15 set of jpeg images of size 256X256. Fig 3.1(a) the original image is (b) encrypted using RSA algorithm then undergoes (c) wavelet decomposition by initialising the decomposition level as 3 then processed decomposed image is (d) decoded then the image is (e) decrypted to obtain the (f) original (or) reconstructed image.



(a) Input image (b) RSA Encryption

(c) Discrete Wavelet Transform (d) Decoding

(e) RSA Decryption (f) Output (or) Reconstructed image

Fig. 3.1 Simulation outputs obtained using ETC Algorithm

(a)Input image (b) Output (or) Reconstructed image

Fig. 3.2 Simulation outputs obtained using CTE Algorithm

The Compression Then Encryption algorithm has been executed in MATLAB r2013a and it is verified or tested for various jpeg images of size 256X256. Fig 3.2(a) original image undergoes wavelet decomposition by initializing the decomposition level as 3 then processed decomposed image is encrypted using RSA algorithm to prevent the image from malicious attacks. Then the cipher image is then decrypted when the private key is used by the owner, the image is then decrypted to obtain the (b) original (or) reconstructed image. In this paper section IV relates performance parameters.

IV. PERFORMANCE PARAMETERS

A. Compression Ratio

Compression Ratio (CR) is the ratio between reconstructed file size and input file size. For any algorithm compression Ratio (CR) should be higher in order to achieve better compression.

$$\text{Compression Ratio} = \frac{Size\ after\ compression}{Size\ before\ compression} \quad ---1$$

B. Peak Signal to Noise Ratio (PSNR)

PSNR is defined as the ratio between the maximum signal value (MAXf) to the square root of MSE. PSNR value should be less than 40.

$$PSNR = 20\log_{10}\left(\frac{MAXf}{\sqrt{MSE}}\right)(dB) \quad ---2$$

C. Mean Square Error

Mean Square Error is given by,

$$MSE = \frac{1}{MxN}\sum_{0}^{m-1}\sum_{0}^{n-1}||f(i,j) - g(i,j)||^2 \quad ---3$$

Where f = matrix data of the Input image
g = matrix data of degraded image.

D. Mean Structural Similarity (MSSIM)

It is used to measure the resemblance in quality between two images (i.e.,with original image and compressed image).The SSIM metric is calculated on various windows of an image is given by

$$MSSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad ---4$$

Table. 4.1 Comparison of Compression Ratio (CR) for ETC and CTE System

IMAGE NO	COMPRESSION RATIO (ETC)	COMPRESSION RATIO (CTE)
1	10.00305:1	8.00293:1
2	9.00293:1	8.00305:1
3	11.00076:1	8.00293:1
4	9.00231:1	8.00305:1
5	10.00305:1	8.00293:1
6	12.00678:1	8.00293:1
7	10.00273:1	8.00293:1
8	11.00234:1	8.00076:1
9	12.00112:1	8.00305:1
10	13.07683:1	8.00293:1

The above table 4.1 shows the comparison of Compression ratio for ETC and CTE system. For Test image 10, the Compression ratio is 13.07683:1 by using ETC algorithm and by using CTE algorithm CR is 8.00293:1.Hence an ETC system has high CR compared to that of CTE system.

Table. 4.2 Comparison of PSNR Value (DB) for ETC and CTE System

IMAGE NO	PSNR(dB) (ETC)	PSNR(dB) (CTE)
1	28.98	26.12
2	31.95	29.01
3	33.62	31.10
4	36.15	34.45
5	39.63	34.72
6	34.83	30.30
7	31.29	28.43
8	33.49	30.21
9	34.07	30.12
10	31.61	29.09

The above table 4.2 shows the comparison of PSNR (dB) for ETC and CTE system. For Test image 5, the PSNR value is 39.63 by using ETC algorithm and by using CTE algorithm PSNR value is 34.72. Hence an ETC system has high PSNR value compared to that of CTE system.

Table. 4.3 Comparison of MSSIM Value (DB) for ETC and CTE System

IMAGE NO	MSSIM (ETC)	MSSIM (CTE)
1	0.90	0.86
2	0.85	0.80
3	0.91	0.87
4	0.91	0.85
5	0.96	0.92
6	0.91	0.88
7	0.89	0.84
8	0.97	0.94
9	0.85	0.82
10	0.87	0.84

The above table 4.3 shows the comparison of MSSIM for ETC and CTE system. For Test image 3, the MSSIM value is 0.91 by using ETC algorithm and by using CTE algorithm MSSIM value is 0.85. Hence an ETC system has high MSSIM value compared to that of CTE system. In this paper section V relates conclusion.

V. CONCLUSION

This paper compares lossless Encryption then Compression (ETC) technique which uses image encryption (i.e., RSA algorithm) used to encrypt the image by ensuring privacy in transmission without any malicious attacks and image compression (i.e., SPIHT Compression) for compressing the encrypted image with that of Compression then Encryption (CTE) technique .By using ETC technique ,the compression ratio is high compared to CTE technique .The performance evaluation factors are measured using Compression ratio, PSNR and MSSIM.

The proposed ETC system has greater compression ratio, fast execution time and good image quality than CTE system.

REFERENCES

1. Asma Banu. S and A. Sreenivas Murthy, "Implementation and Comparison of a Secure Lossless Image Encryption-then-Compression Algorithms", International Journal of Engineering Research & Technology (IJERT), vol. 4, Issue 9, September 2015.
2. Hao Wu, Xiaoyan Sun, Jingyu Yang, Wenjun Zeng and Feng Wu, "Lossless Compression of JPEG Coded Photo Collections", IEEE Transactions on image processing, vol. 25, no. 6, June 2016.
3. Hyun Kim, Albert No and Hyuk-Jae Lee, "SPIHT Algorithm with Adaptive Selection of Compression Ratio Depending on DWT Coefficients", IEEE Transactions on Multimedia-2018.
4. Jiantao Zhou, Xianming Liu, Oscar C. Au, and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on Information Forensics And Security, vol. 9, no. 1, January 2014.
5. Qiufu Li, Derong Chen, Wei Jiang, Bingtai Liu, and Jiulu Gong, "Generalization of SPIHT: Set Partition Coding System", IEEE Transactions on Image Processing, vol. 25, no. 2, February 2016.
6. Said and W.A Pearlman, "A new, Fast and Efficient image Codec Based on set Partitioned in hierarchical trees," IEEE Transaction circuits & systems for video Technology, vol. 6, pp. 243-250 June 1996.
7. Wei Liu, Wenjun Zeng, Lina Dong and Qiuming YaoQun Ding, "Efficient Compression of Encrypted Grayscale Images", IEEE Transactions on Image Processing, vol. 19, no. 4, April 2010.
8. Xinfeng Zhang, Weisi Lin, Ruiqin Xiong, Xianming Liu, Siwei Ma and Wen Gao, "Low-Rank Decomposition-Based Restoration of Compressed Images via Adaptive Noise Estimation", IEEE Transactions on Image processing, vol. 25, no. 9,Sep 2016.
9. C.Ramya,S.Subha Rani," Video denoising without motion estimation using Kmeans clustering", Journal of scientific and industrial research,vol.70,pp251-255,April 2011.
10. C.Ramya, Dr.S.Subha Rani," Rain Removal in Image Sequence Using Sparse Coding", Communications in Computer and Information Science, springer, pp. 361–370, Nov.2012.
11. C.Ramya, Dr.S.Subha Rani 2014, 'A Sparse based rain removal algorithm for image sequences', International Journal of Robotics and Automation, vol. 29, pp. 1-7. Journal ISSN: 0826-8185
12. C.Ramya, C.Priya & Dr.S.Subha Rani, 'Rain streaks removal in images based on sparse representation,' International Journal of Applied Engineering Research, Vol. 9 No.26 (2014) pp. 8935-8938.
13. C.Ramya ,C.Priya,'A Robust Image Enhancement using Fuzzy based Filtering Method',International journal of Pure and Applied Mathematics,Vol.118,No.20(2018),pp.403-409.
14. C.Priya,C.Ramya'An Efficient region based lossless compression for Medical Images',International journal of Pure and Applied Mathematics,Vol.118,No.20(2018),pp.539-546.
15. C.Priya,C.Ramya'Medical Image compression based on Fuzzy Segmentation',International journal of Pure and Applied Mathematics,Vol.118,No.20(2018),pp.603-610.
16. C.Priya,C.Ramya'A Robut Encryption Then Compression method for medical images',International journal of Pure and Applied Mathematics,Vol.118,No.20(2018),pp.539-546.
17. Priya C, Kesavamurthy T, Wavelet Based Biomedical Image Compression using SVD and Interpolation Techniques, Journal of Pure And Applied Microbiology, 9: 227-233,(2015).
18. Priya C, Kesavamurthy T & Uma Priya M, An Efficient Lossless Medical Image compression using Hybrid Algorithm, Advanced Materials Research,984: 1276-1281 (2014).
19. PriyaC, Kesavamurthy T & Umapriya M, 'Sparse Approximation Using M - Term Pursuit For Bio – Medical Images', International Journal of Applied Engineering Research, 9(26): 9137-9141 (2014).
20. C. Ramya & C. Priya, FPGA Implementation for Contrast Enhancement in Images Using Xilinx System Generator,(IJSR) , 5(11):901-905(2016).
21. Priya C & Kesavamurthy T, Medical Image Compression Using Wavelet Transform,International J. of Innovative Research in Science, Engineering and Technology, vol. 2, no. 6, pp.2543-2546 (2013).