International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 4: April 2016, pp 11-14. www.aetsjournal.com ISSN (Online) : 2394-6237

An Efficient Compression and Decompression of Henon Chaotic System Based Encryption

K.P.Sathyaprakash, M.H.Anandbabu , M.Sathyanarayanan

Abstract— In this paper, a new lossless image compression method is proposed. For continuous and discrete time cases, wavelet transform and wavelet packet transform has emerged as popular techniques. This work proposes a novel scheme for lossless compression of an encrypted image with flexible compression ratio. Henon Chaotic image encryption system is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from DWT transform based SPIHT method. In this process we get the clear bit rate and compression ratio values. Required bit rate of encoding is small. Since quantized compresses the original image into a set of indices in the codebook, we can save a lot of storage space and channel bandwidth. The other advantage is that quantization has a simple hardware structure for providing a fast decoding procedure. Percentage of compression indicates by how much the size of the image has been reduced from its original size and it is given by, Compression ratio(CR) = (Original file size/ compressed file size) x 8.

Index Terms—Lossless compression, Encrypted image, Henon Chaotic image encryption, DWT, SPIHT

I. INTRODUCTION

The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder integrating decompression and decryption functions will be used to reconstruct the original data. The original binary image is encrypted by adding a pseudorandom string, and the encrypted data are compressed by finding the syndromes with respect to low-density parity-check (LDPC) channel code. In the latter one, the original data is encrypted by adding an Gaussian sequence, and the encrypted data are quantized and compressed as the syndromes of trellis code. The compression of encrypted data for both memory less sources and sources with hidden Markov correlation using LDPC codes is also studied. By employing LDPC codes into various bit-planes and exploiting the spatial and cross-plane correlation among pixels, a few methods for lossless compression of encrypted gray and color images are introduced. The encrypted image is decomposed in a progressive manner, and the most significant bits in high levels are compressed using rate-compatible punctured turbo codes. The decoder can observe a lowresolution version of the image, study local statistics based on it, and use the statistics to obtain the content in high levels. Furthermore, by developing statistical models for source data and extending these models to video, presents some algorithms for a compressive sensing technique is introduced to achieve lossy compression of encrypted image data, and a basis pursuit algorithm is appropriately modified to enable joint decompression and decryption. After the encryption we using wavelet based on SPIHT compression and reconstruction. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. Major advantage of this algorithm it has a simple structure. Required bit rate of encoding is small. Since quantized compresses the original image into a set of indices in the codebook, we can save a lot of storage space and channel bandwidth. The other advantage is that quantization has a simple hardware structure for providing a fast decoding procedure. The distinct advantage of simultaneous lossless compression and strong encryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. Image compression forms the backbone for several applications such as storage of images in a database, picture archiving, TV, facsimile transmission and video conferencing. Compression of images involves taking advantage of the redundancy in the data present within an image. In order to achieve useful compression various algorithms were developed in the past. A compression algorithm has a corresponding decompression algorithm that, given the compressed file, reproduces the

K.P.Sathyaprakash , Assistant Professor-Department of Electronics and Communication Engineering, Syed Ammal Engineering.College , (Email : 1sathya1988@gmail.com)
M.H.Anandbabu ,Assistant Professor-Department of Computer Science and Engineering, Syed Ammal Engineering.College (Email : 2mhanand007@gmail.com)
M.Sathyanarayanan ,Assistant Professor-Department of Information Technology Ganapathy Chettiar College of Engineering and Technology Ramanathapuram, Tamilnadu, India (Email :3sathyakcgit@gmail.com)

original file. There have been many types of compression algorithms developed. These algorithms fall into two broad types, Loss less algorithms and Lossy algorithms. A lossless algorithm reproduces the original exactly. Whereas, a lossy algorithm, as its name implies, loses some data. Data loss may be unacceptable in many applications. For example, text compression must be lossless because a very small difference can result in statements with totally different meanings. There are also many situations where loss may be either Unnoticeable or acceptable. But various applications require accurate retrieval of image, where in one such application is medical processing. The image quality is measured in terms of PSNR and MSE:

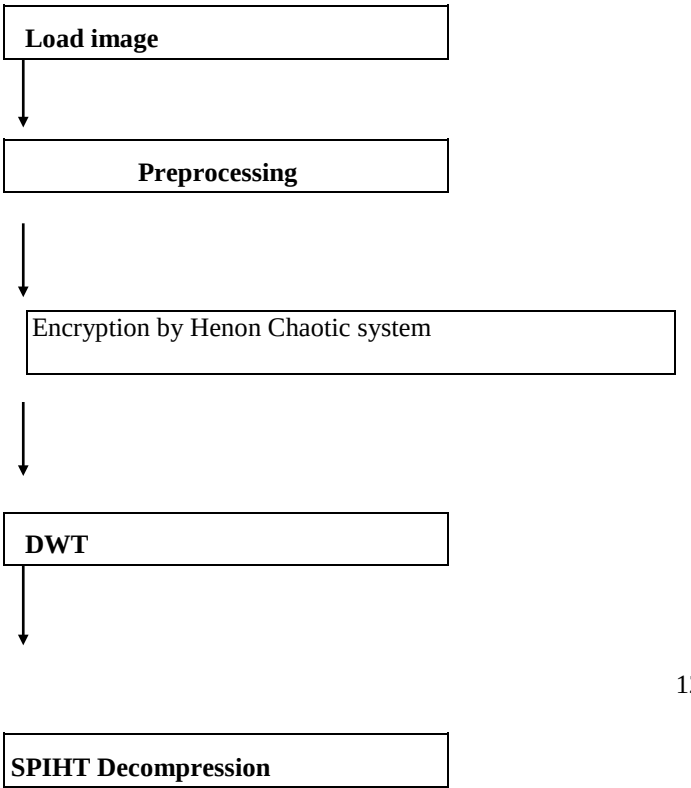
$$MSE = \frac{1}{N.M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left[\left|f(i,j)-f'(i,j)\right|^2\right]$$

where, f (i, j) is the original image data and f ' (i, j) is the compressed image value. Another quantitative measure is the peak signal-to-noise ratio (PSNR), based on the root mean square error of the reconstructed image. For good quality image, PSNR value should be as high as possible and MSE value should be as low as possible.

II. PROPOSED SYSTEM

We propose a novel system for lossy compression of encrypted image with flexible compression ratio, which is made up of image encryption, tailor-made compression and decompression phases. After encryption of the image, we using the Discrete wavelet transform based SPIHT encoding and decoding method. Here the Compression format will give the bit stream values. It is more secure because which converts the image information into bit values so there is no way to identify the original data information applications.

III. MODULE DIAGRAM



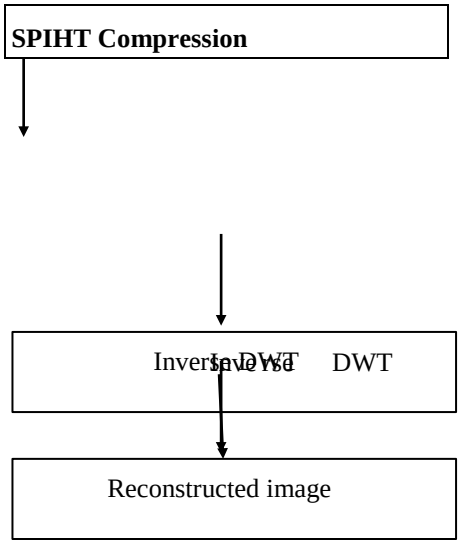


Fig.1. Sequence of operation

IV. MODULES DESCRIPTION

A. LOAD IMAGE:

[X, map] = imread(...)

A = imread(filename, *fmt*) reads a grayscale or color image from the file specified by the string filename. If the file is not in the current folder, or in a folder on the MATLAB path, specify the full pathname.

B. PREPROCESSING:

In signal processing, it is often desirable to be able to perform some kind of noise reduction on an image or signal. The median filter is a nonlinear digital filtering technique, often used to remove noise. Such noise reduction is a typical pre-processing step to improve the results of later processing (for example, edge detection on an image). Median filtering is very widely used in digital image processing because, under certain conditions, it preserves edges while removing noise. This approach is due to and is an approximation of the median filter. If we apply a two dimensional filter in the spatial domain we can accelerate its performance if it is separable. This is a common approach where instead of applying a two dimensional, we can apply two one dimensional flters.

C. ENCRYPTION BY HENON CHAOTIC SYSTEM

At first the image fusion is completed between the original image and the key image. Then pixel values of fusion image are encrypted by Henon Chaotic system. Graphics fusion technique can be used in image fusion. According to the image pixel, image fusion can be completed between same size images. Image fusion can be described as following: E(i, j) = {w * [K(i, j) – O(i, j)]} + O(i, j). Where 'w' is a parameter, K(i, j) is the pixel values of key image, O(i, j) is the pixel values of original image and E(i, j) is the pixel values of

fusion image. In our scheme, Henon chaotic system is adopted to encrypt the fusion image

Step 1: Henon chaotic system is converted into one dimensional chaotic map which is defined as $X_{i+2} = 1 - aX^2_{i+1} + b_{xi..}$ The parameter a , b and initial values x0 and x1 may represent the key.

Step 2: Set encryption key for the fusion image, including structural parameters a, b and initial values x0 and x1.After image fusion, we adopt henon chaotic map to change the pixel values of fusion image.

D.DWT

- The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression.
- Because of their inherent multiresolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important
- Wavelet transform decomposes a signal into a set of basis functions.
- These basis functions are called wavelets
- Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilations and shifting.
- The wavelet transform is computed separately for different segments of the timedomain signal at different frequencies.
- Multi-resolution analysis analyzes the signal at different frequencies giving different resolutions

E. DWT BASED SPIHTCOMPRESSION

In the compression section, best suitable algorithm is SPIHT (Set Partitioning In Hierarchical Trees) is a wavelet based algorithm. Normally the SPIHT algorithm is decomposed using hierarchical wavelet decomposition to form many sub bands. The wavelet transformation is decomposed depending on the frequency, where they are sub sampled by horizontal and vertical channels using sub band filters. Here the reconstruction is done by applying using the inverse discrete wavelet transform. SPIHT is computationally very fast among the image compression algorithms known today. This method saves lots of bits during transmission compared with the Embedded zero tree wavelet transforms. The structure below shows the decomposition of an image into various sub bands namely LL, LH, HL, and HH. The input image is thus first encrypted using stream cipher and then compressed using SPIHT algorithm. In SPIHT, the partitioning decisions are binary decisions that are transmitted to the decoder. Providing a significance map encoding, which is efficient than the EZW algorithm.

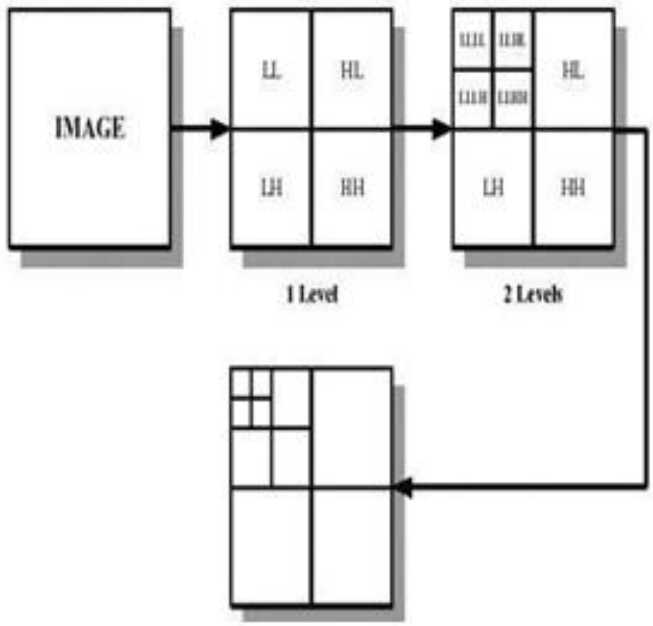


Fig.2. Discrete Wavelet Transform

The SPIHT compression steps are given as follows.

- Apply DWT on the original fingerprint image.
- Make all the coefficients of this DWT positive.
- Apply SPIHT on the DWT obtained after step 2 ignoring the sign bit and compressed bit stream is obtained

F. SPIHT DECOMPRESSION

1. Apply inverse SPIHT on the bit stream recovered after step 2, again ignoring the sign bit since it has not been encoded. 2. Change the sign of all those pixels whose sign had been reversed during compression.3.Apply IDWT on this transform to get back the original image

G. IDWT

Given the coefficient sequence $s(M)$ for some $M<J$ and all the difference sequences $d(k)$, $k=M,...,J-1$, one

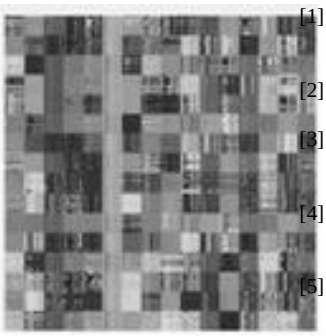
$$s_n^{(k+1)} := \sum_{k=-N}^{N} a_k s_{2n-k}^{(k)} + \sum_{k=-N}^{N} b_k d_{2n-k}^{(k)}$$

c

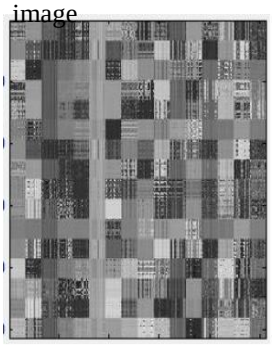
computes recursively for $k=J-1,J-2,...,M$ and all . In the Z-transform notation

V.EXPERIMENTAL RESULT

(a) Original image



(b) Encrypted image



(c) Compressed image

(d) Reconstructed image

Fig.3. Implemented outputs

The method is experimented with an image in matlab. Using matlab we can get simulation result. The image is first undergoes encryption using pseudorandom permutation and then it is compressed using DWT based SPIHTmethod Here we take the original image as 'lena.jpg'. The compression ratio is found to increase as the number of compression steps increases.

VI. CONCLUSION

This work proposed a novel idea for compressing and encrypted image and designed a practical made up of image encryption, lossless compression, and iterative reconstruction. The original image is encrypted by Henon Chaotic system and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. When having the compressed data, an iterative updating procedure is used to retrieve the values of coefficients by exploiting spatial correlation in natural image, leading to a reconstruction of original principal content. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In general, the higher the compression ratio and the smoother the original image gives better quality of the reconstructed image.

REFERENCES

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pt. 2, pp. 2992 – 3006, Oct. 2004.

[2] R. G. Gallager, "Low Density Parity Check Codes," Ph.D. dissertation, Mass. Inst. Technol., Cambridge, MA, 1963.

[3] 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.

[4] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey-level and color images," in Proc.16th Eur. Signal Processing Conf. (EUSIPCO 2008), Lausanne, Switzerland, Aug. 2008.

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

[6] 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.

[7] Kumar and A. Makur, "Lossy compression of encrypted imageby compressing sensing technique," in Proc. IEEE Region 10 Conf. (TENCON 2009), 2009, pp. 1–6.

[8] 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.

[9] 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.

[10] J.C. Yenand J.-I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realization," Proc. Inst. Elect. Eng., Vis. Image Signal Process., vol. 147, no. 2, pp. 167–175, 2000.

[11] N. Bourbakis and C. Alexopoulos, "Picture data encryption using SCAN patterns," Pattern Recognit., vol. 25, no. 6, pp. 567–581, 1992.

[12] David A. Clunie "Lossless Compression of Grayscale Medical Images-Traditional and State of the Art.

[13] S. Singh, V. Kumar. H. K. Verma ," DWT-DCT hybrid scheme for medical image compression", Journal of Medical Engineering & Technology, Vol 31, Issue 2 , pp.109 – 122, March 2007.

[14] David A Koff, MD; Harry Shulman, MD, FRCPC, FACR "An Overview of Digital Compression of Medical Images: Can We Use Lossy Image Compression in Radiology?" Canadian Association of Radiologists Journal, Vol 57 , pp. 211-217, October 2006.

[15] Se-Kee Kil, Jong-Shill Lee, Dong-Fan Shen, Je-Goon Ryu, Eung-Hyuk Lee, HongKi Min, Seung-Hong Hong."Lossless Medical Image Compression using Redundancy Analysis", IJCSNS International Journal of Computer Science and Network Security, Vol.6 No.1A, pp. 5057, January 2006.