A Joint Image Compression–Encryption Algorithm Based on SPIHT Coding and 3D Chaotic Map

Ramkrishna Paira

Abstract In this paper, the author has proposed secure and fast joint image compression–encryption algorithm using discrete wavelet transform (DWT), set partitioning in hierarchical trees (SPIHT) algorithm, and 3D chaotic map. The proposed approach is divided into three phases for partial encryption, full encryption, and permutation in order to elaborate the cryptographic properties. Compression part is carried out via secure SPIHT. This inclusion of security in SPIHT has no reflex on compression properties. Intensive experiments are performed to justify and validate the proposed approach.

Keywords Image compression · Image encryption · SPIHT · DWT · Chaotic map

1 Introduction

In this era of Internet and smartphones, an enormous amount of data, especially images are produced. Thus, it has become a challenge for us to store and circulate image securely over the Internet. Hence, the two important factors are considered.

(1) Image compression—It means to reduce the size of an image without degrading the image quality. This allows us to store images in limited disk or memory space. It is also useful in transmitting the image in low bandwidth. For instance, normally the pictures of size 15 MB from the smartphones are taken with an Internet speed of 64 k bit/s. It would take one hour to transfer but on applying image compression, it can be done in few minutes. The basic steps for image compression include transformation, followed by quantization and entropy coding (Fig. 1).

The most frequently used transformations in digital image processing are discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet

R. Paira (✉)
Department of Computer Engineering, Smt. S. R. Patel Engineering College,
Unjha 384170, Gujarat, India
e-mail: pairaram@gmail.com

J. K. Mandal and D. Bhattacharya (eds.), *Emerging Technology in Modelling and Graphics*, Advances in Intelligent Systems and Computing 937,
https://doi.org/10.1007/978-981-13-7403-6_34

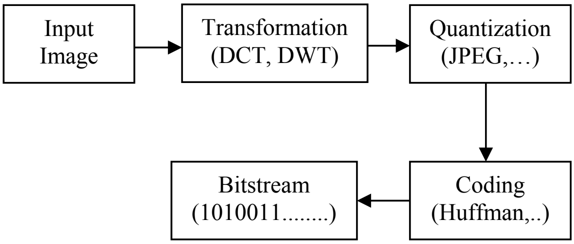


Fig. 1 Image compression process

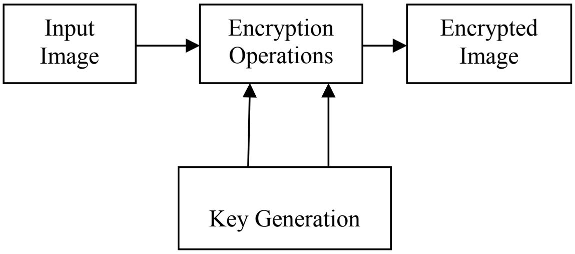


Fig. 2 Image encryption process

transform (DWT). DCT is basic in many lossy image compression methods. The image is divided into 8 × 8 blocks and then, DCT is performed. The motive of DCT is to assemble energy in terms of a sum of sinusoids with different frequencies and amplitudes. However, image compression algorithms based on DWT are highly efficient and diminish blocking artifacts [1]. In DWT, images are divided into sub-bands (LL, HL, LH, HH) by using wavelet filters [2]. The classic compression standard, i.e., JPEG 2000 is based on DWT while old JPEG is based on DCT. After transformation, quantization is applied. There are several quantization methods like embedded zerotree of wavelet (EZW), SPIHT, etc. The SPIHT coder is an efficient and fast algorithm for image compression [3]. In the final step of entropy coding, the output of the SPIHT algorithm is combined with Arithmetic, Huffman Coding, etc.

(2) Image encryption—The process using encryption algorithms to convert an image into a secret image so that unauthorized user can’t access it (Fig. 2).

From security point of view, few suggested the direct transmission of an encrypted image without compression, but it requires a lot of bandwidth. Other proposed algorithms which compress the image in the first step and then encrypt the image in the second step, but it needs more time to execute. However, very few proposed the encryption of image before the compression. While some suggested novel methods have a joint image compression and encryption process.

2 Study on DWT and SPIHT

(1) *Discrete wavelet transform (DWT)*: The wavelet transform is practically used in image and signal processing. The Joint Photographic Experts Group (JPEG) has unleashed its new image compression standard, i.e., JPEG 2000, which is based upon DWT. This transform break signals into set of basis functions, called wavelets and which are obtained from mother wavelets [4]. DWT has various transforms such as Haar wavelet, Daubechies wavelets, Biorthogonal wavelets, and Meyer wavelet. In this process, image is analyzed by passing through filter banks at each decomposition stage. A 2D transform takes place by performing two isolated 1D transforms. In first stage, image is filtered along x-dimension, then sub-image along y-dimension. Finally, the input image is splitted into four sub-bands [1, 5]. The four sub-bands, i.e., LL, LH, HL, and HH images which contain all the information in the original image. The LL sub-band has the significant information called approximation sub-band of the original image. The LH, HL, HH has vertical, horizontal, and diagonal information of the original image, respectively (Fig. 3).

(2) *Set partitioning in hierarchical trees (SPIHT)*: It is the improved version of embedded zerotree wavelet (EZW) algorithm [6]. It is wavelet based on image encoding technique [7]. It is suitable for both lossy as well as lossless image compression [3].

For each coordinate value, there is a significance test function to valuate the significance. Let, t be a coordinate on which significance has to be checked and n is the integer value, then the significance test function is $S_n(t)$.

```
If($\max(i, j)\{|c_{i,j}|\} \geq 2^n$)
    $S_n(t) = 1$
else
    $S_n(t) = 0$
```

where $c_{i,j}$ defines the coefficient value at location (i, j). If $S_n(t) = 1$, then coordinate t is said to be significant at the threshold value $T = 2^n$ otherwise, insignificant [3].

Fig. 3 Two-level decomposition

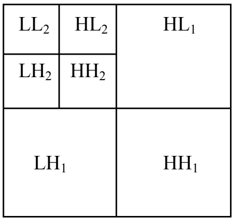
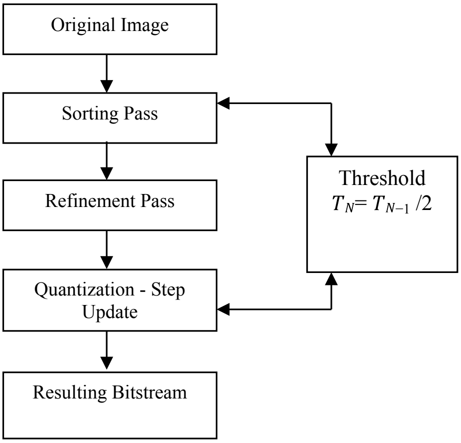


Fig. 4 Flowchart of SPIHT



This algorithm has three lists to store information namely, list of insignificant pixels (LIP), list of significant pixels (LSP), list of insignificant sets (LIS). All the entries in the list are identified by the pixel value (i, j) (Fig. 4).
Algorithm:

1. Input image.
2. Perform transformation using DWT.
3. Initialization of LSP, LIP, LIS using significant test where threshold value $\mathrm{T} = 2^{\mathrm{n}}$ and n is given by:

$$\mathrm{n} = \lfloor \log_2\big(\max(\mathrm{i},\mathrm{j})\{|\mathrm{c}_{\mathrm{i,j}}|\}\big)\rfloor.$$

4. Output n sent this output value to the decoder.
5. Output μn and sign of each μn pixel coordinates the such that $2^{\mathrm{n}} \leqq |c_{\eta}(\mathrm{k})| \leqq 2^{\mathrm{n+1}}$ (Sorting Pass).
6. Output the *nth* most significant bit of all the coefficients with $|c_{i,j}| \geqq 2^{\mathrm{n+1}}$ (i.e., those coordinates were transmitted in the past go), in a similar request used to send the pixel coordinates (Refinement Pass).
7. $n = n\text{-}1$ (Quantization-step Update), and go to (Step 2).

3 Proposed Algorithm

The approach, “Joint image compression & encryption based on SPIHT algorithm & 3D chaotic map” is grounded on wavelet transformation, SPIHT algorithm, bitwise encryption and permutation of the output bitstream using chaotic secure system. It

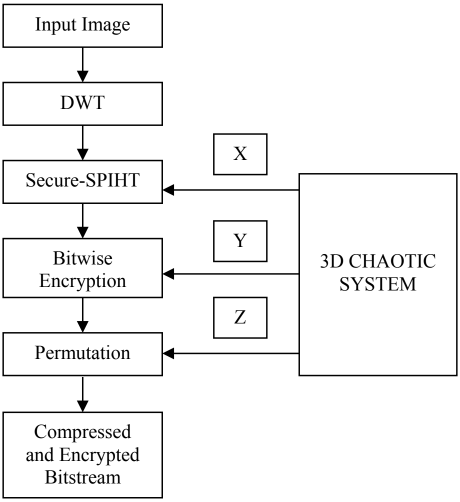


Fig. 5 Flowchart of proposed algorithm

is a fast algorithm for an image compression and encryption process. The proposed method has good PSNR ratio which is required for proper reconstruction of the image (Fig. 5).
Proposed Algorithm:

1. Input image.
2. Apply DWT on the input image.
3. Perform secure SPIHT for joint image compression and partial encryption process.
4. Bitwise encryption on output bitstream of secure SPIHT encoding.
5. Permutation.
6. Compressed and encrypted output.

(1) *Chaotic System*: The simplest way of chaos generation is defined by the logistic map. The equation for the logistic map is given by:

$$X_{n+1} = \mu X_n(1 - X_n)$$

$0 < X_n < 1$ and $\mu = 4$ are the basic conditions to make the chaotic equation [8]. Hongjuan Liu gives us the 2D logistic map employing quadratic coupling for security enhancing and it is upgraded to 3D version, which is given by the following equations:

$$X_{n+1} = \gamma X_n(1 - X_n) + \beta Y_{n^2} X_n + \alpha Z_{n^3}$$
$$Y_{n+1} = \gamma Y_n(1 - Y_n) + \beta Z_{n^2} Y_n + \alpha X_{n^3}$$
$$Z_{n+1} = \gamma Z_n(1 - Z_n) + \beta X_{n^2} Z_n + \alpha Y_{n^3}$$

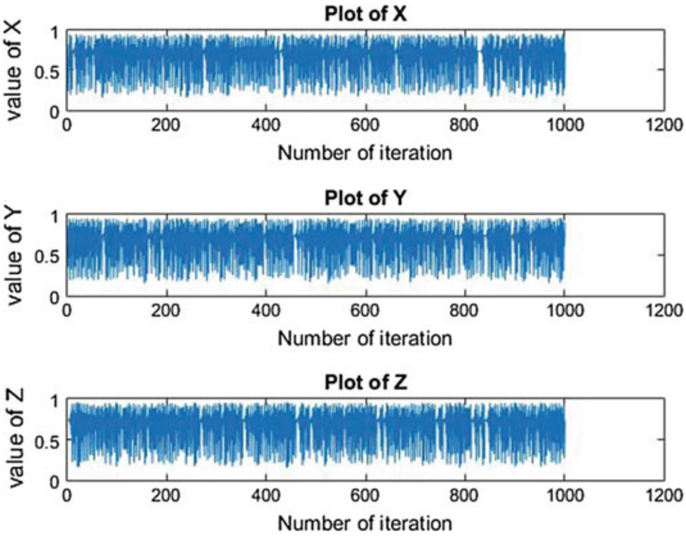


Fig. 6 3D chaotic sequence

where $3.53 < \gamma < 3.81$, $0 < \beta < 0.022$, and $0 < \alpha < 0.015$. The initial input values of the X, Y, and Z are lying between zero and one. The secure chaotic system is hypersensitive to the initial conditions. The two very close initial values will never follow the same path [9].

Figure 6 shows the generated chaotic sequence for the initial values $X(1) = 0.235$, $Y(1) = 0.350$, $Z(1) = 0.735$, $\alpha(1) = 0.0125$, $\beta(1) = 0.0157$, $\gamma\ (1) = 3.7700$ [10].

(2) *Secure SPIHT*: This process encapsulated the encryption in the SPIHT algorithm to enhance the security. The data is not only compressed but also encrypted, which will enhance the cryptographic property of the bitstream. For each coefficient, there is a need to check if its value is greater than threshold (T) value, where $T = 2^n$ and n is obtained by

$$\lfloor n = \log_2\left(\max(i, j)\{|c_{i,j}|\}\right)\rfloor.$$

In this case, the output is 1 else the output is 0. These output bits are encrypted using the key value [11].

Modified LIP sorting pass process is shown below.

```
For each entry in the LIP
    If (current coefficient ≥ threshold( T ) )
        Output = bitxor( 1, key )
            If ( sign( current coefficient ) > 0)
                Output = bitxor( 1, key)
            Else
                Output = bitxor( 0,key)
    Else
        Output = bitxor( 0, key )
End
```

Encryption of LIP sorting pass at encoder end.

```
For bitstream at decoder
    If ( bitxor ( bitstream, key ) == 1)
        Update the coefficient with regards sign and
        magnitude
            If ( bitxor (bitstream, key ) == 0)
                Coefficient ≥ threshold( T )
            Else
                Coefficient ≤ threshold( T )
    Else
        Insignificant coefficient
End
```

Decryption of LIP sorting pass at decoder end.

(3) *Bitwise Encryption*: This process encrypts the output bitstream of secure SPIHT algorithm. Encryption process is based on the key value. The number of key values depends on the number of compressed code stream generated from the secure SPIHT. In this process, the initial four bitstreams are ignored as they carry the important information to the decoder, which includes *T* value, number of rows, columns, and levels [6] (Fig. 7).

(4) *Permutation*: For the last stage of security enhancement, this step permutates the encrypted output to give new location based on the chaotic sequence [12] (Fig. 8).

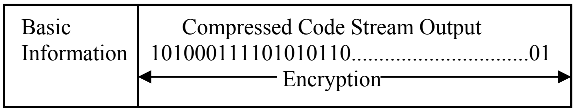


Fig. 7 Bitwise encryption of code stream

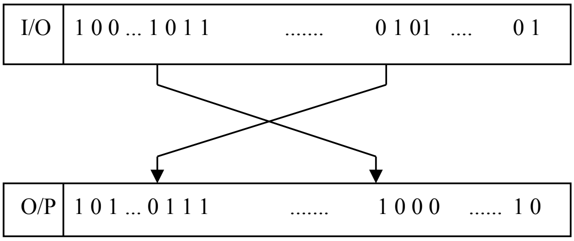


Fig. 8 Permutation of code stream

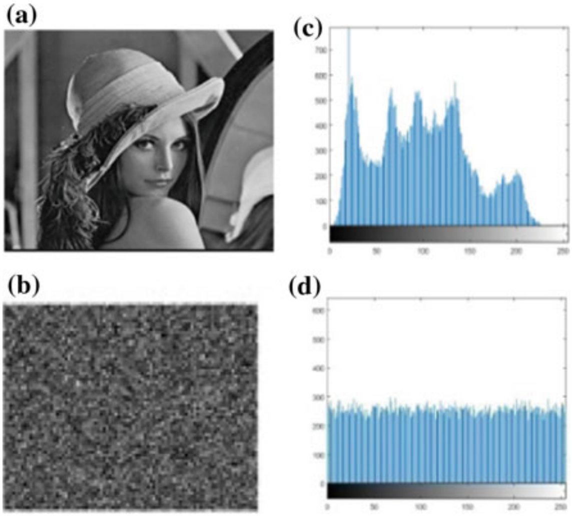


Fig. 9 **a** Lena image, **b** Encrypted image, **c** Histogram of (**a**), **d** Histogram of (**b**)

4 Experimental Results

(1) *Histogram*:

All Fig. 9 experiments have been performed on MATLAB. For ensuring encryption quality, there is a need to perform histogram test of the input and encrypted image.

(2) *Peak Signal-to-Noise Ratio* (*PSNR*): It is given by the formula mentioned below

$$\mathrm{PSNR} = 20\log_{10}\frac{255}{\sqrt{\mathrm{MSE}}}$$

where MSE is given by $\mathrm{MSE} = \frac{1}{\mathrm{LL}}\sum_{i=1}^{L}\sum_{j=1}^{L}\left(m_{ij} - n_{ij}\right)^2$, m and n are output and input image coordinates, respectively at location (i, j).

Table 1 shows the PSNR value for the proper reconstructed image at the decoder end. For the quality of image to be better, PSNR value should be high.

Table 1 PSNR table

Image	PSNR
Lena	32.61
Cameraman	28.15
Airplane	32.16
Rice	31.87
Moon	31.21

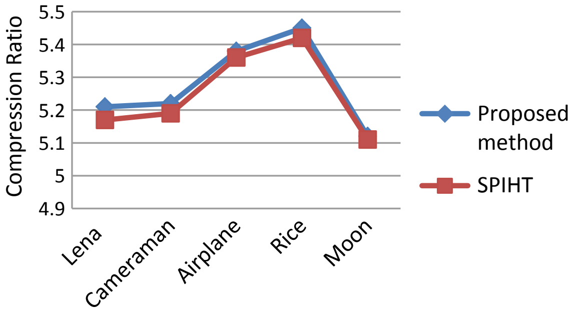


Fig. 10 Compression ratio chart

Table 2 Key sensitivity test table

Image	PNSR (1 bit modification)
Lena	1.15
Cameraman	2.17
Airplane	1.28
Rice	1.38
Moon	2.16

(3) *Compression Ratio*: By definition, it is the ratio of uncompressed image to the compressed image size (Fig. 10).
The above chart shows that the compression ratio is not affected by the encryption process.

(4) *Key Sensitivity Test*: An algorithm is said to be good if it is key sensitive. A minute modification in the key value should make a huge difference. In this, one bit in the key value is modified, which leads to the failure of decryption process at the decoder end (Table 2).

5 Conclusion

This paper presented secure and fast joint image compression and encryption algorithm which is based on DWT, secure SPIHT, and 3D chaotic system. This chaos values are very secure and sensitive in nature, which provides excellent encryption process, while compression part is carried out by basic SPIHT. By employing various evaluation parameters, security tests and performance tests are performed to validate the goals.

References

1. M. Vetterli, J. Kovacevic, *Wavelets and Subband Coding* (Prentice Hall, Englewood Cliffs, NJ, 1995)
2. M. Zhang, X. Tong, Joint image encryption and compression scheme based on IWT and SPIHT. Opt. Lasers Eng. (2017)
3. A. Said, W.A. Pearlman, A new fast and efficient image codec based on set partitioning in hierarchical trees (1996)
4. A. Alice Blessie, J. Nalini, S.C. Ramesh, Image compression using wavelet transform based on the lifting scheme and its implementation. IJCSI Int. J. Comput. Sci. Issues **8**(1) (2011)
5. *Wavelet Methods*, Data Compression (2007)
6. M. Hamdi, R. Rhouma, S. Belghith, A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map. Signal Process. (2017)
7. R. Sudhakar, R. Karthiga, S. Jayaraman, Image compression using coding of wavelet coefficients–A survey. ICGSTGVIP J.
8. S. Al-Maadeed, A new chaos-based image-encryption and compression algorithm. J. Electr. Comput. Eng. (2012)
9. Md. Billal Hossain, Md. Toufikur Rahman, A.B.M. Saadmaan Rahman, S. Islam, A new approach of image encryption using 3D chaotic map to enhance security of multimedia component, in *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*
10. P.H. Kharat, S.S. Shriramwar, A secured transmission of data using 3D chaotic map encryption and data hiding technique, in *2015 International Conference on Industrial Instrumentation and Control (ICIC)* (2015)
11. T. Xiang, J. Qu, C. Yu, X. Fu, Degradative encryption: an efficient way to protect SPIHT compressed images. Opt. Commun. (2012)
12. L. Bao, Y. Zhou, C.L. Philip Chen, H. Liu, A new chaotic system for image encryption,in *2012 International Conference on System Science and Engineering (ICSSE)* (2012)