Indian Journal of Science and Technology, *Vol 8(12), DOI: 10.17485/ijst/2015/v8i12/62433, June 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Increased Security in Image Cryptography using Wavelet Transforms

M. B. Parthasarathy[1*] and B. Srinivasan[2]

[1]School of computing, SASTRA University, Tamil Nadu - 613401, India; bharathy0391@gmail.com
[2]SASTRA University, Tamil Nadu - 613401, India; srinivasan@core.sastra.edu

Abstract

Objective: The main objective of the paper is to enhance the security of the images using three different wavelet while transmission of the images. **Method:** In the Existing system, images are directly encrypted using HAAR wavelet which provides frequency sub bands and they are exchanged in single level deliberately. Hence, it is prone to guess the wavelet and can be applied to detect the process to retrieve the original image. In our proposed work, three different wavelets are used to encrypt the image along with a password. The main advantage of the method is to enhance the security level in encryption process. **Result:** A password will be assigned to the image a key will be generated through the password using a key generation algorithm. Key is used to select the wavelet mechanism and two levels of frequency sub band exchange process will be carried out to ensure the security of the image. The originality of the image is compared through their PSNR Values. There will be no loss of data in the process is an additional advantage of our proposed work. **Conclusion:** Thus the original image is retrieved in the process and the method is highly secure for transmitting the image. Only intended users can retrieve the original image by using password.

Keywords: Image Cryptography, Image Encryption, Image Encoding with Key, Image Security, Wavelet Image Encryption

1. Introduction

The main aim of cryptography is hiding the data or message from the intruders. In medical and military fields, images are transferred in encrypted forms due to security reasons. It will be sent only to the intended users, hence intruders cannot view the image. Hence Images are encrypted with several methods, and it will be shared with the receivers. Receiver will reverse the same process and get the original image. But in the above process, it is possible that intruders may access the encryption technology, hence unauthorized may access the image. Hence, a new technology is implemented in the proposed system. A secret key will be generated using a password which assigned during encryption, based on the key, image will be encrypted. Haar, Daubechies and Symlet are the three wavelets are used for encryption process. Any of the above wavelet will be chosen for encryption based on the key generated at the initial step. Secret password and the encrypted image will be shared with the intended receiver. Hence the receiver can decrypt the image using same key. After applying the key, same wavelet which is used for encryption will be selected and applied to the encrypted image. The whole process will be reversed and original image will be retrieved.

Different schemes are proposed for image encryption, a video steganography method using Haar Image Wavelet (IWT) and Least Significant Bits (LSB) to hide the data[1]. Key generation based encryption used to encrypt the image using keys from the text[2]. Secret images are encrypted using AES algorithm, Non-Uniform Block Adaptive Segmentation on Image (NUBASI) and randomized secret sharing algorithm to hide the message in an

*Author for correspondence

image[3]. Bit-plane slicing and rotation of pixels are used to increase the security in image encryption[4]. New technology to improve the security using Message Digest, IDEA and GOST algorithms during message transmissions[5]. A lossless method which results compression and encoding of binary as well as gray-scale images[6]. A shuffling algorithm, which gets input data and using key generated by the algorithm, image will be encrypted[7]. A chaos based image encoding algorithm, where the pixels of the image will be repositioned and the relation between original and encoded image will be collapsed[8]. A cipher technology, where an external key will be used to perform chaotic operation to remove the relationship between original image and encoded image[9]. An encryption scheme, in which Discrete Cosine Transform (DCT) applied to the intended image, lowest frequency of the particular image will be used a key for encryption[10]. Hence, data loss will be lesser when compared with other encryption schemes. Similarly, Discrete Cosine Transform (DCT) applied to the targeted image and used highest frequency co-efficient to encrypt the image[11]. A digital signature is created using Bose–Chaudhuri Hochquenghem (BCH) code and included in the encoded version of an image to encrypt the image[12] . Properties of Spectral and Haar wavelets are investigated and some features are extracted to show the distribution of coefficients[13]. Multilevel 2-D wavelets are used to decompose the image and are compressed to produce the encrypted image[14]. Haar Wavelets are used to decompose the image and positions of pixels are rearranged to ensure the security of image[15]. Hence, the human visibility will remain in the encoded image. Some researchers are using image based transform to encrypt the images. The most common method for encrypting the image is 2-D Haar wavelet transform. 2-D wavelet transform will be applied to the image, resulted frequency sub bands will be shuffled and repositioned in different ways. On the contrast whole process will be reversed for retrieving the original image. In this paper, Wavelet transform is chosen for encryption process. Discrete Wavelet transform provides more information and higher flexibility for processing the image. Data of images will be retrieved exactly rather than other block based transformations. HAAR, DAUBECHIES and SYMLET are the three wavelets chosen in this paper for encryption.

1.1 Haar Wavelet

HAAR Wavelet was introduced by Alfred Haar in 1909. Haar wavelet produces square shaped functions based on the wavelet selected. Based on the number of inputs given in the list of 2^n values, Haar wavelet combines the input values, saves the differences and passes the sums. At last, it results 2^n-1 difference value and a single sum value. HAAR wavelet transform can be denoted as $A=XBX^T$ where B is an m×m matrix, X is the m×m Haar transform matrix and A is the resultant matrix.

1.2 Daubechies Wavelet and Symlet Wavelet

Daubechies wavelets are similar to the Haar wavelet, Daubechies wavelets are represented as 'dbn', Where n is the order of wavele, n = [1,2,3,4,5,6,7,8,9]. 'db1' wavelets are similar to haar wavelet. It was invented by the mathematician Ingrid Daubechies. Daubechies proposed another wavelet also named as Symlet, it will generate all symmetrical wavelets. 'sym1' wavelet produces the results similar to haar wavelet.

1.3 Frequency Sub Bands in Wavelet Transforms

If the above wavelets are applied to an image, image sub bands will be produced as XX, XY, YX and YY format. XX is the low-low frequency sub band, XY is the low-high frequency sub band, YX is the high-low frequency sub band and YY is the high-high frequency sub band. Figure 1 shows the frequency sub bands generated through wavelet transforms.

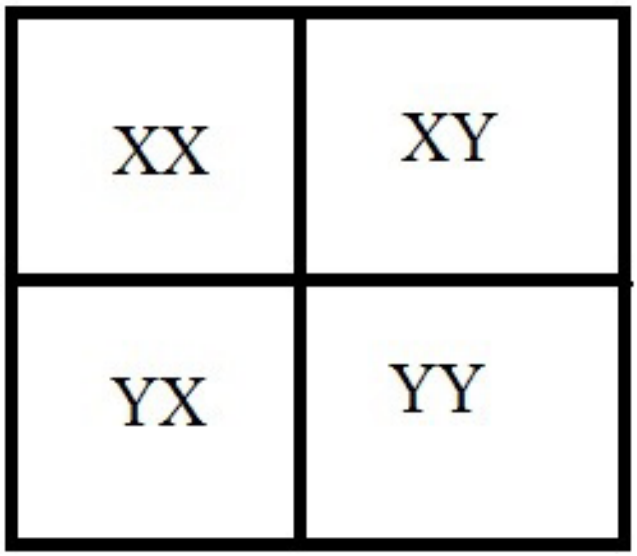

Figure 1. Frequency Sub bands after applying wavelet transform to an image.

2. Proposed Work

2.1 Encryption Algorithm

At the first step, Password will be created for encrypting the image. Text or special characters of the password will be used by the key generating algorithm a secret key will be generated. This generated key will not even known to the sender. Based on the key, encryption process will be carried out. At first, wavelet transform will be chosen from the wavelet choosing function in the algorithm. Possible wavelets are Haar, Daubechies and Symelet. First level of wavelets produces four sub band matrix for the given image. XX -> low-low frequency sub band, XY-> low-high frequency sub band, YX-> high-low frequency sub band, YY-> high-high frequency sub band. Next step is decreasing the values of low-low frequency sub band by XX(i,j)->XX(i,j)/(m×n), where m and n are the dimensions of the low-low frequency sub band. Next step will be reversing the signs of XY, YX and YY sub bands, to inverse the magnitude of sinusoidal co-efficient. It will make brighter side to darker and darker side to brighter. Next two steps are the important process of this paper. Positions of the sub bands will be exchanged through three patterns, 1. Exchanging XX with YX and YX with YY. 2. Exchanging XX with XY and YX with YY. 3. Exchanging XX with YY and XY with YX. Based on the key, any one of the pattern will be chosen for exchanging the positions of sub bands. This process will be carried in two steps, at first step, a pattern will be applied and in the second step, another pattern will be chosen for exchanging the positions of sub bands. Figure 2 explains the process of

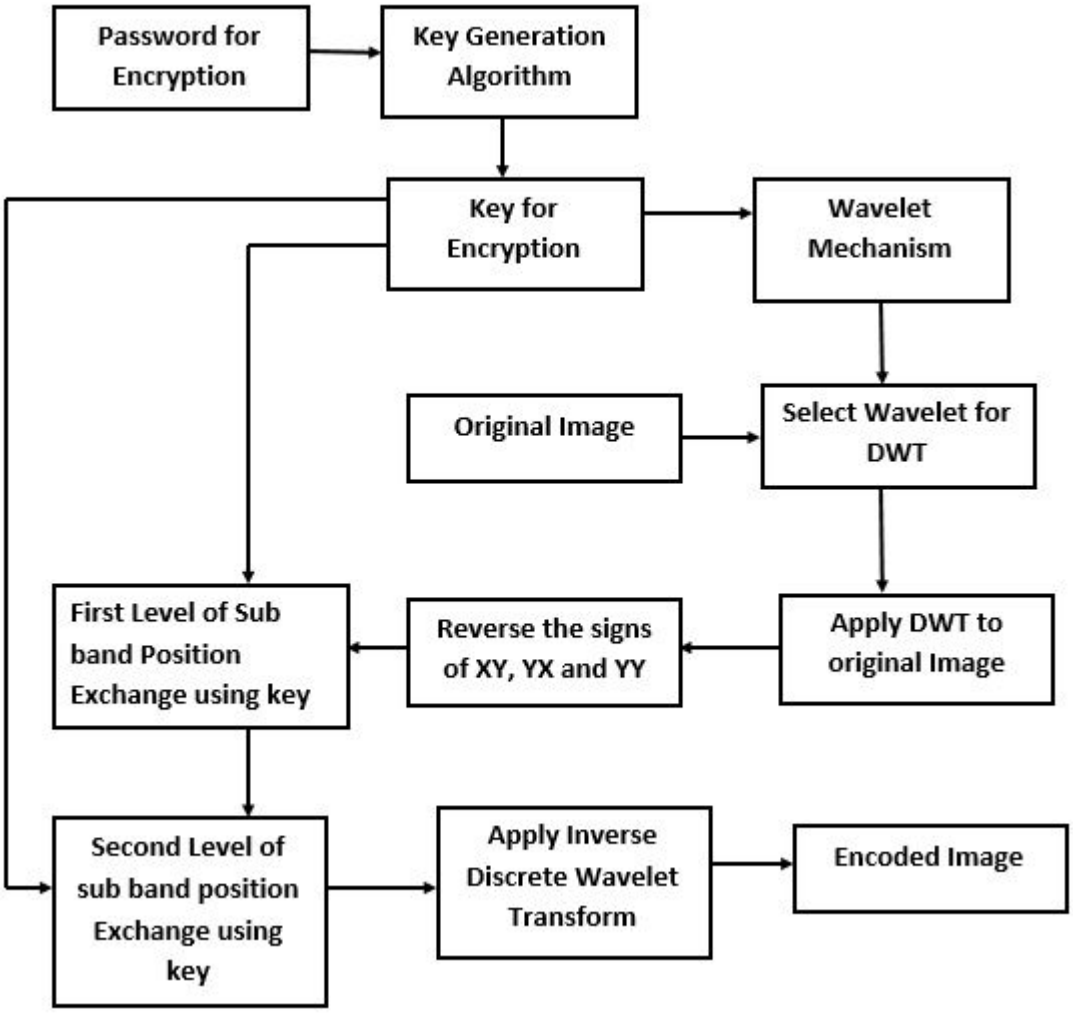

Figure 2. Encryption Process.

choosing wavelet mechanism and exchange of frequency sub bands. Now the Inverse Discrete Wavelet Transform (DWT) will be applied to produce the encrypted image. Thus the encrypted image and password will be shared only with the intended receiver.

2.2 Key Generation Algorithm

For generating the key, Password given by the sender will be passed to the algorithm initially.

STEP 1: [key_alg(pwd)]

Number of elements in the password will be calculated and based on the numbers, modulo will be taken to all characters, thus the number produced will be assigned as key.

STEP 2: [WI FLSE SLSE]

Three values of the key will be chosen and they are assigned to different tasks such as Wavelet Identifier, First Level Sub band Exchanger and Second Level Sub band Exchanger.

STEP 3: WI will be passed to the wavelet selection mechanism, based on the value derived from the key, a wavelet will be chosen.

STEP 4: FLSE is the key value, which will be used for selecting the pattern for exchanging the sub band matrix positions.

STEP 5: SLSE is the key value, which will be used for selecting second level of exchanging patterns in the already exchanged sub band matrix.

2.3 Decryption Algorithm

In the decryption algorithm, whole process will be reversed to generate the original image. Receiver will be prompted to enter the password for generating the decrypted image. If the password is same given by the

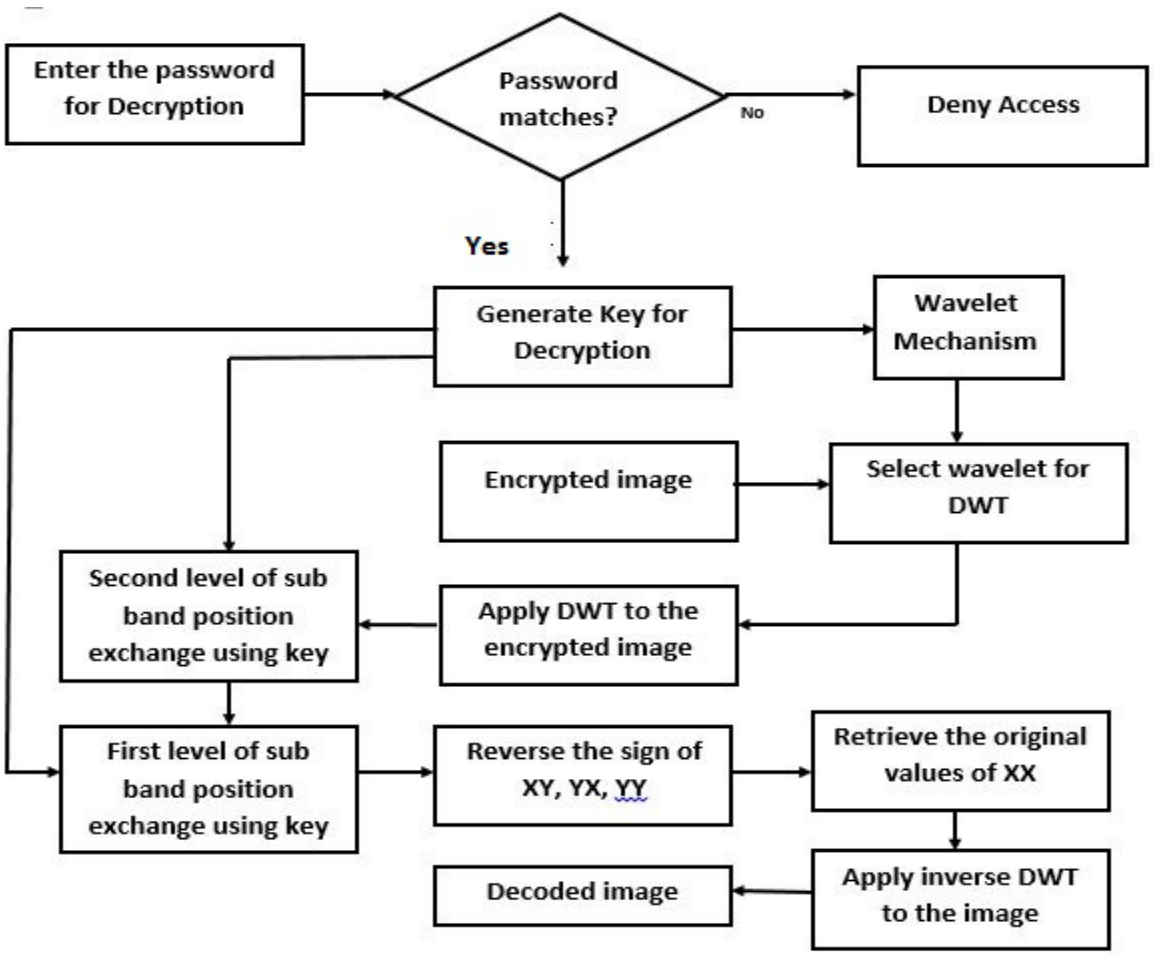

Figure 3. Decryption Process.

sender, receiver will be allowed to decrypt the image, otherwise decryption process will be terminated. Similarly a key will be generated from the given password, hence, wavelets will be chosen to apply Discrete Wavelet Transform (DWT). First step of the decryption will be second level of exchanging the sub band. Second step is exchanging the sub band as in the first level of encryption process. Now the values of XY, YX and YY will be inversed by multiplying (-1). During Encryption process, values of XX were lessened, now the same values will be recreated through XX(i,j)->XX(i,j)×(m×n). Figure 3 shows the decryption process. Thus at the final step, inverse wavelet transform will be applied to bring back the original image.

3. Experimental Analysis

Different images in different sizes were used for experimental analysis, the above algorithm fits to all test carried out. PSNR (Peak Signal Noise Ratio) is the main test conducted to verify the originality of the received image. If the resultant value of PSNR is 30db or greater, then there will not be a difference between original and decrypted image. In the proposed algorithm PSNR value lies between 25db and 35db. Figure 4 explains the Encryption and decryption process, At the left Original Lena and Boat images are shown, Encrypted images of Lena and Boat images are shown in the center, Decrypted images of Lena and Boat images are shown at the right. Hence, there will be a small distortion in a decrypted image. Similarly Figure 5 and

Figure 4. From top to bottom, standard images Lena and Boat, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

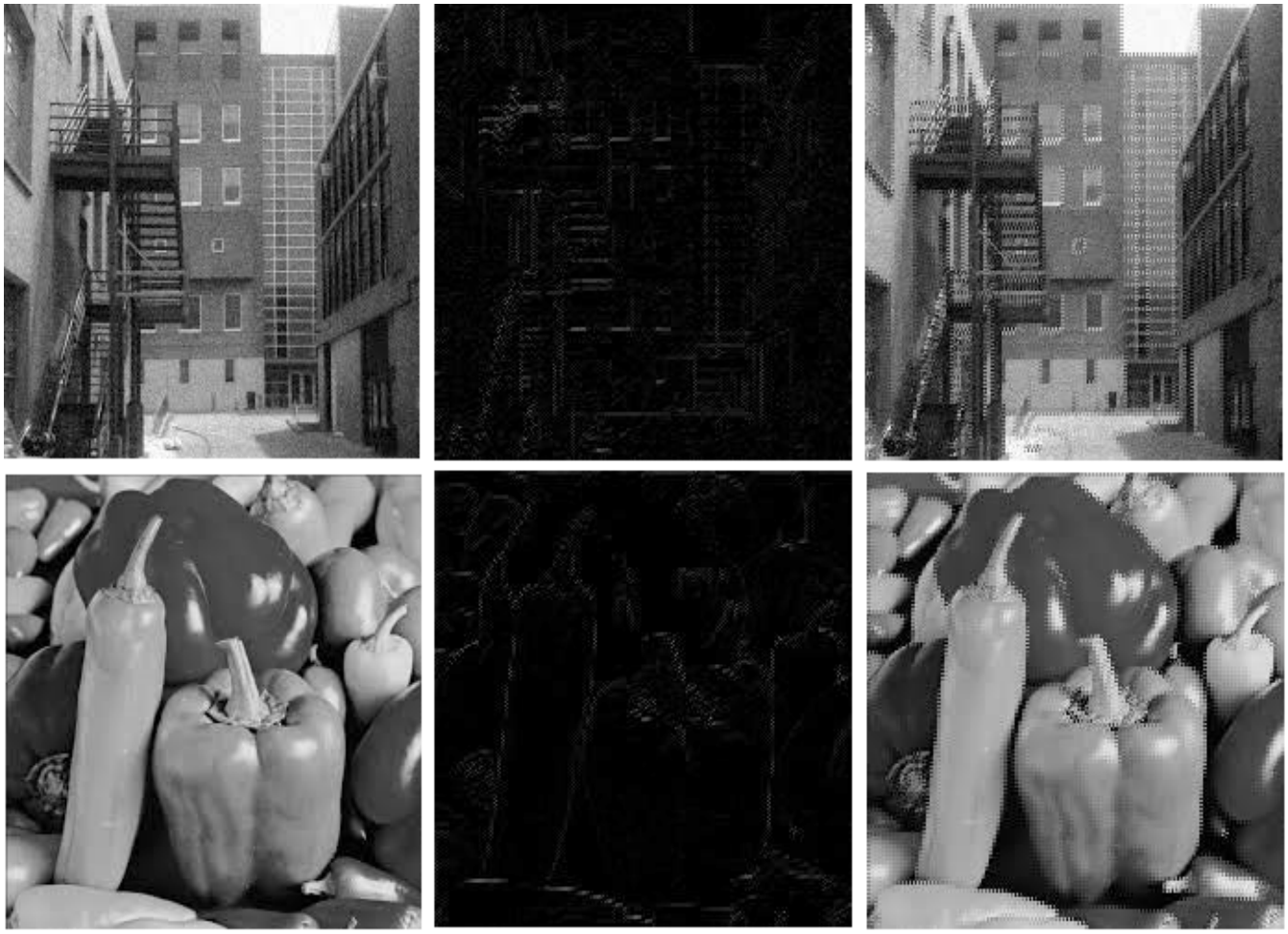

Figure 5. From top to bottom, standard images Building and Fruits, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

6 shows the same result using the proposed encryption and decryption process. Therefore, intruders cannot trace the logic behind encryption and decryption involved in the proposed algorithm. Table 1 shows the comparison of PSNR values between encrypted and decrypted images.

4. Security Analysis

In our proposed work, symmetric key is used for both encryption and decryption. Key will be generated separately by the sender using a password. Same password will be shared with the receiver to decrypt the image. Values of generated keys cannot be determined by the hackers without knowing the algorithm used for creating the keys. Computations of key generation also very less, hence it will not cause additional overhead to the system.

Table 1. Results of PSNR test with various standard images and decrypted images

Standard Image	PSNR between Original and Decrypted Images.
Lena	29.02
Building	29.60
Parrot	31.93
Photographer	28.37
Fruits	25.43
Butterfly	28.81
Woman	29.33

Figure 6. From top to bottom, standard images Photographer and Woman, from right to left, the figure presets the Original, Encrypted and Decrypted algorithm results.

5. Conclusion

Many algorithm proposed under frequency domain of an image, similarly in this paper, frequency domain is used for encrypting the image. The frequency sub bands plays a vital role in encryption part of this algorithm, positions of frequency band will be rearranged in a random manner, which cannot led to any guess for intruders. Hence the security of the image is bolted in this paper. Various security measures have been carried out to analysis the efficiency of the algorithm and the results of the test shows the robustness of the algorithm. Algorithm compared with many different benchmark algorithms and hence the proposed work shown the expected result.

6. References

1. Ramalingam M, Isa NAM. Video steganography based on integer haar wavelet transforms for secured data transfer. Indian Journal of Science and Technology. 2014; 7(7):897–904.
2. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015; 8(3):216.
3. Srinivasan B, Arunkumar S, Rajesh K. A novel approach for color image, steganography using NUBASI and randomized, secret sharing algorithm. Indian Journal of Science and Technology. 2015; 8(7):228.
4. Vijayaraghavan R, Sathya S, Raajan N. Security for an image using bit-slice rotation method-image encryption. Indian

Journal of Science and Technology. 2014;7(4):1–7.
5. Ganeshkumar K, Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. Indian Journal of Science and Technology. 2014; 7(S6):1–5.
6. Maniccam S, Bourbakis NG. Lossless image compression and encryption using SCAN. Pattern Recognition. 2001; 34(6):1229–45.
7. Yahya AA, Abdalla AM. A shuffle image-encryption algorithm. Journal of Computer Science. 2008; 4(12):999.
8. Ye R. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications. 2011; 284(22):5290–8.
9. Ismail IA, Amin M, Diab H. A digital image encryption algorithm based a composition of two chaotic logistic maps. IJ Network Security. 2010;11(1):1–10.
10. Tedmori S, Al-Najdawi N. Lossless image cryptography algorithm based on discrete cosine transform. Int Arab J Inf Technol. 2012; 9(5):471–8.
11. Van Droogenbroeck M, Benedett R, editors. Techniques for a selective encryption of uncompressed and compressed images. Advanced Concepts for Intelligent Vision Systems (ACIVS). 2002 Sep 9-11: Ghent, Belgium.
12. Sinha A, Singh K. A technique for image encryption using digitalsignature.Opticscommunications.2003;218(4):229–34.
13. Porwik P, Lisowska A. The Haar-wavelet transform in digital image processing: its status and achievements. Machine graphics and vision. 2004; 13(1/2):79–98.
14. Samson C, Sastry V. A novel image encryption supported by compression using multilevel wavelet transform. International Journal of Advansed Computer Science and Applications. 2012; 3(9):178–83.
15. Sethi N, Sharma D. A novel method of image encryption using logistic mapping. Int J Comput Sci Eng. 2012; 1(2):115–9.