ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

DESIGNING AN EFFICIENT IMAGE ENCRYPTION-THEN-COMPRESSION SYSTEM VIA RANDOM PERMUTATION AND WAVELET TRANSFORM FOR AN IMAGE OF HUMAN BRAIN

[1]Kumari Kiran, [2]Sunitha.N
Student, Department of Electronics and Instrumentation, Sathyabama University, Chennai, India.
Assistant professor, Department of Electronics and Instrumentation, Sathyabama University, Chennai, India.
Email: kirankapri135@gmail.com

Received on 18-02-2016 *Accepted on 12-03-2016*

Abstract

In this growing world, multimedia and technology is growing very fastly and there is a rapid development and so it becomes mandatory to take care of the security and privacy of an individual. To design and implement a secure system for the transmission of data so that possibility of data getting hacked could be made negligible for which designing and implementation of image encryption and compression system is taken in which lossy compression is considered. To achieve reasonably high level of security, a scheme for image encryption with random permutation method is taken into account.

This scheme is operated in prediction error domain. Image compression was done prior to encryption and hence we need to design a pair of encryption and compression algorithm such that compression can be applied to encrypted image efficiently. The encrypted image becomes noisy as a noise is produced for the higher security of image which in turn needs a larger space for the storage and process, to overcome this issue we propose a novel algorithm called COIFLET wavelet transform to compress the data.

Keywords: Encryption, Compression, Decompression Decryption.

Introduction:

In secure transmission of redundant data, there are generally two ways so that the data can be transmitted as well as kept secure and can be accessed only by the selected group of members to whom the data is concerned which are as follows

1. CTE(compression-then-encryption)
2. ETC(encryption-then compression)

CTE

In this type of method compression is done prior to encryption i.e the image is taken as the input which is compressed and hence the size of the image in context with the occupied space is reduced, after compressing the image it is then encrypted and hence converted to a not understandable format so that it can be kept secret, this image is then sent to the next level for transmission and is sent to the concerned person, now this encrypted image is decrypted by the receiver and hence the compressed image is recovered, finally this image is decompressed to recover the exact input image which is sent by the sender .This can be illustrated from the figure 1.

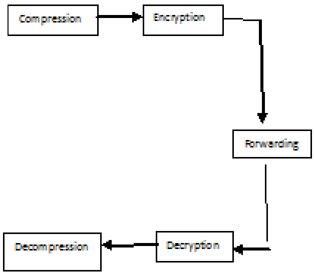


Fig 1: Block diagram of compression-then-encryption system

ETC (encoding-then compression)

In this system encoding is done prior to compression i.e in the beginning itself the input image is encrypted and converted into a format which can't be understood by the people who are not concerned and hence the image is already secure but the space occupied by the encrypted image is greater as compared to the input image, to overcome this issue the image is then compressed by removing the redundant data and hence the size of image is reduced and the space required is now less for the transmission of this image. now the image is forwarded to the receiver , after receiving this image decompression is performed on the image and the image is resized to the actual image and finally the key given by the sender to the receiver is used to recover that exact input image which is sent by the sender and hence the image is extracted. This can be illustrated from the figure 2.(from reference 1).

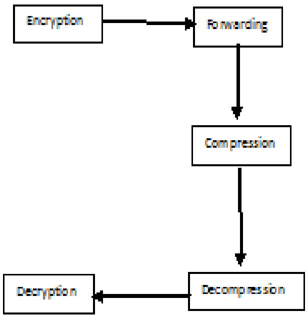


Fig 2: Block diagram of encryption-then-compression system

Explanation for keywords:

Encryption:

In cryptography, encryption is the process of encoding messages or information in such a way that only authorised parties can read it. Encryption does not itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plain text, is encrypted using an encryption algorithm, generation cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usuallyuses a pseudo-random encryption key which is gene rated by an algorithm. It is in principle possible the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorised recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorised interceptors.

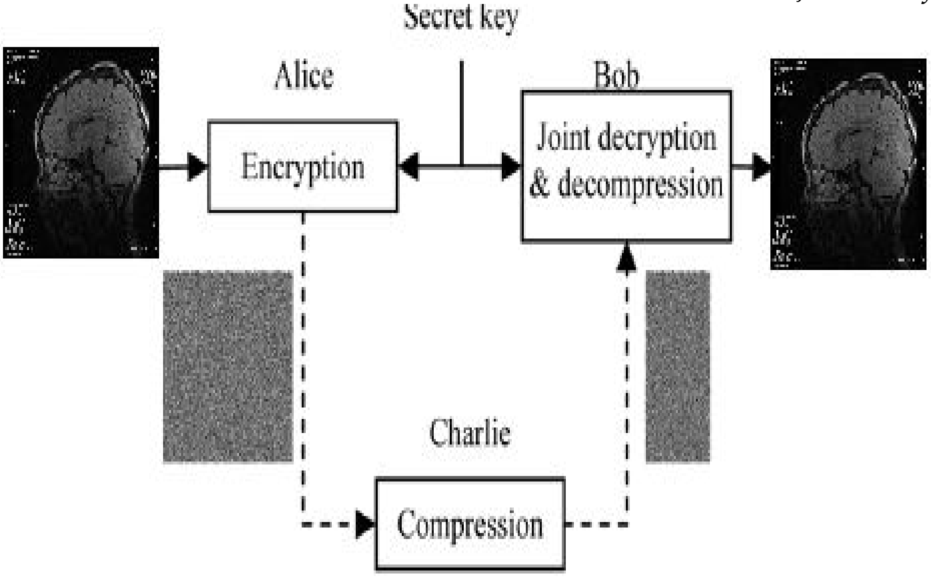
Compression:

In signal processing, data compression involves encoding information using fewerbits than the original representation. Compression can be either lossless or lossy. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying unnecessary information and removing it. The process of reducing the size of data file is referred to as data compression. Compression is important because it is used to reduce the resource usage such as data storage space or transmission capacity. The design of data compression schemes involves trade-offs among various factors, including the degree of compression, the amount of distortion introduced and the computational resources required to compress the data.

Decompression:

Decompression is a process which is exactly the reverse of compression which is used to recover the data by the concerned person. In this process the expansion of data takes place and hence the space required by the data after decompression increases. For decompression of data, storage space should be bigger than the space is required for the compressed data.

Decryption: Decryption is the process of recovery of the coded image and its conversion to the required format so that the data can be understood by the receiver and the concerned group of people. Decryption is performed by the receive with the help of the key which is given by the originator to the concerned person. After decryption the image which is sent in the beginning is recovered completely in the same format.



Block diagram of encryption-then-decryption system

Explanation of process:

In this process of designing a pair of encryption and then compression system, an example is taken where the input image is given by Alice which is a black and white image, this image is then encrypted by a method called random permutation method.

Random permutation method allows the rearrangement of its own bits in a regular manner according to a given code and a noise is produced using a pseudo noise source and is added to this image so that this image can be secured and can be prevented from hackers. Encoded image occupies more space as the pseudo noise is added to it, to overcome the problem of extra space and use of extra resources for its transmission, compression of the encoded image is required to reduce its size and hence the space required for it can be reduced.

In order to compress the encrypted image a novel algorithm called COIFLET wavelet transform. In this correspondence, we propose a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level.

Hence, in this process Alice just encrypts the input image by random permutation and gives the key to Bob, Charlie compresses the encrypted image given by Alice using COIFLET wavelet transform and then forwards the compressed image to Bob. Now, Bob receives the image studies statistical data and produces an image with better resolution and decompresses the image and finally he performs decryption with the help of the key given by Alice on the decompressed image and hence the he recovers the exact image which is sent by Alice.

Technique used for encryption and compression

1. Random Permutation

2. COIFLET wavelet transform

Explanation of techniques:

Random Permutation:

A random Permutation is a random ordering of a set of objects, that is, a permutation valued random variable. The use of random permutation is often fundamental to the fields that use randomised algorithm such as coding theory, cryptography, and simulation. A good example of a random permutation is the shuffling of a deck of cards: this is ideally a random permutation of 52 cards.

Generation of random permutation

One method of generating a random permutation of a set of length n uniformly at random (i.e., each of the n factorial permutation is equally likely to appear) is to generate a sequence by taking a random number between 1 and n sequentially, ensuring that there is no repetition, and

Output after encryption of image

Interpreting this sequence(x1, xn) as the permutation

(1 2 3. . . n)

(x1 x2 x3 . . . xn),

Shown here in two-line notation.

This brute-force method will require occasional retries whenever the random number picked is a repeat of a number already selected. This can be avoided if, on the ith step (when x1. . . . xi-1 have already been chosen) , one chooses a number j at random between 1 and n-i+1 and sets xi equal to the jth largest of the numbers that are not chosen .

Coif let wavelet transform:

Coif let with two vanishing moments

Coif lets are discrete wavelets designed by Ingrid Daubechies, at the request of Ronald Coifman, to have scaling functions with vanishing moments. The wavelet is near symmetric, their wavelet functions have N/3 vanishing moments and scaling functions N/3 -1, and has been used in Calderon-Zygmud Operators.

Input Images

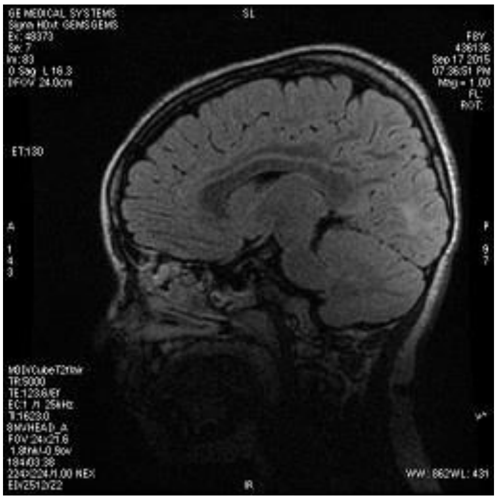


Image 1

Image description of input image 1

Number of bits: 256*256

Number of layers: 1

Colour description: black and white

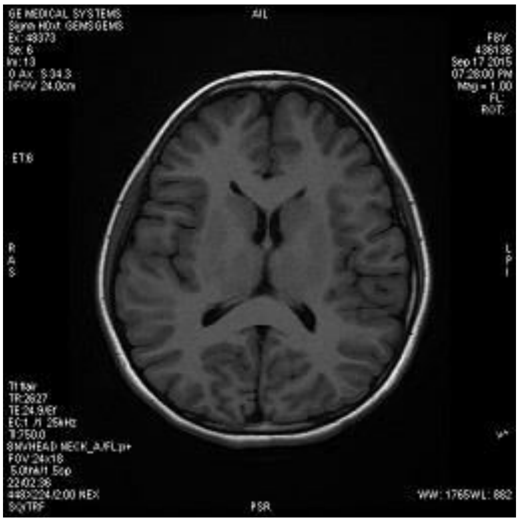


Image 2

Image description

Number of bits =256*256

Number of layers = 1

Colour description: black and white

Outputsof the encrypted image

Image 1

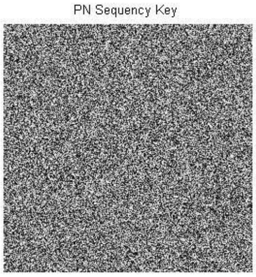
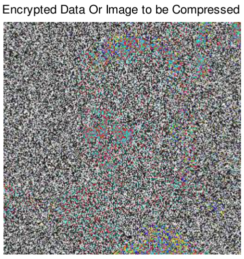


Image 2



References:

1. J. Zhou, X. Liu, and O. C. Au, “On the design of an efficient encryption then-compression system,” in *Proc. ICASSP*, 2013, pp. 2872–2876.

2. 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.

3. T. Bianchi, A. Piva, and M. Barni, “Encrypted domain DCT based on homomorphic cryptosystems,” *EURASIP J. Inf. Security*, 2009, Article ID 716357.

4. T. Bianchi, A. Piva, and M. Barni, “Composite signal representation for fast and storage-efficientprocessing of encrypted signals,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 180–187, Mar. 2010.

5. M. Johnson, P. Ishwar, V. M. P Prabhakaran, D. Schonberg, and K. Ramachandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004.

6. D. Schonberg, S. C. Draper, and K. Ramacandran, “On compression of encrypted Images,” in Proc. IEEE Int. Conf Images Process., Oct. 2006,pp.269-272.

7. D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, “On Compression of data encrypted with block ciphers,” IEEE Trans. Inf. Theory, Vol. 58, no. 11,pp.6989-7001, Nov . 2012.