Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 2, February 2013, pg.58 – 63

RESEARCH ARTICLE

Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression

[1]*Mohini Chaudhari*
Department of Computer Application,
Samrat Ashok Technological Institute, Vidisha. (M. P.) – 464001
chaudhari_mohini_21@yahoo.co.in

[2]*Dr. Kanak Saxena*
Department of Computer Application,
Samrat Ashok Technological Institute, Vidisha. (M. P.) – 464001
kanak.saxena@gmail.com

Abstract— With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. While storing and transmitting multimedia data are not easy and they need large storage devices and high bandwidth network systems. Compression and encryption technologies are important to the efficient solving of network bandwidth and security issues. This paper focus on dual approach of compression and security where compression is achieved through lossless algorithm (either Huffman coding or LZW) according to size and type of image data and compressed data is encrypted using traditional DES Algorithm.

Indexed Terms: - encryption, compression, Huffman, decompression, BMP image.

I. INTRODUCTION

Internet based communications are evolving at a tremendous rate. The Internet has facilitated the development of a worldwide 'Virtual Community' free from the constraints of time and geography. Due to the internet there is no distance between a person located in one place and experts around the globe. Through electronic mail / voice mail / video mail it is possible to solicit the opinion of experts. Moreover, Telemedicine is becoming popular in the specialties of radiology, pathology, critical care and psychiatry, where data is in the form of image. The internet has become a hostile environment with both wired and wireless channels offering no inherent assurance of confidentiality. It is required to ensure confidentiality and security for transmitting certain multimedia data over the internet. Encryption of data has become an important way to protect data resources especially on the Internet, intranets and extranets. The another challenge in multimedia applications is the transport services to both discrete media such as text and digital images and continuous media such as audio and video with limited bandwidth and huge data size. With the huge demand for bandwidth due to the large data transmitted in multimedia applications, it becomes necessary to apply compression algorithms on transmitted data. So the best way of fast and secure transmission is by using compression as well as encryption of multimedia data.

In the literature it has been seen that the dual approach of image compression & encryption is carried out in any one of the following ways based on the order of these two processes [1].

1. Individual or independent compression and encryption

a) *Compression followed by Encryption (CE)*: In this sequence an intruder have less cleave to access image but encryption may again increase the size.

b) *Encryption followed by Compression (EC)*: In this sequence size is not again increased but an intruder may have more clues to access the image. In some case sequence size decreased so not efficiently compressed.

2. Joint Compression and Encryption (JCE):

This approach is recently used which may be fast as compared to previous two but procedure is complicated.

Encryption applied by different researchers by means of encrypting algorithm which encrypt the entire or partial multimedia bit sequence using a fast conventional cryptosystem . Much of the past and current research targets encrypting only a carefully selected part of the image bit stream in order to reduce the computational load, and yet keep the security level high. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography.

Image compression algorithms are used use to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial and psychovisual redundancies. Mathematically, visual data compression typically involves transforming (encoding) a 2-D pixel array into a statistically uncorrelated data set. Two types of compression are lossless compression and lossy compression. If same image can be generated from the compressed image then it is Lossless compression otherwise it is lossy compression.

This study focuses on CE pattern in which compression is followed by symmetric key encryption. Compression of multimedia data such as images achieved through two lossless algorithm Huffman coding and LZW. Therefore in this paper comparative study of two image compression algorithm and their variety of features discussed and that factors are used to choose best among them for further encryption phase.

II. LITERATURE SURVEY

- Nikolaos G. Bourbakis [2] presented an image data compression-encryption scheme by using the words (patterns, or orders) produced by an image processing language called SCAN.
- S.S. Maniccam and N.G. Bourbakis [3] have presented a new methodology which performs both lossless compression and encryption of binary and gray-scale images. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology.
- Howard Cheng, Xiaobo li [4] performed compression using Quadtree compression Algorithm. But partial encryption is applied.
- Ebru Celikel, Mehmet Emin Dalkilic [5] performed experiments on a secure compression algorithm. Results are compared using different compression techniques like Arithmetic coding, Huffman Coding, Lempel-Ziv, Prediction by Partial Matching and Burrows Wheeler. Encryption is performed using symmetric key BBS PRNG. The authors applied algorithm on text file in English and Turkish.
- Masanori Ito *et al*. [6] proposed a method combining encryption and compression based on Independent Component Analysis (ICA) and Discrete Cosine Transform (DCT)..
- Younggap You, Hanbyeori Kim [7] performed compression using DWT (Discrete Wavelet Transform). For encryption Standard Encryption algorithm AES or ARIA is used.
- D. Maheswari, V. Radha [8] employed lossless compression using a novel layer based compound image compression technique that uses XML compression and JPEG to compress data. The encryption scheme, called, Shuffle Encryption Algorithm (SEA), proposed by Yahya and Abdalla (2008), is used..
- A. Alfalou C. Brosseau *et al.* [9] performed compression based on the discrete cosine transform (DCT). Two levels of encryption are used. The first one is due to the grouping of the DCTs in the spectral domain and after a second transformation, i.e. to hide the target images, one of the input images is used as encryption key.
- Goh Han Keat *et al.* [10] observed Embedded Zerotree Wavelet (EZW) encoder which specially designs for wavelet compression. Stream ciphers RC4 is selected as the encryption algorithm.
- N. V. Thakur and O. G. Kakde [11] proposed the compression and encryption based on the fractal coding and spiral architecture but the compression method are lossy.
- D. Kesavaraja *et al.* [12] observed that the conventional image compression algorithm does not run faster therefore they performed comparative study of three image compression algorithm and their variety of features and factors to choose best among them for cluster processing. For security they proposed a Distributed Intrusion Detection System to monitors all the nodes in cluster. If an intrusion is detected then a prevention step based on RIC (Robust Intrusion Control) is taken.

III. PROPOSED APPROACH AND METHODOLOGY

In this paper CE order i.e. compression is followed by encryption is applied on colour and grayscale image of different size and type. Here compression is performed by either Huffman or LZW lossless coding algorithm which is depending on user choice and contents of data. For resultant compressed data is secured by DES (Data Encryption Standard) encryption algorithm. The schematic block diagram of this proposed approach is given in Figure No. 1

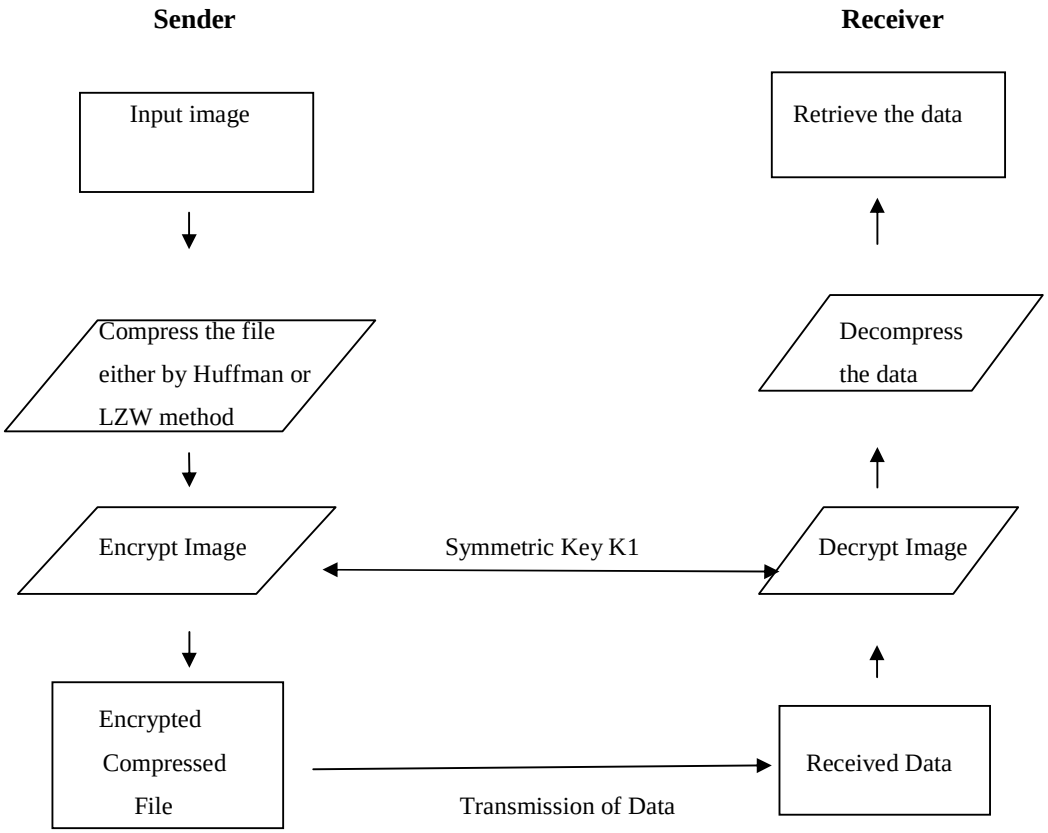


Fig 1 The schematic block diagram of proposed approach

Steps followed are as follow.

1) Browse or consider any standard grayscale or colored image which sender want to transmit securely and speedily.
2) Then sender choose any lossless algorithm either Huffman coding or LZW for compressing selected file.
3) Compressed image is encrypted by symmetric key k1 using DES algorithm and sent to receiver.
4) Receiver decrypt received data using same shared symmetric key k1.
5) Decompression of decrypted data is done either decompression algorithm of either Huffman or LZW to retrieve original transmitted data from sender.

Huffman coding:

Huffman code procedure is based on the two observations

a. More frequently occurred symbols will have shorter code words than symbol that occur less frequently.

b. The two symbols that occur least frequently will have the same length. The Huffman code is designed by merging the lowest probable symbols and this process is repeated until only two probabilities of two compound symbols are left and thus a code tree is generated and Huffman codes are obtained from labeling of the code tree

LZW compression:

It is a lossless 'dictionary based' compression algorithm. Dictionary based algorithms scan a file for sequences of data that occur more than once. These sequences are then stored in a dictionary and within the compressed file, references are put where-ever repetitive data occurred. LZW compression replaces strings of

characters with single codes. The code that the LZW algorithm outputs can be of any arbitrary length, but it must have more bits in it than a single character. The first 256 codes (when using eight bit characters) are initially assigned to the standard character set. The remaining codes are assigned to strings as the algorithm proceeds.

Data Encryption Standard:

DES is the Data Encryption Standard, a United States government standard encryption algorithm for encrypting and decrypting unclassified data of the same length. It uses a symmetric key, which means that the same key is used to convert cipher text back into plaintext. The DES block size is 64 bits.

IV. EXPERIMENTAL SETUP AND RESULTS

The proposed compression and encryption mechanism is implemented with NetBeans IDE7.1.2 and jdk6u34-windows using windows XP operating system with i4 processor and 4GB RAM. The experiments are carried out on some standard gray level or colored JPEG and BMP images. The performance evaluation factors compression ratios R and time requirement for encryption is obtained from different image is summarized in various table.

TABLE I
BMP IMAGES COMPRESSION DATA

Image No.	**Image Type**	**Original Size of Image (kb)**	**Compressed image size in kb & time**			
Colored BMP images			**Huffman**	**Time (Sec)**	**LZW**	**Time (Sec)**
01	16 color	25822	8455	0.06	6546	0.055
02	24 bit	151374	121307	0.24	133728	0.87
03	256 color	51586	29202	0.18	25809	0.16
Grayscale BMP images						
04	16 color	131190	30303	0.19	17205	0.11
05	24 bit	151218	117763	0.715	144861	0.88
06	256 color	11078	4297	0.035	2907	0.02

From the above table No 1 and 2, Lzw compression algorithm was showed better result for BMP images, especially with grayscale as compared to colored images. Lzw was more effective in 16 colored or 256 colored grayscale scale or colored image while its performance was poor for 24 bit grayscale scale or colored image. LZW compression works better with black and white bitmapped files. You will save memory space an average of about 30-40% with LZW compression, and in some cases you can save up to 80%. How much the file size will be reduced all depends on gradients and noise in input file. There are cases in which the LZW compression may make the file bigger if there is a noise in the file. As well as when image is compressed with lzw tech then it requires less time for encryption as comparative to Huffman coding so from above both table it is observed that lzw tech provide better result as compare to Huffman when input data is of bmp images using this approach.

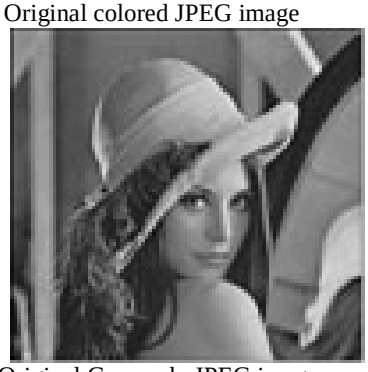
TABLE II
JPEG IMAGES COMPRESSION

Image No.	**Original Size of Image (kb)**	**Compression Method (Compressed size in kb)**			
Colored JPEG images		**Huffman**	**Time (Sec)**	**LZW**	**Time (Sec)**
01	27071	17612	0.938	35014	0.515
02	23029	20478	1.609	28278	0.78
Grayscale JPEG images					
01	26589	17174	0.234	34233	0.453
02	20504	17902	1.391	24510	1.922

JPEG images are fully compressed file format and especially used in case of lossy compression technique so while applying Huffman algorithm on JPEG image then on an average 10 to 20 % space reduction can be achieved While we get better result for following two JPEG images. Reconstructed image have same quality as compare to original because of lossless approach. On black and white or grayscale bmp images Huffman give better results. While discussing security of DES algorithm it has 64-bit key length so it is not easily affected by any attack except brute force. Time required to encrypt or decrypt image data is less so DES algorithm is fast and it achieves a good image encryption rate.


Original colored JPEG image


Reconstructed image


Original Grayscale JPEG image


Reconstructed image

V. CONCLUSION AND FUTURE SCOPE

The best way of fast and secure transmission is by using compression and encryption of multimedia data like images. The research works have been categorized this dual approach in the following three categories based on the order of the two process viz. CE, EC or JCE. From the above result, it is concluded that LZW compression is effective for grayscale bmp files as well as large text files. While it give effective result for 16bits or 8bits or 256 color image as compare to 24 bits image.

In the proposed approach the key is required to send separately. This is a different issue of securely transmitting the secret key. Future scope of the proposed work is that we can design the mechanism to securely

transmit the key so that unauthorized person should have no access to it. While currently this approach only focuses on multimedia data i.e. images but in future we will apply this approach on remaining data type e.g. audio and video and choose appropriate algorithm for encryption and compression which are suitable for them. The performance evaluation factors are Compression ratio and coding decoding time for compression and encryption respectively. But the balancing parameter for the combined process is not yet been defined.

REFERENCES

[1] A. Razzaque, N. V. Thakur, "Image compression and encryption: an overview", *International Journal of Engineering Research & Technology*, Vol. 1. 5, pp. 1-7, July 2012.

[2] N. G. Bourbakis, "Image data compression-encryption using G-scan patterns", *IEEE computational cybernetics and simulation*, vol.2 pp. 1117-1120, Oct 1997.

[3] S. S. Maniccam, and N. G. Bourbakis, "SCAN based lossless image compression and encryption", *IEEE Information intelligence and system*, pp. 490-499, 1999.

[4] H. Cheng and X. Li, "Partial encryption of compressed images and videos", *IEEE Transactions On Signal Processing*, Vol. 48. 8, pp. 2439-2451, August 2000.

[5] E. Celikel and M. E. Dalkilic, "Experiments on a secure compression algorithm", *Proceedings of the International Conference on Information Technology*: *Coding and Computing*, vol. 2, pp 150-152, April 2004.

[6] M. Ito, N. Ohnishi, A. Alfalou and A. Mansour, "New image encryption and compression method based on independent component analysis", *IEEE information an-d communication technologies from theory to application*, pp 1-6, April 2008.

[7] Y. You, H. Kim, "Endoscopy image compression and encryption under fault tolerant ubiquitous environment" IEEE *Biomedical circuit and system conference*, pp. 165-168, Nov 2009.

[8] D. Maheswari, V. Radha, "Secure layer based compound image compression using xml compression" *IEEE Computational intelligence and computing research*, pp 1-5, Dec 2010.

[9] A. Alfalou, C. Brosseau, N. Abdallah, M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images", *Optics express*, Vol. 19. 24, pp 24023-24029, Nov 2011.

[10] G. H. Keat, A. Samsudin, Z. Zainol, "Enhanced performance of secure image using wavelet compression" *World Academy of Science, Engineering and Technology*, Universiti Sains Malaysia, pp. 633-636, 2007.

[11] N. V. Thakur, and O. G. Kakde, "Compression mechanism for multimedia system in consideration of information security" *Proceeding of International workshop on machine intelligence research*, pp 87-96, 2009.

[12] D. Kesavaraja, R. Balasubramanian, D. Jeyabharathi, D. Sasireka, "Secure and faster clustering environment for advanced image compression" *Int. J. Advanced Networking and Applications*, Vol 02. 03, pp. 671-678, 2010.

