ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A RESEARCH PAPER ON A SECURE IMAGE ENCRYPTION-THEN COMPRESSION SYSTEM USING WAVELET VIA PREDICTION ERROR CLUSTERING AND RANDOM PERMUTATION

Er. Maninder Kaur*, Er. Navneet Choudhary
pHead of Department(CSE) Gurukul Vidyapeeth institute of Engineering and Technology, Banur
PUNJAB TECHNICAL UNIVERSITY ,JALANDHAR.

ABSTRACT

Images can be encrypted in many ways; several techniques have used different encryption methods. In this research, we apply a new modified International Data Encryption Algorithm to encrypt the full image in an efficient secure manner, after encryption the original file will be compressed and we get compressed image. This paper introduced a highly efficient image encryption-then compression (ETC) system using wavelet. The proposed image encryption scheme operated in the prediction error domain is able to provide a reasonably high level of security. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. We also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only slightly worse, in terms of compression efficiency, than the state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency. For the implementation of this proposed work we use the Image Processing Toolbox under Matlab software.

KEYWORDS: Compression of encrypted image, encrypted domain signals processing, image compression and image encryption.

INTRODUCTION

With the rapid development of multimedia and network technologies, the security of multimedia becomes more and more important, since multimedia data are transmitted over open networks more and more frequently. Typically, reliable security is necessary to content protection of digital images and videos. Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. For example, real-time encryption of an entire video stream using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level, this can be achieved using selective encryption that leaves some perceptual information after encryption.

Government, military and private business amass great deal of confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense) product, financial-status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer, if these confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands, than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement. We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is worldwide accepted fact that securing file data is very important, in today's computing environment. Good encryption makes a source look completely random, traditional algorithms are unable to compress encrypted data. For this reason, traditional systems make sure to compress before they encrypt. We are using the concept of public key encryption, for the encryption and decryption of image. In this public key's of

sender and receiver is known to both but private key's are kept secret. Neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain.

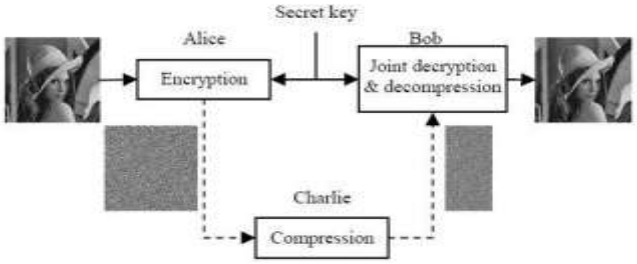

Figure: ETC system

S. Dharanidharan AP/CSE, S. B. Manooj kumaar in 2013. He proposed Modified International Data Encryption Algorithm using in Image Compression Techniques. Images can be encrypted in many ways; several techniques have used different encryption methods. In this research, we apply a new modified International Data Encryption Algorithm to encrypt the full image in an efficient secure manner, after encryption the original file will be segmented and converted to another image files. By using Huffman Algorithm the segmented image files are merged. Shaimaa A. El-said Khalid F. A. Hussein Mohamed M. Fouad in 2010. He proposed Securing Image Transmission Using in-Compression Encryption Technique. Multimedia is one of the most popular data shared in the Web, and the protection of it via encryption techniques is of vast interest. In this paper, a secure and computationally feasible Algorithm called Optimized Multiple Huffman Tables (OMHT) technique is proposed. OMHT depends on using statistical-model-based compression method to generate different tables from the same data type of images or videos to be encrypted leading to increase compression efficiency and security of the used tables. A systematic study on how to strategically integrate different atomic operations to build a multimedia encryption system is presented.

The remainder of this paper is organized as the following. At first, in Section II we illustrate the various components of our proposed technique to image encryption then compression. Further, in Section III we present some key experimental results and evaluate the performance of the proposed system. At the end we provide conclusion of the paper in Section IV and state some possible future work directions.

PROPOSED TECHNIQUE

This section illustrates the overall technique of our proposed image compression. In this paper we "A Secure Image Encryption-Then Compression System using Prediction Error Clustering and Random Permutation". In this paper we selects grey scale image to stimulate for encryption and compression. Wavelet transform is the latest method of compression where its ability to describe any type of signals both in time and frequency domain. So researchers take full advantage of the characteristic after wavelet transform and employ proper method to process the image coefficients for achieving effective compression.

Why Compression is needed?

In the last decade, there has been a lot of technological transformation in the way we communicate. This transformation includes the ever present, ever growing internet, the explosive development in mobile communication and ever increasing importance of video communication. Data Compression is one of the technologies for each of the aspect of this multimedia revolution. Cellular phones would not be able to provide communication with increasing clarity without data compression. Data compression is art and science of representing information in compact form. Despite rapid progress in mass-storage density, processor speeds, and digital communication system performance, demand for data storage capacity and data-transmission bandwidth continues to outstrip the capabilities of available technologies. In a distributed environment large image files remain a major bottleneck within systems. Image Compression is an important component of the solutions available for creating image file sizes of manageable and transmittable dimensions. Platform portability and performance are important in the selection of the compression/decompression technique to be employed.

Why we need image encryption?

If security of the image is paramount, then the usual method is to take the image file and encrypt that like any other data file. This has several drawbacks: first, if you're not well-educated in cryptography and computer programming,

you have to run out and buy somebody else's encryption software. Then there's the very likely possibility that the software company or some government agency has a 'backdoor' method of reading files encrypted by the software. Finally, any cryptographic system that isn't based on a random, one-time key is theoretically breakable. Encryption is the technology of keeping information secret. In this context, we define secret as "being protected from unauthorized access and attack." Although you may not think of your graphics files or their contents as ever being under attack, you may want to keep the information contained in these files from being copied or viewed by unauthorized people or computers. If copies of the files are freely available, the only way to keep the files secret is to encrypt them. Cryptography may seem to be a black art requiring extremely complex mathematics and access to supercomputers. This may be the case for professional cryptanalysts (code breakers). But for ordinary people who need to protect data, cryptography can be a strong, often simple to use, and sometimes freely available tool. This section doesn't try to explain cryptography, nor the details of particular cryptosystems.

Principle behind Image Compression

Images have considerably higher storage requirement than text; Audio and Video Data require more demanding properties for data storage. An image stored in an uncompressed file format, such as the popular BMP format, can be huge. An image with a pixel resolution of 640 by 480 pixels and 24-bit colour resolution will take up 640 * 480 * 24/8 = 921,600 bytes in an uncompressed format. The huge amount of storage space is not only the consideration but also the data transmission rates for communication of continuous media are also significantly large. An image, 1024 pixel x 1024 pixel x 24 bit, without compression, would require 3 MB of storage and 7 minutes for transmission, utilizing a high speed, 64 Kbits /s, ISDN line. Image data compression becomes still more important because of the fact that the transfer of uncompressed graphical data requires far more bandwidth and data transfer rate. For example, throughput in a multimedia system can be as high as 140 Mbits/s, which must be transferred between systems. This kind of data transfer rate is not realizable with today's technology, or in near the future with reasonably priced hardware.

Discrete Wavelet Transform

The discrete wavelet transform (DWT) refers to wavelet transforms for which the wavelets are discretely sampled. A transform which localizes a function both in space and scaling and has some desirable properties compared to the Fourier transform. The transform is based on a wavelet matrix, which can be computed more quickly than the analogous Fourier matrix. Most notably, the discrete wavelet transform is used for signal coding, where the properties of the transform are exploited to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. The discrete wavelet transform has a huge number of applications in Science, Engineering, Mathematics and Computer Science. Wavelet compression is a form of data compression well suited for image compression (sometimes also video compression and audio compression). The goal is to store image data in as little space as possible in a file. A certain loss of quality is accepted (lossy compression). Using a wavelet transform, the wavelet compression methods are better at representing transients, such as percussion sounds in audio, or high-frequency components in two-dimensional images, for example an image of stars on a night sky. This means that the transient elements of a data.

Clustering

Clustering can be considered the most important *unsupervised learning* problem; so, as every other problem of this kind, it deals with finding a *structure* in a collection of unlabeled data. A loose definition of clustering could be "the process of organizing objects into groups whose members are similar in some way". A *cluster* is therefore a collection of objects which are "similar" between them and are "dissimilar" to the objects belonging to other clusters.

EVALUATION AND RESULTS

To verify the effectiveness (qualities and robustness) of the proposed a secure image Encryption-Then Compression system using Prediction Error Clustering and Random Permutation. We conduct several experiments with this procedure on several images. There are some steps of our proposed technique are given below:

Phase 1: Firstly we develop a particular GUI for this implementation. After that we develop a code for the loading the image file in the Matlab database.

Phase 2: Develop a code for the encryption algorithm using the wavelet with suitable key in proposed work. When code is develop then apply on the image.

Phase 3: Develop a code for the compression technique using Prediction Error Clustering and Random Permutation.

Phase 4: After that we develop code for the decompression and decryption process.

Flow Chart of proposed method

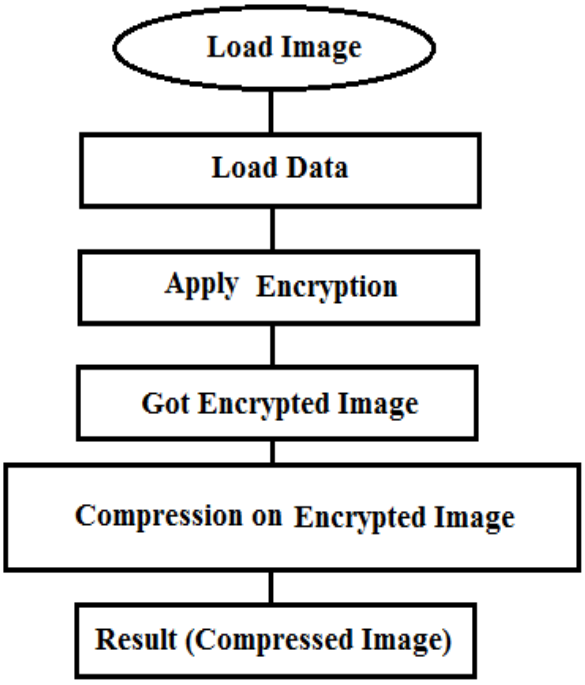

Figure.1: Flow chart of proposed method

Results

When we simulate our implementation then we got these result which more accurate than previous work:

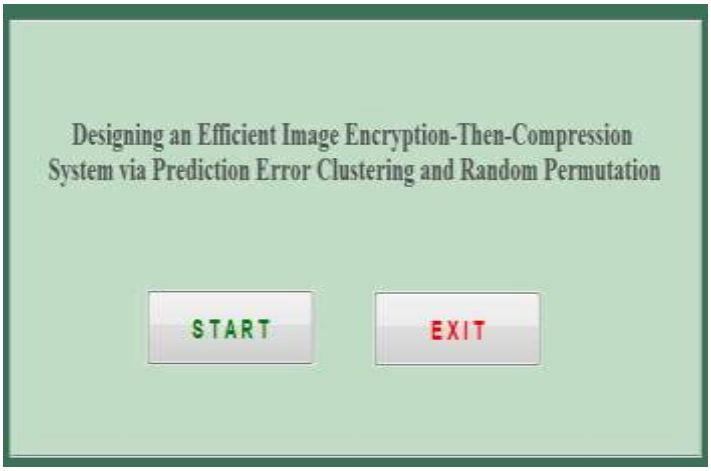

Figure.2: Main Figure Window

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

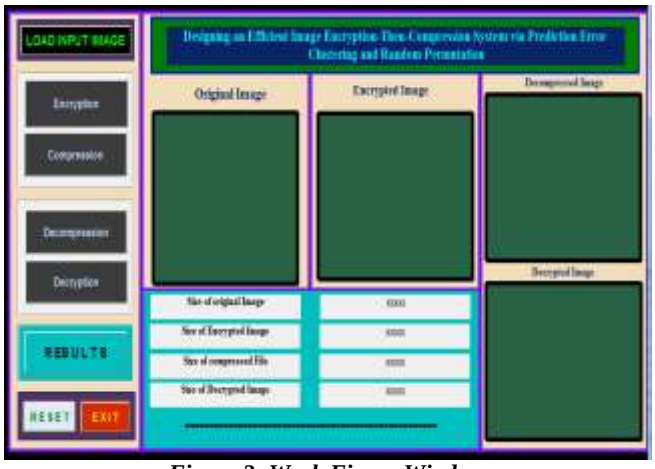

Figure.3: Work Figure Window

Figure.4: Running Work Figure Window

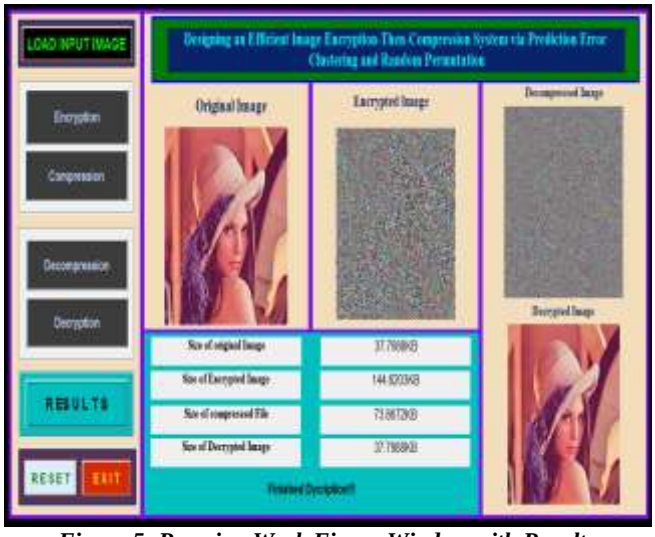

Figure.5: Running Work Figure Window with Results

	Size of original image (kb)	size of encrypted image	Size of compressed image(kb)	Size of decrypted image(kb)	PSNR(db)
Image1	1351	267	118	76	36
Image2	732	145	75	37	35
Image3	768	148	76	27	34
Image4	2025	396	157	101	34
Image5	768	151	70	31	35

Comparision Tabl

CONCLUSION

In this paper we "A secure image Encryption-Then Compression system using Wavelet via Prediction Error Clustering and Random Permutation". In this paper we selects grey scale image to stimulate for encryption and compression. Wavelet transform is the latest method of compression where its ability to describe any type of signals both in time and frequency domain. Within the proposed framework, the image encryption has been achieved via prediction error clustering and random permutation. Highly efficient compression of the encrypted data has then been realized by a context-adaptive arithmetic coding approach. Both theoretical and experimental results have shown that reasonably high level of security has been retained. More notably, the coding efficiency of our proposed compression method on encrypted images is very close to that of the state of the art lossless/lossy image codes, which receive original, unencrypted images as inputs.

REFERENCES

[1] R. C. Gonzalez and R. E. Woods, Digital Image Processing 2/E. Upper Saddle River, NJ: Prentice-Hall, 2002.
[2] J. J. Ding and J. D. Huang, "Image Compression by Segmentation and Boundary Description," June, 2008.
[3] G. K. Wallace, 'The JPEG Still Picture Compression Standard', Communications of the ACM, Vol. 34, Issue 4, pp.30-44.
[4] M. Campista, P. Esposito, I. Moraes, L. H. Costa, O. C. Duarte, D. Passos, C. V. de Albuquerque, D. C. Saade, and M. Rubinstein, outing metrics and protocols for wireless mesh networks,‖ IEEE Netw., vol. 22, no. 1, pp. 6–12, Jan.–Feb. 2008.
[5] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ―An efficient filter-based addressing protocol for auto configuration of mobile ad hoc networks,‖ in Proc. IEEE INFOCOM, Apr. 2009, pp.2464–2472.
[6] P. B. Velloso, R. P. Laufer, O. C.M. B. Duarte, and G. Pujolle, ―Trust management in mobile ad hoc networks using a scalable maturity based model,‖ IEEE Trans. Netw. Service Manage. vol. 7, no. 3, pp. 172–185, Sep. 2010.
[7] D. Passos and C. V. N. Albuquerque, ―A joint approach to routing metrics and rate adaptation in wireless mesh networks, in Proc. IEEE INFOCOM Workshops, Apr. 2009, pp. 1–2.
[8] S. Biswas and R. Morris, ―ExOR: Opportunistic multi-hop routing for wireless networks,‖ in Proc. ACM SIGCOMM, Aug. 2005, pp. 133–143.
[9] Mitra, Y. V. Subba Rao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques"
[10] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image" IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.
[11] Daniel Schonberg, Stark C. Draper, Chuohao Yeo, Kannan Ramchandran, "Towards Compression of Encrypted Images and Video Sequences"
[12] Ibrahim Fathy El-Ashry, "Digital Image Encryption" A Thesis Submitted for The Degree of M. Sc. of Communications Engineering.
[13] D. Schonberg, S. C. Draper, C. Yeo, K. Ramchandran, "Toward compression of encrypted images and video sequences" IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.
[14] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inform. Theory, vol. IT-19, pp. 471–480, July 1973.
[15] A.Wyner and J. Ziv, "The rate-distortion function for source coding withcside information at the decoder," IEEE Trans. Inform. Theory, vol. IT-22, cpp. 1–10, Jan. 1976.

[16] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," IEEE Trans. Inform. Theory, vol. 49, pp. 626–643, Mar. 2003.
[17] T. M. Cover and J. A. Thomas, Elements of Information Theory. New York: Wiley, 1991.
[18] M.W. Marcellin and T. R. Fischer, "Trellis coded quantization of memory less and Gauss-Markov sources," IEEE Trans. Commun., vol. 38, pp. 82–93, Jan. 1990.
[19] G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. Inform. Theory, vol. IT-28, pp. 55–67, Jan. 1982.
[20] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–175, 1949.