ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

Modified International Data Encryption Algorithm using in Image Compression Techniques

[1]S.Dharanidharan AP/CSE, [2]S.B.Manoojkumaar AP/CSE ,[3]D.Senthilkumar AP/IT
JKK Munirajah College of Technology

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 segmented and converted to another image files. By using Huffman Algorithm the segmented image files are merged. And we merge the entire segmented image to compress into a single image. Finally we retrieve a fully decrypted image. Next we find an efficient way to transfer the encrypted images to multipath routing techniques, The above compressed image has been sent to the single path way and now we enhanced with the multipath routing algorithm, finally we get an efficient transmission and reliable, efficient image.

Index Terms— **Image Processing, Stenography, Cryptography, Multipath Routing.**

I. INTRODUCTION

It is one of the emergent technologies, its uses in a variety of characteristics of a business. Image Processing plays a vital role in the research areas of computer science disciplines besides. An image can be converted into digital structure and act upon some function on it using Image processing; this is in order to obtain an enriched image. An input that can be given in the form of images, like video or photo and the output may be image or inimitability coupled with that image. Image processing system frequently contains treating images as two dimensional signals while giving an efficient set signal processing methods to them. It can be classified into five different types. It follows as visualization, image sharpening &restoration, image retrieval, measurement of patterns and image recognition.

A. STEGANOGRAPHY HISTORY:

The Steganography is the art of recent modern techniques in the world of multimedia and computer science for hiding information in communication. The word steganography is comes from Greek word which means “covered writing” it’s called stenography [2]. The most of the text where written on wax-covered tablets. This is to send a hidden message; anyone would scrape off the growth and write the message on the basic wood.

i. Modern steganography:

The Modern steganography not only buries the data, but it’s encrypts. Data are not only hided in images or any other, but it is also digital file. Due to deviations in the encoding of a song, it is also many different digital footprints which construct it difficult to use relative analysis to become aware of differing versions.

B. Wireless Networking:

In recent years a lot of networking techniques have been using several research methodologies. Networking, is an inter communication between the one system to another system. In our research we need to compress the image from one system to another system in multipath routing techniques in wireless networks. The sender sends the data from one system to another system; they need some more path, i.e)., sender send the data to the receiver through several nodes that are interconnection between those. Heretofore they are using one way communication in wireless networking, here we going to use multipath communication in our research to secure and reliable transfer of image.

C. Cryptography:

The word cryptography comes from cryptology which lies in earliest Greek. The word cryptology is has two components: namely "kryptos"& "logos", kryptosit means hidden and logosit means word. It is one of the very oldest safeguard military and sensitive communications. We define with an example, where the famous Roman emperor Julius Caesar used a Caesar cipher method to protect the messages from the unauthorized. The cryptology has two major divisions: they are cryptography and cryptanalysis [3]. The cryptographer looks for the methods to

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

ensure the protection and security of conversations whereas the cryptanalyst is a method to undo the previous work by splitting the systems.

II.EXISTING SYSTEM

In this paper, we are combining more than one domain like image processing, stenography, cryptography and wireless networking in orderly each has some of the drawbacks in every domain. Now we see algorithms that are used in the existing system and the drawbacks of the existing system.

A. Compression techniques:

The loss compression of JPEG standard technique has been introduced. JPEG (Joint Photographic Experts Group) is an international compression standard for regular-manner where it uses both grayscale and color. By using this wide range of applications for regular-manner images can be measured[2][3]. The two major basic compression methods of JPEG standard are one for loss compression, and another for lossless compression.

They have introduced just only the basic concepts of image compression of PEG standard. Although they don't have much more point to detail out. The JPEG standard has become the most popular image form and has some properties to improvement. Fig-i it represents the comparison of the exiting quality of an image and its improvements.

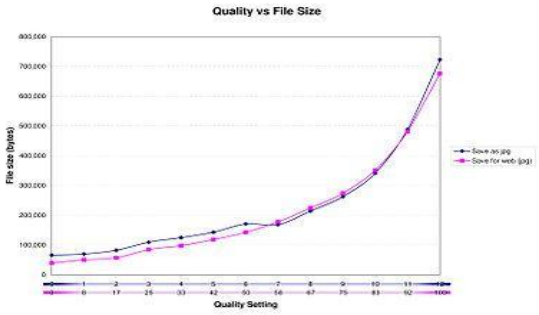


Fig-I JPEG Quality comparison

B Cryptography techniques:

This technique intends a novel scheme for separable reversible data hiding in encrypted images. The original uncompressed image can be encrypted using an encryption key [14] [16]. Later, a data-hider may be used to compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver knows the encryption key, then the receiver can decrypt the received data to obtain an image which is similar to the original one, but we cannot extract the additional data of the image that has been decrypted. Where if the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data which is not too large.

III.PROPOSED WORK

A. Huffman Algorithm

An algorithm which is used to compress lossless data is called **Huffman coding [13]**. This Huffman coding use of avariable-length code table for encoding a source symbol. With the use of that it builds an extended binary tree with a minimum weighted path length from a set of given weights. Let us consider with a linked list of partial trees. Initially, the list contains one entry for each character. In every iteration, we have to choose the two partial trees of least weight and construct a new tree consisting of an internal node plus these two as its children. Again insert the new tree back onto the list, where its weight must equal to the sum of its weights of the children's. The length of the list should be reduced by 1 after n-1 iterations we have a list consisting of a single node, which is our decode tree. The principle is demonstrated as below. However, this isn't the way the how the code actually works out. For convenience, it builds the list backwards.

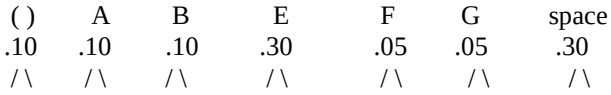
Note: The weight of the least tree should be printed with italics in each step

Initial list:

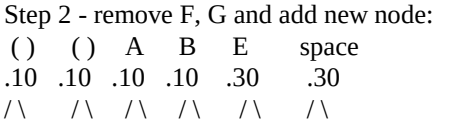
A B C D E F G space

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

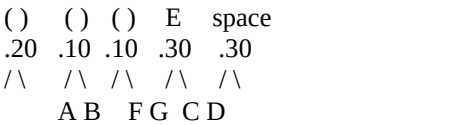
Step 1 - remove C, D and add new node:



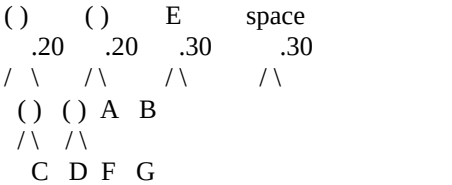
Step 2 - remove F, G and add new node:



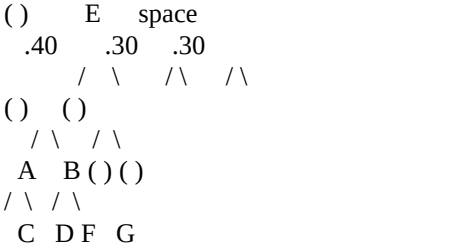
Step 3 - remove A, B and add new node:



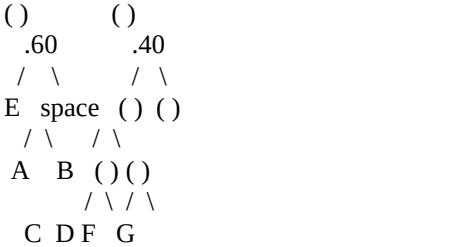
Step 4 - remove two partial trees and add new node:



Step 5 - remove two partial trees and add new node:

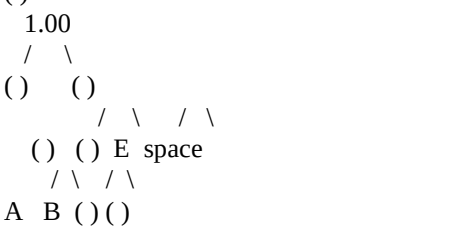


Step 6 - remove E, space and add new node:



Chapter 2: Lossless compression

Step 7 - construct final tree:



ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

/ \ / \
C D F G

For the performance of the algorithm structure of the initial list is O(n). Transforming to a tree involves n-1 (= O(n)) iterations. On each iteration, we scan the entire list to find the two partial trees of least weight = O(n) - so this process, using the simplest mechanism for storing the list of partial trees is O(n2). (It can be made O(n log n) by storing the partial trees in a heap. Printing the tree is O(n).Overall is therefore O(n2). However, we could reduce time to O(n log n) by using a more sophisticated data structure for the "list" of partial trees - e.g. a heap based on weight.We have applied this technique to individual characters in an alphabet. It could also be profitably applied to larger units - e.g. we might choose to have a single code for frequently occurring words (such as "the") or sequences of letters within words (such as "th" or "ing".

B. Steganography:

This concept introduces a best approach for Least Significant Bit (LSB) based on image steganography which improves the surviving LSB substitution techniques to improve the security level of hidden information. This is a new approach to substitute LSB of RGB true color image. The new security conception hides secret information within the LSB of image where a secret key encrypts the hidden information to protect it from unauthorized users. In common, LSB methods [20], hidden information is stored into a specific position of LSB of image. We have to know the reasons for the retrieval methods; hence anyone can extract the hidden information. In our research, the hidden information's are stored into different position of LSB of image depending upon the secret key. As an end result, it is very difficult to extract the hidden information from the retrieval methods. We have used the Peak Signal-to-Noise Ratio (PSNR) [22] [20] to measure the quality of the stego images. The significance of PSNR gives better end result because our proposed method changes very small number of bits of the image. The result attained shows that the proposed method results in LSB based image steganography using secret key which provides good security issue and PSNR value than general LSB based image steganography methods.

C. Cryptography techniques:

In our paper, we propose a novel scheme for separable reversible data hiding in encrypted image, which consists of image encryption, data embedding and data-extraction &image-recovery phases. In our first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, we can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, we can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in[1] or [2] is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. Though, the loss compression method in [3] compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossycompression deserves further investigation.

Fig – (i). Original Image

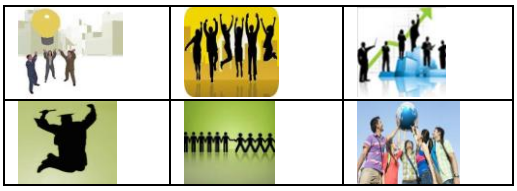


Fig-(ii) The segmented images after encryption

Fig- (iii). After merging image

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

D. Multipath routing algorithm:

Routing is a challenging technique in a wireless multi-hop networks owing to the high loss rate and dynamic quality of wireless links. The recently proposed routing for any path has a way to avoid these shortcomings by using multiple next-hops for each destination [7]. We present a new routing pattern which generalizes opportunistic routing for wireless multi-hop networks. A packet is broadcast to the nodes in the set, and one of them forwards the packet on to the destination. In multi-rate [11] any path routing, each node uses both a set of next-hops and a selected transmission rate to reach a destination. Up to date, there is no theory capable of jointly optimizing both the set of next-hops and the transmission rate used by each node. We solve this by introducing Floyd's algorithms for routing and which provides the proof of its optimality. The proposed algorithms will have roughly the same running time as regular shortest-path algorithms and are therefore suitable for deployment in routing protocols [5][7]. The measurements will be conducted in an 802.11b test bed network, and our trace-driven analysis will be examined for multi-rate any path routing is on average 80% better than 11-Mbps any path routing, with a factor of 6.4 improvements in the best case. If the rate is fixed at 1 Mbps instead, performance improves by a factor of 5.4 on average.

IV.CONCLUSION

In this paper, we introduce three important techniques namely cryptography, multipath routing algorithm and steganography. The cryptography introduces a novel scheme for separable reversible data hiding [21]. The steganography approach for Least Significant Bit (LSB).And the multipath routing algorithm involves in the dynamic quality of wireless links. These three techniques are combined together along with the Huffman algorithm, to encrypt the image in an efficient way. The image that can be divided into six segments and which end results in a different new image

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] Z. Zhong, J. Wang, S. Nelakuditi, and G.-H. Lu, ―On selection of candidates for opportunistic any path forwarding, ‖ Mobile Comput. Commun. Rev., vol. 10, no. 4, pp. 1–2, Oct. 2006.

[10] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, ―Trading structure for randomness in wireless opportunistic routing in Proc. ACM SIGCOMM, Aug. 2007, pp. 169–180.

[11] H. Dubois-Ferrière, M. Grossglauser, and M. Vetterli, ―Valuable detours: Least-cost any path routing, IEEE/ACM Trans. Netw., vol. 19, no. 2, pp. 333–346, Apr. 2011.

[12] L. Kleinrock, ―On giant stepping in packet radio networks, UCLA, Los Angeles, CA, Packet Radio Temporary Note #5, PRT 136, Mar. 1975.

[13] Dr. Charles F. Hall, "A Hybrid Image Compression Technique," Acoustics Speech & Signal Processing, IEEE International Conference on ICASSP' 85, Vol. 10, pp 149- 152, Apr, 1985.

[14] Wen Shiung Chen, en- HuiYang & Zhen Zhang, " A New Efficient Image Compression Technique with Index Matching Vector Quantization," Consumer Electronics, IEEE Transactions, Vol. 43, Issue 2, pp 173- 182, May 1997.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 2, March 2013

[15] David H. Kil and Fances Bongjoo Shin, "Reduced Dimension Image Compression And its Applications," Image Processing, 1995, Proceedings, International Conference,Vol. 3 , pp 500-503, 23-26 Oct.,1995.

[16] C.K. Li and H.Yuen, "A High Performance Image Compression Technique For Multimedia Applications," IEEE Transactions on Consumer Electronics, Vol. 42, no. 2, pp 239-243, 2 May 1996.

[17] Shi-Fei Ding, Zhong –Zhi Shi,Yong Liang , Feng- Xiang Jin, " Information Feature Analysis and Improved Algorithm of PCA," Proceedings of the 4th International Conference on Machine Learning and Cybernetics, Guangzhou, pp 1756-1761 , 18-21 August,2005.

[18] Vo Dinh Minh Nhat, Sung Young Lee, "Two- Dimensional Weighted PCA algorithm for Face Recognition," Proceedings 2005 IEEE International Symposium on Computational Intelligence in Robotics and Automation, pp 219-223, June 27-30, 2005, Espoo, Finland.

[19] Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and Videos" IEEE Transactions On Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000.

[20] Masanori Ito, Noboru Ohnishi, Ayman Alfalou and Ali Man sour, "New Image Encryption and Compression Method Based on Independent Component Analysis", IEEE, 2007.

[21] Younggap You, Hanbyeori Kim, "Endoscopy Image Compression and Encryption under Fault Tolerant Ubiquitous Environment" 978-1-4244-4918-7 IEEE, pp. 165- 168, 2009.

[22] A. Alfalou C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images", OPTICS EXPRESS 24024Vol. 19, No. 24 OSA, 2011.

[23] 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 MIR Day GHRCE-Nagpur, India, pp. 87-97, 2009.

[24] A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, " Lossless Image Compression And Selective Encryption Using A Discrete Radon Transform" IEEE-1-4244-1437- 7/07,ICIP, pp.IV 465-468, 2007.

AUTHOR BIOGRAPHY

He was born in 1983, he received him BCA (2003) and MCA (2006) degree in bharathiyar university after that his done M.E degree in Anna University 2008, After that he worked at Capital Group of Technology in July 2008 to April July 2010 the role of software developer. After that he is working as an Assistant Professor in JKK.Munirajah College of Technology, T.N.Palayam, Gobichettipalayam, and Erode.
E-Mail ID: dharani.855@gmail.com

He was born in 1988; he received him B.E.Computer Science & Engineering (2009) in S.S.M.College of Engineering (Anna University) and M.E Computer Science & Engineering (2011) in Sasurie College of Engineering (Anna University Coimbatore), after that he is working as an Assistant Professor in JKK.Munirajah College of Technology, T.N.Palayam, Gobichettipalayam, Erode.
E-Mail ID : manoojkumaarsb@gmail.com

He was born in 1983, he received him DCT (2002) in A.J.K.K.S.P.T.C, T.N.Playam and B.TECH (IT) (2008) degree in Nandha engineering college (Anna university) after that he doing M.E degree through MBCBS in Anna University, Trichy. He worked as software engineer at PATNI COMPUTER SYSTEMS PVT LTD, MUMBAI from December 2008 to April 2009. After that he worked as software engineer in Capital Group of Technology in May 2009 to April July 2010. After he is working as an Assistant Professor in JKK.Munirajah College of Technology, T.N.Palayam, Gobichettipalayam, and Erode.
E-Mail ID : senthit83@gmail.com