International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

A Modified Encryption Algorithm for Compression of Color Image

C.MariSelvi[1], Arun Kumar [2]
[1]*ManonmaniamSundaranar University, Tirunelveli*
[2]*JP College of Engineering, Ayikudy.*
[1]mselvi36@gmail.com
[2]arunmecse2013@gmail.com

***Abstract*— The main objective of this project is to compress the encrypted color images. This is done by using Resolution-Progressive Compression (RPC). Usually in secure transmission of redundant data, the data is usually first compressed and then encrypted at the sender side. To recover the data at the receiver side, decryption is performed prior to decompression. In some application scenarios the encryption is done first and then the encrypted data is compressed. In this project the encryption is done by using the Data Encryption Standard (DES) method. After the encryption the encoder gets the cipher text and decomposes it into four sub images. After the decomposition, each sub-image is encoded independently using Run Length coder And the resulting syndrome bits are transmitted from the lowest resolution to the highest Decoding starts from the 00 sub- image of the lowest-resolution level say, level N. Next, other sub-images of the same resolution level are interpolated from the decrypted 00N sub images. Context Adaptive Interpolation is used in this project. Then the up sampling process is done to get the encrypted image. Finally the decryption is applied to get the compressed image.**

***Keywords*— Encryption, Resolution, Decryption, Color, Decoding.**

I. INTRODUCTION

Image compression has been the key technology for transmitting massive amount of real-time image data via limited bandwidth channels. The data are transferred in the form of image, graphics, audio and video. These types of data have to be compressed during the transmission process. Otherwise the data need a large storage capacity and transmission bandwidth if it is uncompressed. Huge amount of data can't be fit if there is low storage capacity present. To solve this problem the data has to be compressed by using any one of the algorithms and then it can be sent easily.

Data compression is the process of converting an input data stream into another data stream that has smaller size. There are two types of image compression: lossless and lossy. With lossless compression, the original image is recovered exactly after decompression. Much higher compression ratios can be obtained if some error, which is usually difficult to perceive, is allowed between the decompressed image and the original image. This is lossy compression. In many cases, it is not necessary or even desirable that there be error-free reproduction of the original image. In such a case, the small amount of error introduced by lossy compression may be acceptable. Another application where lossy compression is acceptable is in fast transmission of still images over the Internet.

Compression – An Overview

In the recent years, large scale information transfer by remote computing and the development of massive storage and retrieval systems have witnessed a tremendous growth. To cope up with the growth in the size of databases, additional storage devices need to be installed and the modems and multiplexers have to be continuously upgraded in order to permit large amounts of data transfer between computers and remote terminals. This leads to an increase in the cost as well as equipment. One solution to these problems is-"COMPRESSION" where the database and the transmission sequence can be encoded efficiently. Compression is possible only because data is normally represented in the computer in a format that is longer than necessary i.e. the input data has some amount of redundancy associated with it. The main objective of compression systems is to eliminate this redundancy. When compression is used to reduce storage requirements, overall program execution time may be reduced. This is because reduction in storage will result in the reduction of disc access attempts.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

The compression algorithms help to reduce the bandwidth requirements and also provide a level of security for the data being transmitted. A tandem pair of coder and decoder is usually referred to as code.

S. S. Pradhan and K. Ramchandran [2] proposed to compress data in a wireless sensor network in order to reduce communication energy in sensor nodes.

Power is a precious resource in wireless sensor networks due to the limited battery capacity.

J. García-Frías and Y. Zhao [3] introduced an iterative decoding approach for compression of correlated binary sequences. Each source is independently encoded using a punctured turbo code, and the correlation between sources is not used in the encoding process.

A. Liveris, Z. Xiong, and C. Georghiades [4] proposed that how low-density paritycheck (LDPC) codes can be used as an application of the Huffman theorem for correlated binary sources. This project focus on the asymmetric case of compression with side information.

D. Varodayan, A. Aaron, and B. Girod [5] presented rate-adaptive LDPCA and SLDPCA codes for the case of asymmetric distributed coding in which the encoder is not aware of the joint statistics between source and side information.

M. Weinberger, G. Seroussi, and G. Sapiro [6] proposed that LOCO-I (LOwCOmplexityLOsslessCOmpression for Images) is the algorithm at the core of the new ISO/ITU standard for lossless and near-lossless compression of continuous- tone images, JPEG-LS. It is conceived as a "low complexity projection" of the universal context modeling paradigm, matching its modeling unit to a simple coding unit.

A. Aaron, S. Rane, E. Setton, and B. Girod [7] proposed a transform-domain Wyner- Ziv video codec which uses intraframe encoding and interframe decoding. This type of codec is useful for systems which require simple encoders but can handle more complex decoders.

The remainder of this paper is organized as follows. In section 2 describe about Methodologies section 3 explains the Experimental setup and section 4 Concludes the paper.

II. METHODOLOGIES

ALGORITHM OF THE PROPOSED METHOD

1. Get the input color image

2. Encrypt the image using DES Algorithm

3. The encrypted color image is downsampled to create sub images

4. Each sub images is encoded by using Huffman and arithmetic coder

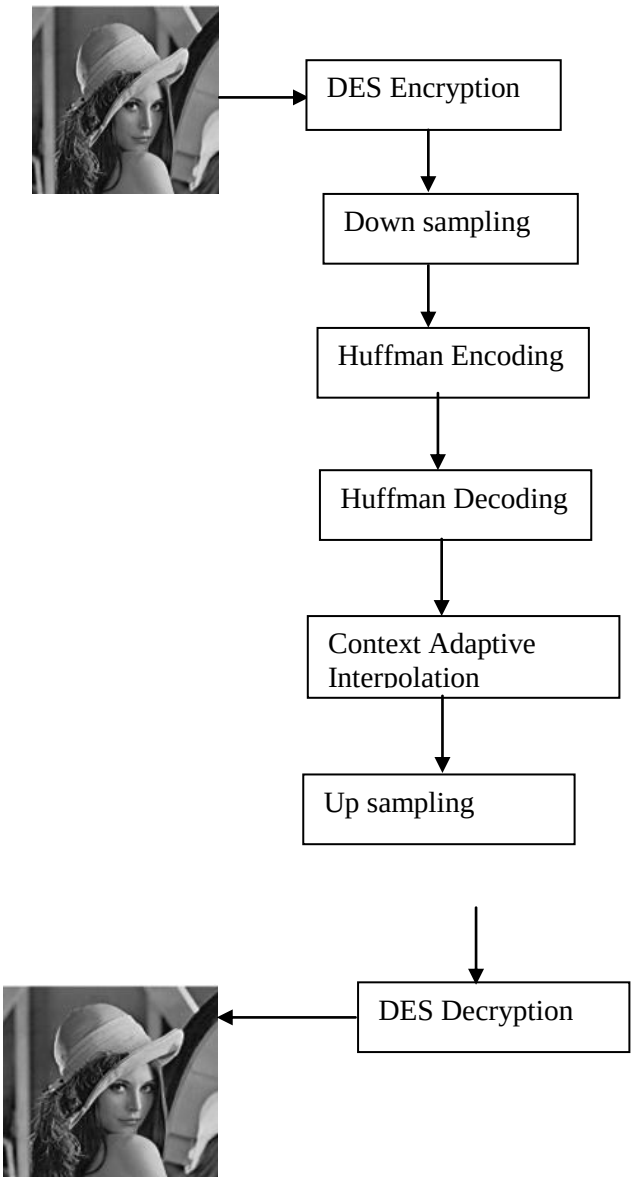
5. The decoding starts from the lower level of the sub images

6. The remaining sub images in the same level is extracted by using the Context adaptive interpolation technique

7. All the sub images are combined to get the compressed image

8. Finally the compressed image is decrypted by using the DES algorithm

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)



DES Encryption:The first module of this project is DES Encryption. DES is the most popular symmetric key encryption method. It is based on research by IBM Standardized by the USA government in 1977.

Complex series of bit substitutions, permutations and re-combinations. Basic DES: 56-bit keys. Crackable in hours using specialized hardware Triple DES: effective 112-bit ke. Three stages of encryption with two keys.Uncrackable by known techniques. Block = 64 bits. Key = 56 bits. In this project the input image is first encrypted using DES.

Down sampling the Encrypted Image: The second module of this project is applying down sampling the encrypted images. The encoder gets the ciphertext Y and decomposes it into four subimages, namely, the 00, 01, 10, and 11 sub-images. Each sub-image is a downsampled-by-two version of the encrypted image. The name of a sub-image denotes the horizontal and vertical offsets of the downsampling. The 00 sub-image is further downsampled to create multiple resolution levels. This project use 00n to represent the 00 sub- image in the n– th resolution level.The 00n sub-image can be losslessly synthesized from the 00n+1, 01n+1, 10n+1 and 11n+1 sub-images.

Huffman encoding and decoding: The third module of this project is to apply the Huffman encoder and decoder. In 1951, David Huffman and his MIT information theory classmates gave the choice of a term paper or a final exam. Huffman hit upon the idea of using a frequency-sorted binary tree and quickly proved this method the most efficient In doing so, the student outdid his professor, who had worked with information theory inventor Claude Shannon to develop a similar code. Huffman built the tree from the bottom up instead of from the top down. Take the two least probable values in the image (longest codewords, equal length, differing in last values).Combine these two values into a single value, and repeat.

Context Adaptive Interpolation : The fourth module of this project is to apply the context adaptive interpolation. First, sub-image 11 is interpolated from sub- image 00. After sub-image 11 is decoded, this method uses both 00 and 11 to interpolate 01 and 10. Let be the pixel value to be interpolated, T=[t1,t2,t3,t4]T' be the vector of neighboring. The interpolator classifies the local region into four types: smooth, horizontally-edged, vertically-edged and other

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

In smooth regions, a mean filter is applied; in horizontally/vertically edged regions, the interpolation is done along the edge Otherwise this method use a median filter.

DES Decryption : The last module of this project is decrypting the compressed image. To decrypt the image DES algorithm is used. After completing this module the compressed image is got.

III. Experimental Results

A. *Peak Signal-to-Noise-Ratio*

We use the peak signal-to-noise ratio (PSNR) to evaluate the quality between the attacked image and the original image. The PSNR formula is defined as follows:

$$PSNR=10x\log_{10}$$

B. *Compression Ratio*

We use the Compression Ratio (CR) to find the how many number of bits are compressed by using the compression algorithm. The CR formula is defined as follows:

CR= (Number of compressed bits/total number of bits)*100

The PSNR and CR values for the various compressed images are calculated by using the proposed algorithm. The result is given below.

	3 Level Decomposition		5 Level Decomposition	
	PSNR Value	Compression Value	PSNR Value	Compression Value
Lena	54.25	32.14	52.19	35.20
Pepper	51.87	31.38	49.28	34.52
Boat	49.72	32.67	46.21	28.30
Baboon	56.89	34.56	52.16	30.32

TABLE I Performance Analysis of the Proposed Method

	Arithmetic Coding		Huffman Coding	
	PSNR Value	Compression Ratio Value	PSNR Value	Compression Ratio Value
Lena	50.15	26.22	54.25	32.14
Pepper	46.26	27.13	51.87	31.38
Boat	45.15	28.17	49.72	32.67
Baboon	53.82	30.12	56.89	34.56

In the above table the PSNR and CR values for the various images of the RPC are given. From the above table it is shown that PSNR and Compression value is higher for Huffman Coding Algorithm.

The PSNR and CR analysis of the RPC based compression is shown in below figure.

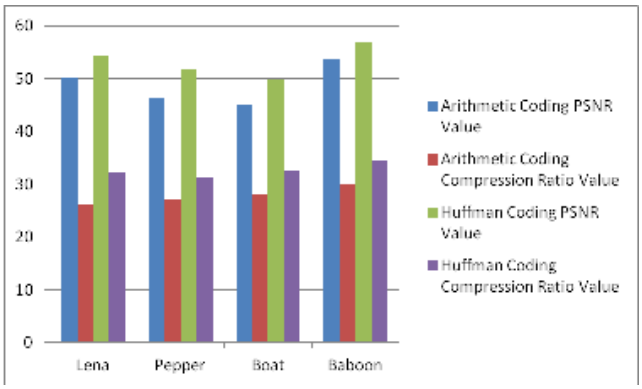


Fig..1 Performance Analysis of Color Images

The PSNR and CR values for the various compressed images are calculated by using the proposed algorithm. The result is given below.

TABLE II Performance Analysis of the Huffman Encoding Algorithm

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

In the above table the PSNR and CR values for the various images of the RPC are given. From the above table it is shown that PSNR and Compression value is higher for Huffman Coding Algorithm.

The PSNR and CR analysis of the RPC based compression is shown in below figure.

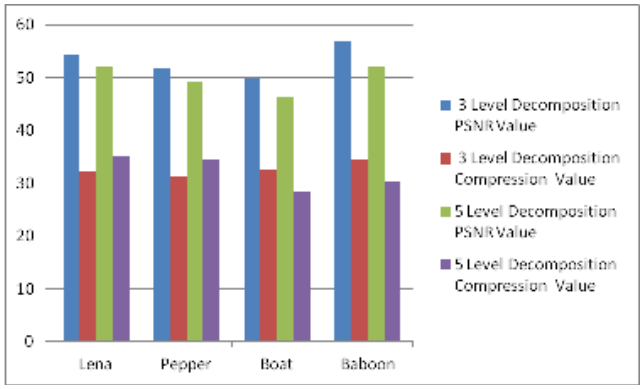


Fig..2 Performance Analysis of Color Images

IV. CONCLUSION

In this system, a robust location fingerprint and the SSD are defined, which provides a more robust Location signature. SSD based localization algorithms outperform the traditional RSS fingerprints, as well as several other techniques that are designed to mitigate the effects of hardware. The SSD based localization is more effective and find out the accurate locations. In the existing method,the RSS value is calculated and is matched with that of the data set and then locates the required place.The location is identified using Received Signal Strength (RSS) and Signal Strength Difference (SSD) .Then the performance of the two techniques is compared.In future following can be considered :The location of a mobile device can be determined based on thestrength of the signal from the Access point to which it is connected. The range of each access point can be determined with the distance between the access points within an organization or institution.

V. REFERENCES

[1]Battiti.R, M. Brunato, and A. Villani, "Statistical learning theory for location fingerprinting in wireless LANs," Universitadi Trento, Dipartimento di Informatica e Telecomunicazioni, Tech. Rep. DIT-02-0086, Oct. 2002.

[2]Chang.C and A. Sahai, "Estimation bounds for localization," in Proc. IEEE SECON'04, Oct. 2004, pp. 415–424.

[3] E. Elnahrawy, X. Li and and R. P. Martin, "The limits of localization using signal strength: A comparative study," in IEEE SECON, Santa Clara, CA, 2004.

[4] Kaemarungsi.K and P. Krishnamurthy, "Properties of indoor received signal strength for WLAN location fingerprinting," in Proc. MobiQuitous'04, San Diego, CA, 2004, pp. 14–23.

[5] Ladd.A, K. Bekris, G. Marceau, A. Rudys, L. Kavraki, and D. Wallach, "Robotics-based location sensing using wireless ethernet," Department of Computer Science, Rice University, Tech. Rep. TR02-393, 2002.

[6]MahtabHossain.M.K.A, Yunye Jin, Wee-SengSoh, and Hien Nguyen Van," SSD: A Robust RF Location Fingerprint Addressing Mobile Devices Heterogeneity" 1536-1233/11/$26.00 2011 IEEE Trans.

[7]Li.X, "RSS-based location estimation with unknown pathloss model," IEEE Trans. Wireless Communications, vol. 5, no. 12, pp. 3626–3633.

[8] Roos.T, P. Myllymki, H. Tirri, P. Misikangas, and J. Sievnen, "A probabilistic approach to wlan user location estimation,"International Journal of Wireless Information Networks, vol. 9, pp. 155–164, 2002.

[9] Want.R, A. Hopper, V. Falc˜*a*o, and J. Gibbons, "The active badge location system," ACM Trans. on Information Systems,vol. 10, no. 1, pp. 91–102, Jan. 1992.