Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 3 (2016) 6 - 10. Submitted 1/08/2016. Published 19/08/2016

IMAGE COMPRESSION AND ENCRYPTION SCHEME USING JULIA SET AND FRACTAL DICTIONARY

[1]V. Yuvarani, [2]Ms. M.Anita Madona,
[1]M.Phil Scholar, Dept of Computer science, Auxilium College, Vellore,
[2]Asst prof, Dept of Computer science, Auxilium College, Vellore.

Abstract:

The image encryption is to transmit the image securely over the network so that no unauthorized user can decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging, tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful to protect secret information. Encryption will be defined as the conversion of plain image into a form called a cipher text that cannot be read by any people without decrypting the encrypted image. Image is initially encrypted into unreadable format is through either auto keying or manual keying. And the encrypted image is compressed in order to reduce the storage size of the image. Entire process is achieved through the Fractal and Julia Set algorithm.

Keywords : Tele-medicine, Encryption, Manual keying, Fractal.

1. INTRODUCTION

The two main problem thatarise in image encryption process with respect to the storage and its security level for real time image encryption for ciphers are preferable to take lesser amount of computational time without compromising security. An encryption scheme which runs very slowly, even though may have degree of security features would be of little practical use for real time processes. Many encryption methods have been used to encrypt the image, and the most common way to protect large multimedia files is by using conventional encryption techniques. Private Key bulk encryption algorithms, such as Triple DES are not suitable for transmission of large amounts of data, such as images. Due to the complexity of theirin ternal structure, they are not particularly fast in terms of execution speed and cannot be applied for images in the real time scenario. Also traditional cryptographic techniques such as DES cannot be applied to images due to intrinsic properties of images such as bulky data capacity, redundancy and high correlation among pixels. Images encryption algorithms can become an integral part of the image delivery process if they aim towards efficiency and at the same time preserve the security level. **Fractal Dictionary is an** image compression technique based on splitting an image into parts that can each be represented by fractal.The representation of an image by a fractal consists of finding an image transformation that, when applied iteratively to any initial image at the decoder, produces a sequence of images that converges to a fractal approximation of the original. Essentially the encoding of the image is then an encoding of the transformation for each part of the image parts, and a description of the decomposition into parts. Fractal compression is computationally intensive. It has the ability to render images that appear lossless at one extreme and on the other hand the compressed images can be very small in size still producing recognizable images.

2. LITERATURE REVIEW

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. Cryptography is most often associated with scrambling plaintext into cipher text (a process called encryption), then back again (known as decryption). The sender and receiver can confirm each other's identity and the origin/destination of the information .Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders. Cryptography is the science of writing in secret code and is an ancient art; when an Egyptian scribe used non-standard hieroglyphs in an inscription. In cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. While using a network transmission, every person either in an organization or at home wants to protect his/her information for the sake of confidentiality of their information. For that purpose, protocol steganographyis used. The information is encoded and network control protocol like TCP/IP protocol is used for the transmission purpose over the network.

3. NARRATIVE OF CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

The fractal dictionary-based encoding is adopted in this scheme to overcome the high encoding computation burden. Then, the Julia set is converted to a stream cipher and encoded with the compressed data before diffusion process. Iterated function systems are introduced as a unified way of generating a broad class of fractals that contains classical Cantor sets, Sierpinski gaskets, Julia sets and much more. Many of these sets are traditionally viewed as being produced by a process of successive microscopic refinement taken to the limit. The classical Julia set is a product of several iterations by a mapping function $f(z) = z_2 + c$. Since the complex number $z = x + iy$ can be uniquely mapped to (x, y) in real number space, a one-to-one relationship can be established between the complex number space and the real number space. In practice, we select an area in complex plane and map it to a screen area Won the computer screen where one pixel is related to a point z_0 in Julia set. The Julia set is constructed by the time-escaped algorithm, which is described as follows. Pixel value swapping is the second type of encryption applied on intensity varied image.

Fig.1. Input Image

Input Image is divided into 4 blocks b1, b2, b3 and b4. During implementation of this algorithm, the exact pixel position where last swap has been done has to be saved, since pixels are accessed sequentially. After the pixels in b1 are swapped completely, process moves ahead to b2, where swapping is continued from the position which underwent last swapping with b1. Same procedure is applied for b3. This procedure is not repeated for b4 since it contains pixels from b1, b2 and b3.

Fig.2.Original image

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. One of the foremost reasons for implementing an encryption-decryption system is privacy.

As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized individuals or organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories.

4. RESULT ANALYSIS

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codes for image compression. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codes, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same code. The PSNR Value of below selected image is 88.0554.

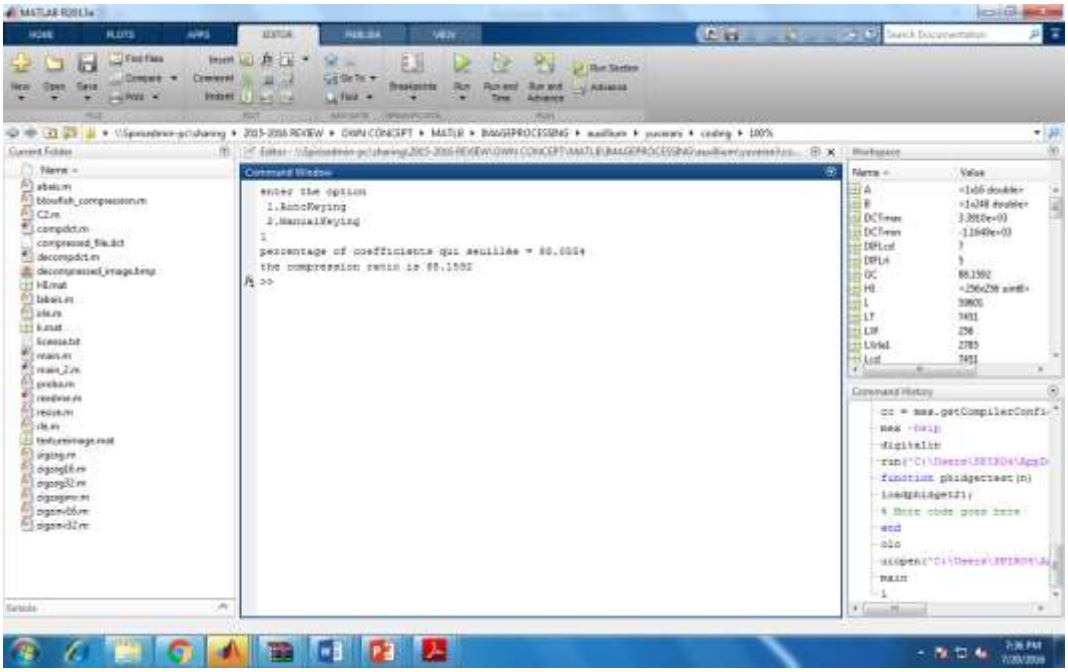

Fig.3. Compression Ratio

CONCLUSION

This proposed a novel compression scheme based on the Fractal Dictionary and Julia Set. In this scheme, the image compression is based on the Fractal Dictionary not only to save time consumption, but also to give a good quality of image reconstruction with a satisfying PSNR.Fractal Dictionary suffer from

the fact that the uncompressed or need have some knowledge of the probabilities of the symbols in the compressed files that needs more bits to encode the file This work may be extended the better compression rate than other compression techniques. This method of fractal image coding based on a fractal dictionary, consisting of rich domain blocks generating from J sets. An image range block can be matched with the best- matching block in the dictionary by less comparison without losing the reconstruction quality.

REFERENCES

1. Ahmed, F., Siyal, M.Y., Abbas, V.U.: "A perceptually scalable and jpeg compression tolerant image encryption scheme". 2010 Fourth Pacific-Rim Symp. On Image and Video Technology (PSIVT), IEEE, 2010, pp. 232–238
2. Yuen, C.H., Wong, K.W.: "A chaos-based joint image compression and encryption scheme using DCT and SHA-1", Appl. Soft Comput., 2011,
11, (8), pp. 5092–5098
3. Hermassi, H., Rhouma, R., Belghith, S.: "Joint compression and encryption using chaotically mutated Huffman trees", Commun. Nonlinear Sci. Numer. Simul., 2010, 15, (10), pp. 2987–2999
4. Bourbakis, N.G.: "Image data compression-encryption using G-scan patterns". IEEE Int. Conf. on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation, IEEE, 1997, no. 2, pp. 1117–1120
5. Lian, S., Chen, X., Ye, D.: "Secure fractal image coding based on fractal parameter encryption", Fractals, 2009, 17, (02), pp. 149–160
6. Lock, A.J.J., Loh, C.H., Juhari, S.H., Samsudin, A.:Compression-encryption based on fractal geometric'. 2010 Second Int. Conf. on Computer Research and Development, IEEE, 2010, pp. 213–217
7. Barnsley, M.F., Demko, S.: 'Iterated function systems and the global construction of fractals', Proc. R. Soc. Lond. A, Math. Phys. Sci.,1985, 399, (1817), pp. 243–275