A New Technique for Image Encryption using RIJNDAEL Block Cipher Algorithms

J. Mahalakshmi
Research Scholar

K.Kuppusamy
Associate Professor

Dept of Computer Science& Engg
Alagappa University
Karaikudi

ABSTRACT
Visual Encryption is most important in transferring image through the communication networks to protect it against reading, alternation of its content, adding false information or deleting part of its content. The block cipher Rijndael algorithm is used to encrypt and decrypt an image with a variable block length, and a variable key length. This paper focused on the quality measurements such as the speed, Encryption Ratio, Correlation Coefficient, Visual Degradation, and Compression Friendliness of the JPEG image encryption with the existing bitmap image encryption. Since, the JPEG files are of compressed format, the compression friendliness is measured here. The result ends with the comparison of performance parameters, based on the type of file formats.

General Terms
Algorithms.

Keywords
Visual Encryption, Block Cipher Encryption, JPEG, Encryption Ratio, Compression Friendliness**.**

1. INTRODUCTION
Network Security is becoming more and more crucial as the volume of data being exchanged on the internet access. Based on the above, the security involves four important aspects: Confidentiality, message authentication, integrity and non – repudiation. Popular application of multimedia technology, and increasingly transmission ability of network gradually leads us to acquire, information directly and clearly through images [7]. Hence, image security has become a critical and imperative issue [8]. Cryptography is the process of transforming information (plain text/Image) into unintelligible form (Cipher text/ Image). The technology of encryption is called cryptology. In the image encryption the AES algorithm is used to encrypt and decrypt the image, because it is considered as a better solution for image encryption [1] and their performance parameters are analyzed. The Rijndael algorithm is used, because of its simplicity, efficient working syntax [11]. Since, AES algorithm is specified, substitution ciphers are used to encrypt the image input. Image encryption techniques, will convert an image into another unreadable form, where at another end decryption receives original image by applying the same key used at the encryption process.

Symmetric key transmission is used in this paper for the image encryption. Hence at both ends, same key is used to encrypt and decrypt information. The quality of the encrypted images is tested with different quality factors.

The paper is organized as follows: section 2 will briefly discuss about the related works done about the paper and the existing bitmap image encryption. Section 3 will discuss the JPEG image compression and encryption of the image. Section 4 discusses the various performance factors that are used as the quality measurements. The result of the paper appears in section 5 with experimental results. Paper is concluded in section 6.

2. RELATED WORK
This section gives a brief overview on the related work done on the bitmap image encryption and its performance parameters. Moreover, the encryption algorithms used for image encryption is discussed.

Visual encryption is important in transferring the images through communication networks to protect it, against malicious attacks. Neil F. Johnson and Sushil Jajodia et al. have provided several Characteristics in information hiding methods to identify the existence of hidden messages and also identify the hidden information [10].

Lisa M.Marel and Charles T. Retterhave presented a method of embedding information within digital images [6]. A hidden message can be recovered by using appropriate keys without any knowledge of the original image. Giuseppe mastronardi et al., have studied the effects of steganography in different images formats (BMP, GIF, JPEG) [3].

In the paper proposed by Nawal El-Fishaway and osama M.Abu Zaid the quality of the encryption parameters are discussed [9].H.Elkam Chouchi and M.A.Markar proposed the measurement of the quality of the bitmap images using the Rijndael and kamkar block cipher algorithms [2].

M.Van Droogenbroeck and R. Benedett, have proposed the various techniques and methods used for the encryption of compressed and uncompressed images [13].I.Venkata Saj Manoj in his paper proposed the various method and the techniques used in the steganography and the cryptography.

2.2 Bitmap Image Encryption

Bitmap (bmp), images are type of uncompressed image format, which can be break down into pixel values as matrix [12]. The encryption of image has two inputs – one is the plain text (Image data) and the encryption key. To encrypt an image, its header should be excluded and start of the bitmap's pixels or arrays begins right after header of file. The rows of images are encrypted from top to bottom. Rijndael algorithm is applied for image encryption, since it is better than RC6, MRC6 algorithm images in the sense of little high frequency components.

The following results show how the encryption of the image is taken place. The Figure -1 is the cover image in which the encrypted image is to be hided. The key generation is next taken place by using the AES standard. After key scheduling, the image is now encrypted and it is now in the scrambled format. Then the scrambled format is now enveloped within the cover image. At the receiving end the receiver when inputs the right key for decryption the original image will be fed as output else if the inputted key is the false input then the encrypted file could not be opened and again over encrypted. The figure -2 shows the image with the encrypted output.

Figure -1 **Figure -2**

Original Image **Encrypted Image**

3. RESEARCH CONTRIBUTION

3.1 JPEG Image Encryption

JPEG is commonly used method for lossy compression technique. JPEG stands for Joint Photographic Experts Group. The degree of compression can be adjusted, allowing selectable tradeoffs, between storage size and image quality. JPEG achieves compression with little perceptible loss in image quality [5]. A JPEG image consists of the sequence of segments each beginning with a marker, each of which begins with 0XFF, followed by the byte indicating what kind of marker it is. Before encryption is done, the compression of image should taken place. The compression scheme is divided into the following stages:

a) Transform the image into an optimal colour space.
b) Down sample the chrominance components by averaging groups of pixels together.
c) Apply Discrete Cosine Transformation technique to blocks of pixels, thus remove redundant data.
d) Quantize each block of DCT coefficients using weighting functions optimized for human eye.
e) Finally, encoding the resulting coefficients (Image Data) with Huffman variable word – length algorithm to remove redundancies in the coefficients.

3.2 JPEG Codec

a) The representation of colors in the image is converted from RGB to Y'CBCR consisting of one luma component, (Y'), representing brightness, and two chroma components (CB, CR) representing colors.

b) The resolution of chroma data is reduced, usually by factor 2 that reflects the fact that the eye is less sensitive, to fine color details than to fine brightness details.

c) The image is split into blocks of 8*8 pixels, and for each block, each of the Y, CB, CR data undergoes a DCT. DCT produces a kind of spatial frequency domain.

d) The amplitude of the frequency components is quantized. Therefore, the magnitudes of the high frequency components are stored with a lower accuracy than low – frequency components.

e) The resulting data for all 8* 8 blocks is further compressed with lossless algorithm, a variant of Huffman coding.

The decoding process reverses, these steps, except the quantization because it is irreversible. This compression is more efficient, because it is confined into a single channel. The encryption of image is done after this compression using AES Rijndael, as same as for the bitmap image. Then, the decryption process is followed by decompression of Image.

In the JPEG image encryption the image to be encrypted should be compressed first and then they will be encrypted. The following images show the image encryption in the JPEG format. As same in the case of the bitmap file encryption, Figure-1 is the first image file in which the data has to be hiding. The final figure – 2 is the final encrypted image of both the JPEG files.

3.3 Procedure for JPEG Image Encryption

The procedure for the image encryption involves both the encryption and the compression. The algorithm is as follows:

a) Select a Figure - 1, which is in the JPEG format.
b) For JPEG Image compression, the Discrete Cosine Transformation (DCT) technique is used, which is one of the lossless compression technique.
c) The pixel values are calculated for their compression.
d) After compressing the Figure - 1, select the Figure - 2, which is to be encrypted.
e) Repeat the steps b and c, so that the Figure - 2 is also get compressed that can be placed within the parental Figure - 1.Finally, using the AES standard algorithm, encrypt the Image.

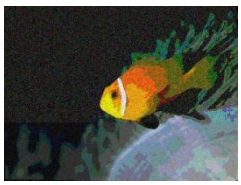

Figure -1 **Figure -2**

Original Image **Encrypted Image**

4. PERFORMANCE PARAMETERS

In this paper, the set of criteria for comparing the existing bitmap file encryption, with the JPEG (Joint Photographic Experts Group) file encryption, where the bitmap file is the uncompressed file while the JPEG file is the compressed format is as follows: Encryption Ratio, Speed, Correlation Coefficient, Compression Friendliness, and Visual Degradation.

4.1 Encryption Ratio

The encryption ratio is the measure of amount of data that is to be encrypted. Encryption ratio has to be minimized to reduce the complexity on computation.

4.2 Visual Degradation

The visual degradation, will measures the distortion of the image data with respect to plain image. For, highly sensitive data, high visual degradation could be desirable to completely disguise the visual content.

4.3 Correlation coefficient

The statistical analysis, as the correlation coefficient is one of the factor that is used to measure the relationship between two variables; the image and its encrypted format. This factor gives the information about the statistical attacks.

4.4 Compression Friendliness

An encryption is said to be compression friendly, if it has no or very little impact on data compression efficiently. It is desirable that size of encrypted data should not increase.

4.5 speed

In case of real – time applications, it is important that both the encryption and decryption should be done fast, to meet real time requirements.

5. RESULTS AND DISCUSSIONS

This section presents performance and comparison among Bitmap image and a JPEG image with respect to various parameters. We can specify the visual degradation, by either high or low. The compression friendliness of JPEG image is measured in, whether it is accepted or not as yes or no. The encryption ratio is measured in terms of percentage. The correlation coefficient is measured by following equation,

$$C.C\ E(x) = \frac{1}{N}\sum_{i=0}^{N} xi$$

$$C.C = \frac{\sum_{i=0}^{n}(Xi - E(x))\,(Yi - E(y))}{\sqrt{\sum_{i=0}^{n}(Xi - E(x))}\sqrt{\sum_{i=0}^{n}(Yi - E(y))}}$$

Where X, Y are the pixel values of the original and encrypted images. The speed is defined by the following term such as fast, slow, moderate. The following table shows the performance parameters and their comparison among the image encryption of the Bitmap image and the JPEG encryption.

Table 1.Performance Evaluation of the Bitmap and JPEG Image Encryption

Parameters Analysed	**Bitmap Image Encryption**	**JPEG Image Encryption**
Encryption Ratio	50- 60 %	92%
Visual Degradation	High	High
Corelation Coefficient	1.00281	1.014455
Speed	Fast	Variable
Compression Friendliness	No Compression	Yes

6. CONCLUSION

We have analyzed and compared both the performance parameters of existing bitmap image encryption with the JPEG image encryption. We analyze, these with respect to various parameters listed in table 1. For both the Bitmap as well as the JPEG image the visual degradation is high because distortion of the plain image is completely immersed with the image to be encrypted in the jpeg file after compression.

The Speed of the bitmap file fast since it can hold about 1024 KB file size and can be exactly encrypted and saved in the file size of about 1115 KB file. As in the case of the Jpeg image the speed will be variable because the size of the image will be vary after the compression technique employed. Hence the speed cannot be as much as the bitmap image encryption. The compression friendliness is acquired in the JPEG file compression since the deviation is very low. Comparing the encryption ratio the JPEG image has the higher encryption ratio than the bitmap image, since it can compress and then encrypted. The correlation coefficient is low in the bitmap image hence the deviation is low in the bitmap image encryption. We can conclude that the quality of the Image encryption is highly possible in the JPEG image encryption with high compression friendliness and with higher encryption ratio and with the bitmap image the encryption is highly secured with the speed and visual degradation. Hence for higher data encryption or multimedia encryption the compressed format can be applied and it yields higher encryption ratio.

7. ACKNOWLEDGMENTS

The first author likes to thank Dr. K.Kuppusamy for his valuable suggestions and guidance given round the clock to complete the task successfully. Eventually the first author thanks to IJCA for introducing this article through its publication to the research world.

8. REFERENCES

[1] B. Gladman, "A Specification for Rijndael, the AES algorithm",May 2003, http://fp.gladman.plus.com/Cryptography_technology/rijndeal/aes.spec.311.pdf.

[2]H.Elkam Chouchi and M.A.Makar, "Measuring Encryption Quality of Bitmap Images Encrypted with Rijndael and Kamkar block ciphers", Twenty Second National Radio Science Conference CNRS(2005), PP.C11, Cairo, Egypt, March 15-17, 2005.

[3]Giuseppe Mastronardi, Marcello Castellano, Francescomaria Marino, "Steganography Effects in Various Formats of Images. A Preliminary Study," International Workshop on Intelligent dataAcquisition and Advanced Computing Systems: Technology and Applications, pp. 116-119, 2001

[4] Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Images and videos", "IEEE Transaction on Signal Processing", Vol.48, No.8, August 2000, PP 2439-2451.

[5] S.Lian,"Multimedia Content Encryption: Techniques and Applications", CRC, 2008.

[6] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE conference on Military

communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[7] J.W. Lee, T.Chen and C.Chien Lee, "Improvement of an Image encryption scheme for binary Images", Pakistan Journal of Information and Technology, Vol.2, no.2,2003 PP.191-200.

[8] A.Mitra, Y.V.SubbaRao and S.R.M. Prasanna, "A new image encryption approach using, combinational permutation techniques", Journal of computer Science, Vol.1, no.1, 2006, PP 127.

[9] Nawal El –Fishaway, And Osama M.Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms", in International Journal of Network Security, Vol.5, No.3, PP.241-251, Nov 2007.

[10] Neil F. Johnson and Sushil Jajodia,1998,, "Steganalysis: The Investigation of Hidden Information," IEEEconference on Information Technology, pp. 113-116, 1998

[11] I.Ozturk and I.Sogukpmar, "Analysis and Comparision of Image encryption Algorithms", Transactions on Engineering, Computing and Technology, Vol.3, PP.1305-1313, 2004

[12] V. Potdar and E.chang, "Disguising text cryptography using Image cryptography", International Network Conference in plumouth , UK, 6-9, July, 2004.

[13] M.Van Droogenbroeck and R.Benedett, "Techniques for a Selective encryption of uncompressed and compressed images", in proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) Ghent, Belgium, September 9-11, 2002, PP.90-97.