ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Applying Security through Selective Image Encryption for Compressed Images Using DCT and RC6 Block Cipher

Anshu Devangan [1], Omprakash Dewangan [2]

M.Tech Student, Department of Computer Science, Rungta College of Engineering and Technology, Bhilai, Chattisgarh, India[1]

Assistant Professor, Department of Computer Science, Rungta College of Engineering and Technology, Bhilai, Chattisgarh, India[2]

ABSTRACT: Nowadays internet is a global medium to transfer the data over communication channel. Rich growth of multimedia application in the internet is the motivation for researchers to contribute in the area of multimedia data security. Various cryptographic techniques can be applied to secure the simplest form of multimedia data (text data) but not appropriate for multimedia data having large file size. Selective encryption is a mechanism to effectively increase the fastness of transmission and to decrease the computational requirements for large amount of multimedia data. In this paper, we have proposed new mechanism for security of compressed images using RC6 cryptographic algorithm together with selective image encryption. Selection of image parts is based on AC and DC coefficients of DCT applying in the whole image. After analysing we conclude that our system is strong against statistical attacks.

KEYWORDS: Selective image encryption, JPEG, Cryptography, DES, AES.

I. INTRODUCTION

In the field of cryptography, secure image transfer is achieved by using strong encryption techniques like DES, 3DES, AES and many more. The encryption of full image using these techniques is complex and time consuming. An effective recent trend is to minimize the computational complexity for securing multimedia data is called selective encryption where only selected parts of the data are encrypted. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet provides a secure transmission. Selective encryption approach reduces the overhead of encrypting the non-sensitive areas [15]. This technique is very useful to protect the most important parts of images like the face or other sensitive information carrying parts like medical images.

Majority of traditional algorithms are basically used for encryption of text data; however they do not fit for the multimedia data particularly images due to their huge size. Furthermore, decrypted text result should be similar to the original text, while decrypted image is not required to be similar with original image. Image encryption algorithms can be categorized into full encryption and partial encryption (also called selective encryption) based on the sum of encrypted data. According to the percentage of the encrypted data, unfortunately, the time for processing of encryption and decryption is the main concern in real-time image communication. Time can be categorized into two levels, one for encryption time and another for time for transferring images. The first step is to choose a robust, fast and easy method to implement in order to reduce the time. Encryption and decryption algorithms are not fast enough to deal with the enormous amount of transmitted data. A significant criteria relating to the method is to decrease the image encryption size and maintain quality of the image. Partial Encryption is a suitable method to encrypt only the lowest portion of data to lessen the computational requirements of enormous amounts of multimedia data [11]. On the other hand, the traditional full encryption algorithms are used to completely encrypt an image and treat all bits similarly; it has greater computational complexity than partial encryption. Furthermore, it takes more time in comparison with partial

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

encryption. Selective encryption is a technique to save computational power, overhead, speed, time and to provide quick security. Therefore, multimedia data needs either a full or selective encryption according to requirements of the application. For instance, applications of military and law enforcement need full encryption. Nevertheless, there is a range of spectrum applications that require lower security levels, as in medical images that are attained by partial encryption [4][14]. In the region based selective encryption, selection of region of interest is done manually or automatically based on the application [6]. Furthermore, the automatic selection can be of two types; block selection or pixel selection [18]. Selective encryption scheme generate the key before starting the process of encryption and decryption, rather than storing it. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately [3].

The DCT transform the data from the spatial domain to the frequency domain. The spatial domain can give us an idea about the amplitude of the color as we move through space. The frequency domain explains that the amplitude of the color is varying fast from one pixel to the other pixel in an image data [9]. DCT separates images into parts of different frequencies where less important frequencies are discarded through quantization and important frequencies are used to retrieve the image during decompression. DCT is primarily a lossy method of compression. It was designed specifically to discard the information that the human eye cannot easily see. Slight changes in color are not perceived well by the human eye, while slight changes in intensity (light and dark) are [7].

$$F(u,v) = \frac{2}{N} C(u) C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi (2x+1) u}{2N}\right] \cos\left[\frac{\pi (2y+1) v}{2N}\right]$$

for $u = 0, \ldots, N-1$ and $v = 0, \ldots, N-1$

where $N = 8$ and $C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$

Fig. 1. The Forward 2D-DCT Transformation.

The image is divided into $N \times N$ pixel blocks and 2D-DCT is applied to each. After DCT transformation, the "DC coefficient" is the element in the upper most left corresponding to (0, 0) and the rest coefficients are called "AC coefficients [8]. Figure 1 shows the general equation for 2D-DCT where F(u,v) denotes the DCT coefficient in any particular row and column of the DCT matrix.

$$f(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u) C(v) F(u,v) \cos\left[\frac{\pi (2x+1) u}{2N}\right] \cos\left[\frac{\pi (2y+1) v}{2N}\right]$$

for $x = 0, \ldots, N-1$ and $y = 0, \ldots, N-1$ where $N = 8$

Fig. 2. The Inverse 2D-DCT Transformation.

The equation for inverse 2D-DCT is shown in figure 2 which is simply $F^{-1}(u,v)$. Compared to other input dependent transforms, DCT has many advantages [7]:

1. It has been implemented in single integrated circuit.
2. It has the ability to pack most information in fewest coefficients.
3. It minimizes the block like appearance called blocking artifact that results when boundaries between sub-images become visible.
4. It is widely accepted standard by Joint Photographic Experts Group (JPEG), a standards committee that had its origins within the International Standard Organization (ISO).

The majority of the selective encryption schemes encrypt a selected number of DC or AC coefficients for JPEG images, when the image is transformed into the frequency domain using discrete cosine transform [17]. In JPEG compressed images, there are many techniques that were developed to encrypt parts of JPEG compressed images. One technique

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

suggested encrypting some of the Discrete Cosine Transform (DCT) coefficients in each N×N blocks. The first value of the DCT coefficients matrix is called the DC coefficient, and the rest are called AC coefficients. The unencrypted high-frequency coefficients provide little information about the original N×N blocks. However, when the image blocks are considered together, the unencrypted high frequency coefficients often show outlines of objects in the image. An alternative technique is to encrypt the bits that indicate the sign and magnitude of nonzero AC coefficients. Since they are highly predictable, the DC coefficients are left unencrypted [13].

RC6 (Rivest cipher 6) is one of the algorithms of a fully parameterized family of encryption algorithms. RC6 is specified as RC6-w/r/b where w is the word size in bits, r denotes the number of rounds and b denotes the length of the encryption key in bytes. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits.

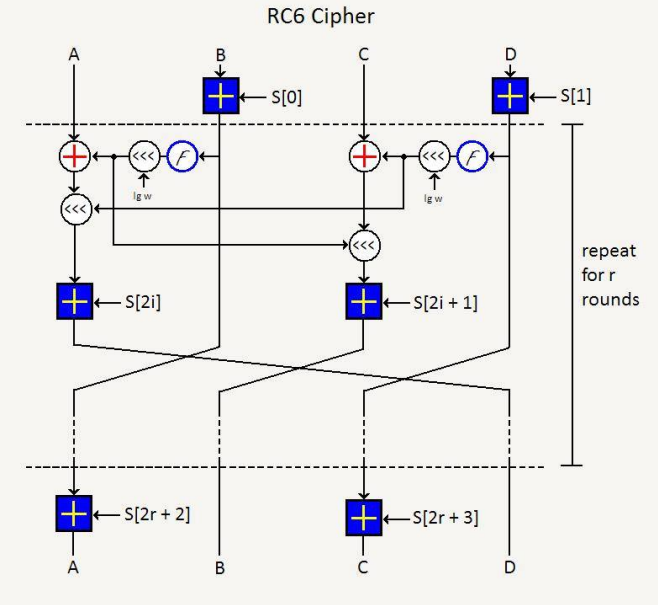

Fig. 3. Working of Standard RC6.

RC6 works with four w-bit registers A, B, C, D which contain the initial input plain-text as well as the output cipher-text at the end of encryption. The first byte of plaintext or cipher-text is placed in the least-significant byte of A, the last byte of plaintext or cipher-text is placed into the most-significant byte of D [10]. The working of standard RC6 algorithm is shown in figure 3.

II. RELATED WORK

In the previous years the existing cryptographic algorithms are used for the selective encryption of compressed images. In this section we are going to discuss some of the recent studies regarding selective image encryption.

Sapna Sasidharan and Jithin R [1] proposed a methodology in the year 2010 in which they used DCT with RC4 stream cipher. They first decomposed the image into 8×8 blocks and DC and some AC coefficients are selected for selective encryption. For better security they used shuffling of blocks. They concluded that their methodology is resistant to statistical attacks because of the different shapes of histograms of encrypted and decrypted images and improves image quality because PSNR values of the different encrypted images are low as compared to the decrypted images.

Belazi Akram, Benrhouma Oussama, Hermassi Houcemeddine and Belghith Safya [13] proposed a methodology in the year 2014 for selective encryption in which they used DCT with AES block cipher. They also use 8×8 image decomposition of original image and selection of DC and some AC coefficients for selective encryption. They performed some statistical experiments and concluded that their methodology is strong enough against attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Priyanka Agrawal and Manisha Rajpoot [14] proposed matrix or grid division method in the year 2012 for selective encryption. The basic idea of their work is selection of image parts by arranging the bit stream in grid form and choosing the diagonal of the grid. They found their work suitable for real time applications because of the properties like uncertain segmentation of multimedia data by reducing the encrypted data volumes and protection of the data in a reasonable computational cost.
Pramod Kumar and Pushpendra Kumar Pateriya [16] proposed their work in the year 2012 in which they used RC4 enrichment algorithm for selective image encryption based on new KSA and PRGA algorithm process, the two stages inside the RC4 algorithm. The result shows that selective image encryption takes less time than the full image encryption and the proposed methodology ensures good security.

III. PROPOSED METHODOLOGY

To enhance the security of image over communication channel RC6 is applied in addition to selective image encryption technique. In the proposed methodology, the original image is first encrypted by selective image encryption using DCT. In DCT, decomposition of the image into blocks is performed first and then the blocks are transformed from the spatial domain to the frequency domain. The DCT block is now scanned in zigzag order from the bottom- left to the top- right for generating the coefficient sequence ordered from the highest frequency to the lowest frequency.

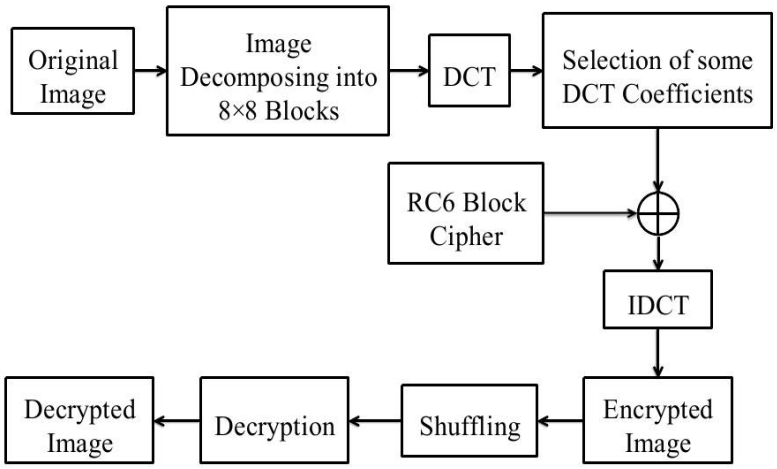

Fig. 4. Block Diagram of Proposed Methodology

The DCT block's energy is denoted by the first coefficient, and rest of the coefficients denotes detailed information in this coefficient sequence. After this we apply the RC6 block cipher in the selected DCT components and we get encrypted image. The original image is recovered by IDCT, shuffling and selective decryption where shuffling is a part of DCT and IDCT. The steps for proposed methodology are shown in figure 4.

IV. EXPERIMENTAL RESULTS

The proposed methodology is implemented using the MATLAB R2012a. The image of lena is used to show the result images in grayscale. However, we can also show the result images in RGB color images. The performance analysis for

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

our proposed methodology is measured using the Histogram Analysis. An image histogram is a representation of tonal variations and the number of pixels in any particular tone.

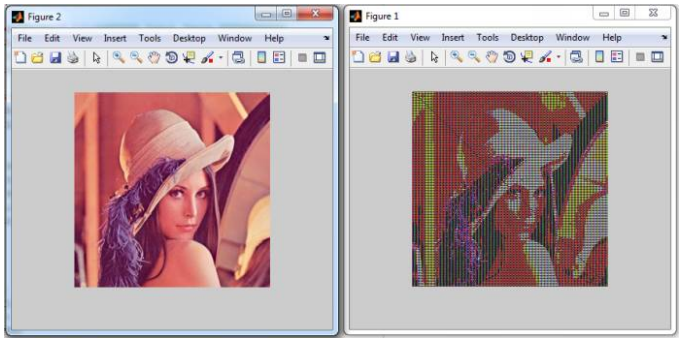

Fig. 5. Selective image encryption.

Figure 5 shows the selective image encryption of our proposed method. The left side image is the original image and the right side image is selectively encrypted image. We are applying the selective image encryption on the whole image. It is clear from the figure that only some parts of image is encrypted and other parts are not encrypted.

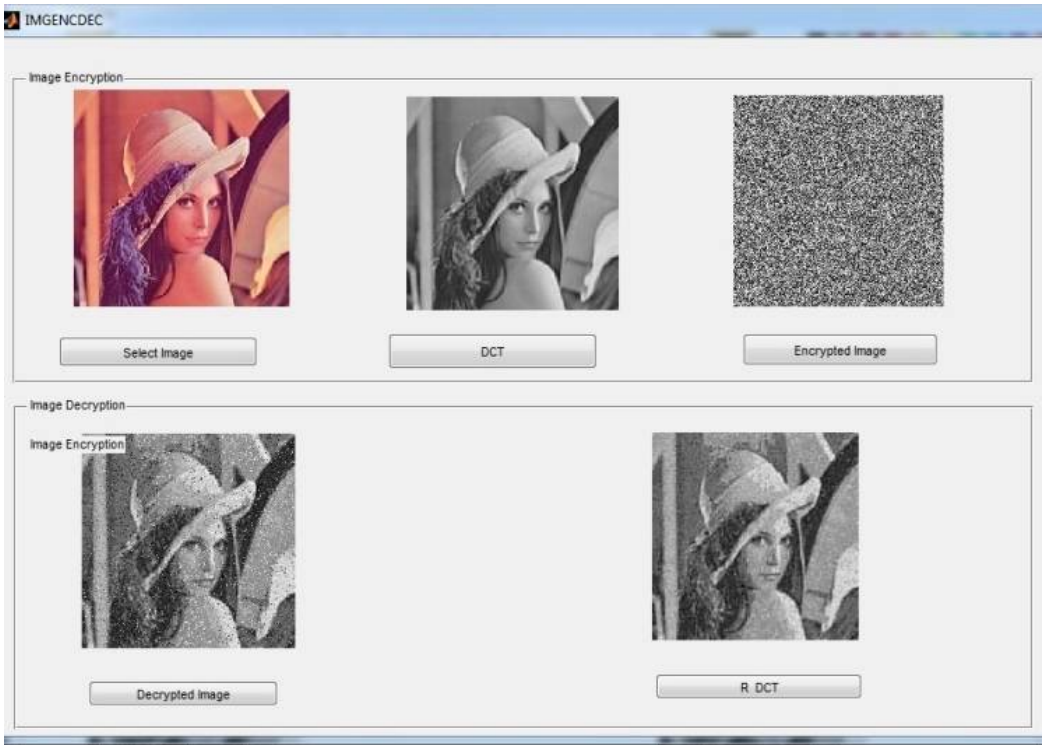

Fig. 6. Experimental Result.

Figure 6 shows the graphical user interface of the proposed method in which five axis and five corresponding buttons are created for original image, transformed image (DCT), encrypted image, reverse transformed image (R DCT) and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

the Decrypted Image. Here image of lena is selected to show the changes in image while pressing the different buttons. The buttons are pressed in an order from top-left to the bottom right.

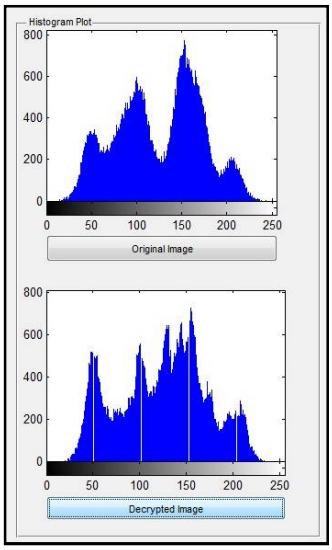

Fig. 7. Histogram plot

The histogram plot between original and decrypted image is shown in figure 7. It is clear that both the histogram plots are different from each other. Histogram analysis is carried out to show that the encrypted image is resistant to statistical attacks.

V. CONCLUSION AND FUTURE WORK

Various efforts have been applied by different authors in the field of selective image encryption of images and different methodologies have their individual merits. But in existing techniques, image encryption ratio is less and provides less security. The proposed methodology is intended to improve the existing encryption algorithms for compressed images. Result of histogram analysis shows the robustness of the methodology against statistical attacks. However, the proposed methodology could still be further improved in certain aspects. For instance, RC6 can be applied with region based selective image encryption like manual selection of region of interest area or multiple selective regions cryptography. Therefore, the future work focuses on applying this methodology with different types of selection criteria of image parts for encryption. DCT is basically a lossy compression technique so our methodology is suitable in the fields where image data loss is acceptable.

REFERENCES

[1] Sapna Sasidharan and Jithin R, "Selective Image Encryption Using DCT with Stream Cipher", International Journal of Computer Science and Information Security, Vol. 8, No. 4, pp. 268-274, 2010.
[2] Jolly Shah and Dr. Vikas Saxena, "Performance Study on Image Encryption Schemes", International Journal of Computer Science Issues, Vol. 8, No. 1, pp. 349-355, 2011.
[3] Abhishek Thakur, Rajesh Kumar, Amandeep Bath and Jitender Sharma, “Design of Selective Encryption Scheme Using Matlab”, International Journal of Electrical & Electronics Engineering, Vol. 1, Issue 1, pp. 14-19, 2014.
[4] W. Puech, A. G. Bors and J. M. Rodrigues, “Protection of Colour Images by Selective Encryption”, in Advanced Color Image Processing and Analysis, Springer, pp. 397-412, 2012.
[5] Upendra Bisht and Shubhashish Goswami, "Analysis and Implementation of Selective Image Encryption Technique Using Matlab", International Organization of Scientific Research-Journal of Computer Engineering, Vol. 16, Issue 3, pp. 108-111, 2014.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

[6] Panduranga H T and NaveenKumar S K, "Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology, Vol. 5, No. 1, pp. 115-121, 2013.
[7] Harish Jindal and Danvir Mandal, "Performance Analysis of Image Compression Using Discrete Cosine Transform with Various Discrete Wavelet Transforms", Journal of Global Research in Computer Sciences, Vol. 3, No.1, pp. 13-16, 2012.
[8] A.M.Raid and W.M.Khedr, "JPEG Image Compression Using Discrete Cosine Transform-A Survey", International Journal of Computer Science & Engineering Survey, Vol. 5, No. 2, pp. 39-47, 2014.
[9] Priyanka dixit and Mayanka dixit, "Study of JPEG Image Compression Technique Using Discrete Cosine Transformation", International Journal of Interdisciplinary Research and Innovations, Vol. 1, Issue 1, pp. 32-35, 2013.
[10] Vikas Tyagi and Shrinivas Singh, "Enhancement of RC6 (RC6_en) Block Cipher Algorithm and Comparison with RC5 and RC6", Journal of Global Research in Computer Science, Vol. 3, No. 4, pp. 39-43, 2012.
[11] Lahieb Mohammed Jawad and Ghazali Bin Sulong, "A Review of Color Image Encryption Techniques", International Journal of Computer Science Issues, Vol. 10, No. 1, pp. 266-275, 2013.
[12] Mahfuzulhoq Chowdhury, Md. Moniruzzaman and Parijat Prashun Purohit, "Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher", International Journal of Grid Distribution Computing, Vol.7, No.3, pp. 189-198, 2014.
[13] Belazi Akram, Benrhouma Oussama, Hermassi Houcemeddine and Belghith Safya, "Selective Image Encryption Using DCT With AES Cipher", Computer Science & Information Technology : Computer Science & Information Technology Conference Proceedings , pp. 69-77, 2014.
[14] Priyanka Agrawal and Manisha Rajpoot, "A Fast and Secure Selective Encryption Scheme using Grid Division Method", International Journal of Computer Applications, Vol. 51, No. 4, pp. 29-33, 2012.
[15] Ms. Pallawi R.Motghare and Dr. Pankaj Agrawal, "Performance analysis of Encryption and Decryption Algorithms for Securing Images", International Research Journal of Engineering and Technology, Vol. 3, Issue 3, pp. 805-810, 2016.
[16] Pramod Kumar and Pushpendra Kumar Pateriya, "RC4 Enrichment Algorithm Approach for Selective Image Encryption", International Journal of Computer Science and Network Security, Vol. 13, No. 4, pp. 95-99, 2013.
[17] Parameshachari B D, Rajashekarappa, K M Sunjiv Soyjaudah and Sumithra Devi K A, "Partial Image Encryption Algorithm Using Pixel Position Manipulation Technique: The Smart Copyback System", 4th International Conference on Artificial Intelligence with Applications in Engineering and Technology, pp. 177-181, 2014.
[18] Lahieb Mohammed Jawad and Ghazali Sulong, "A Survey on Emerging Challenges in Selective Color Image Encryption Techniques", Indian Journal of Science and Technology, Vol. 8, 2015.
[19] Parameshachari B D, K M Sunjiv Soyjaudah and Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications, Vol. 63, No. 16, pp. 33-36, 2013.
[20] A. M. Riad, A. H. Hussein and A. A. El-Azm, "A New Selective Image Encryption Approach Using Hybrid Chaos and Block Cipher", IEEE-8th International Conference on Informatics and Systems, pp. 36-39, 2012.
[21] S. K. Naveenkumar, H. T. Panduranga and Kiran, "Partial Image Encryption for Smart Camera", International Conference on Recent Trends in Information Technology, pp. 126-132, 2013.