International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-9)

Research Article | **September 2015**

Color Image Encryption using 3AES

Arundhati Sahoo*, Pravin Kumar Bisoi
Department of Computer Science Engineering,
Adarsha College of Engineering,
Angul, Odisha India

***Abstract*—**

Digital image transmission over the internet is a challenging task due to the open access by the attacker. Different cryptographic techniques are used for providing security to transmitted data. In this paper, we have proposed a technique to encrypt color image using 3AES algorithm. From the results, it may be concluded that our algorithm is performing better than the existing algorithms.

Keywords*— *3AES; Color Image; Encryption, Decryption; Color Components.

I. INTRODUCTION

Huge data are transmitted over the public network in digital form due to the advancements of Internet technology. Since public network is easily accessible, protection of digital data is a vital issue now a days. For the data protection from the unauthorized people, different algorithms have been developed. The algorithms are categorized as symmetric and asymmetric types [1]. Since the symmetric key cryptographic algorithms work faster than asymmetric key algorithms, different variations of such algorithms have been proposed by different researchers.

Out of the symmetric key cryptographic algorithms, AES (Advanced Encryption Standard) is a secured technique. In this paper, an encryption algorithm has been proposed using 3AES (Three Advanced Encryption Standard) in the color images. Here, the AES algorithm is repeated for three times using different keys for the color components of the inputted image.

II. RELATED WORK

Due to the computing speed, nowadays AES algorithm has got some threats from the attackers [1]. In 2010, AbdulkarimAmerShtewet. al. have found such issues and modified the standard algorithm by modifying the shift row phase involved [2]. In 2010, El-Sayed Abdoul-MoatyElBadawyet. al. have modified the standard AES algorithm by modifying the S-Box generation using 1D logistic chaos equation [3]. Similarly in 2011, Zhang Zhao et. al. have modified the standard AES algorithm by modifying the S-Box generation using 1D logistic maps [4]. In 2011, AlirezaJolfaeiet. al. have identified such issues and modified the standard algorithm by modifying the S-Box using the chaotic map equation [5].

In 2013, Chittaranjan Pradhan et. al. have modified the standard AES algorithm using different chaotic maps for better performance [6]. In 2014, Chittaranjan Pradhan et. al. proposed 3AES algorithm for enhancing the security of the AES algorithm in the color image domain [7]. Motivated by this work, we have worked on the extension for the color image encryption.

III. PROPOSED ALGORITHM

The color image is a collection of pixels and each pixel contains three color components as Red (R), Green (G) and Blue (B). Each color component is represented by 8-bit and quantized separately. The color components of the original image are encrypted separately. When we combine all RGB components, the color image is produced. For the image encryption, 3AES algorithm has been chosen, which consists of three rounds of AES algorithm with different keys.

A. Encryption Process

The encryption of the color image follows the following steps:

1. Read the color image and extract the R, G and B color components.
2. Each color component will be encrypted using 3AES algorithm using different keys.
3. After the encryption process, combine all the components to form the final encrypted image.

The whole encryption process is shown in Fig. 1.

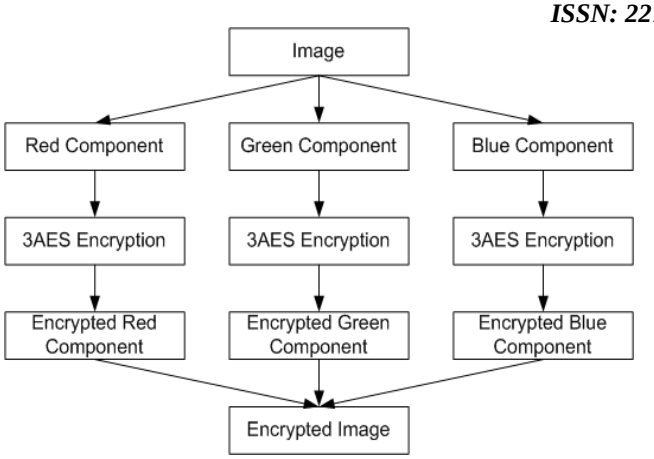

Fig. 1 3AES Color Image Encryption Process

B. Decryption Process

The decryption process is the revere of the encryption process, which is shown in Figure 2. The detailed steps are:

1. Input the encrypted color image; which will be further decomposed into different color components.
2. Decrypt the color components using 3AES algorithm and the respective keys.
3. Finally, the combination of all color components produces the decrypted color image.

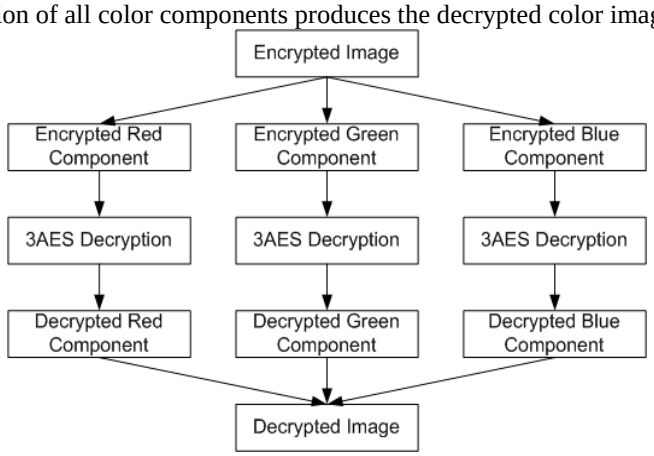

Fig. 2 3AES Color Image Decryption Process

C. Result Analysis

For the experimental analysis, we have taken lena64.bmp as the color image as shown in Figure 3(a). Figure 3(b) shows the extracted color components of the inputted image. The components have gone through the 3AES encryption as show in Figure 3(c). The combination of all the encrypted color components produces the final encrypted image as shown in Figure 3(d).

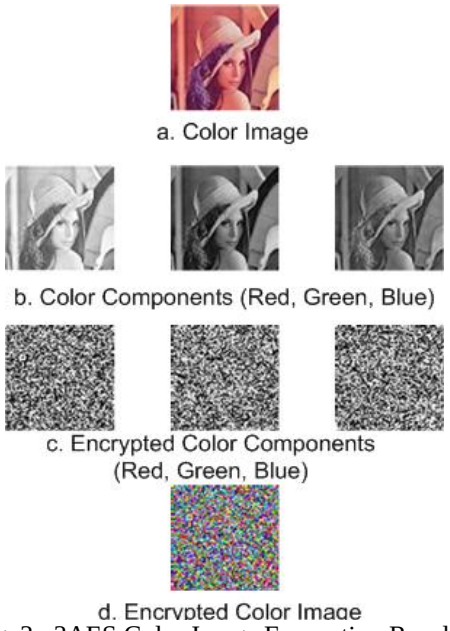

Fig. 3 3AES Color Image Encryption Results

The decryption of this encrypted color image is shown in Figure 4. Figure 4(a) shows the encrypted color image, whose components are extracted as shown in Figure 4(b). The color components are decrypted by using 3AES decryption process (shown in Figure 4(c)). Figure 4(d) shows the final decrypted image.

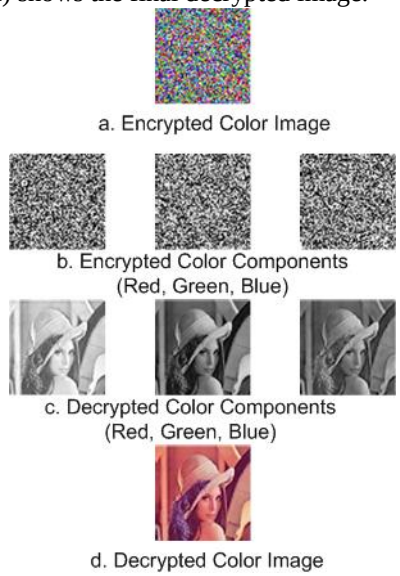

Fig. 4 3AES Color Image Decryption Results

The performance of this algorithm can be evaluated by NPCR (Number of Pixels Changing Rate), UACI (Unified Average Changing Intensity) [8]. The change in cipher image due to a slight change in plain image is an important characteristic for security. There should be a huge difference between encrypted form and the original. NPCR concentrates on the absolute number of pixels while UACI focuses on the average difference between two paired cipher images [8]. Higher the value of NPCR and lower value of UACI is appreciated for an efficient encryption procedure.

Let C1 and C2 be the two cipher images before and after one pixel change in the plain text respectively. The pixel value at grid (i, j) in C1 and C2 are denoted as C1 (i, j) and C2 (i, j) and a bipolar array D is defined as:

$$D(i,j) = \begin{cases} 0, & if\ C1(i,j) = C2(i,j) \\ 1, & otherwise \end{cases} \quad (1)$$

The NPCR and UACI can be mathematically defined as:

$$NPCR(C1,C2) = \frac{\sum_{i,j} D(i,j)}{T} * 100\% \quad (2)$$

$$UACI(C1,C2) = \frac{\sum_{i,j} |C1(i,j) - C2(i,j)|}{F * T} * 100\% \quad (3)$$

where, T denotes the total number of pixels in the cipher image; F denotes the largest supported pixel value compatible with the cipher image format. The NPCR and UACI values of different color components are given in Table 1.

TABLE I. NPCR AND UACI VALUES

Color Component	**NPCR**	**UACI**
Red	94.56	32.40
Green	95.62	30.86
Blue	96.42	31.24

IV. CONCLUSIONS

In this proposed algorithm, we have used 3AES as the encryption algorithm for RGB components of color image. The NPCR and UACI values show that this approach is good enough to resist the differential attacks. In future, some more variations of AES algorithms may be proposed for the color images.

REFERENCES

[1] Behrouzan A. Forouzan, "Cryptography & Network Security", TMH Publisher, 9780070660465, 2010.

[2] AbdulkarimAmerShtewi, BahaaEldin M. Hasan, Abd El fatah, A. Hegazy, "An Efficient Modified Advanced Encryption Standard (AES) Adapted for Image Cryptosystems", International Journal of Computer Science and Network Srecurity, Vol. 10, No. 2, 2010, pp. 226-232.

[3] El-Sayed Abdoul-MoatyElBadawy, Amro Mokhtar, Waleed A. El-Masry, Alaa El-Din Sayed Hafez, " A New Chaos Advanced Encryption Standard (AES) Algorithm for Data Security", International Conference on Signals and Electronic Systems, Poland, 2010, pp. 405-408.

[4] Zhang Zhao, Sun Shiliang, "Image Encryption Algorithm Based on Logistic Chaotic System and S-Box Scrambling", International Congress on Image and Signal Processing, IEEE, 2011, pp. 171-181.

[5] AlirezaJolfaei, AbdolrasoulMirghadri, "Image Encryption using Chaos and Block Cipher", Computer and Information Science, Vol. 4, No. 1, 2011, pp 172-185.

[6] Chittaranjan Pradhan, Ajay Kumar Bisoi, "Chaotic Variations of AES Algorithm", International Journal of Chaos, Control, Modeling and Simulation, Vol. 2, No. 2, 2013, pp. 19-25.

[7] Chittaranjan Pradhan, Bidyut Jyoti Saha, Arundhati Sahoo, Ajay Kumar Bisoi, "Robust Digital Image Watermarking using 3AES in DWT Domain", IUP Journal of Computer Sciences, Vol. 8, No. 4, 2014, pp. 44-51.

[8] N. K. Pareek, "Design and Analysis of a Novel Digital Image Encryption Scheme", International Journal of Network Security & Its Applications, vol. 4, No. 2, 2012, pp. 95-108.

