IOP Conf. Series: Materials Science and Engineering **190** (2017) 012038 doi:10.1088/1757-899X/190/1/012038

Implementation of 128 bits Camellia Algorithm for Cryptography in Digital Image

Bagus Satrio Waluyo Poetro

Department of Informatics, Faculty of Industrial Technology, Sultan Agung Islamic University, Semarang, Indonesia

Bagusswp@unissula.ac.id

Abstract. Nowadays information technology requires stronger cryptographic algorithms. Camellia algorithm is also known for its suitability in terms of the implementation of both software and hardware as well as a high level of safety. The digital image is an image f (x, y) which having the spatial coordinates, and brightness levels are discrete. Unlike text messages, the image data has special features such as high redundancy and a high correlation between pixels. This research conducted a cryptographic process of the digital image using the Camellia algorithm. Comparisons were made on three digital image format .bmp, .jpg, .png with 128 bits key block Camellia algorithm. Results shows that Camellia cryptographic algorithms in digital image can successfully produce encrypted images. In addition, the same algorithm can also reproduce the image when decryption process.

1. Introduction

Cryptography is the study of science and art to keep a message or data information to be safe. Nowadays information technology requires stronger cryptographic algorithms [1]. One of important criterion for a good algorithm is that it should be practically efficient for legitimate users [2].

Camellia algorithm was developed by NTT (Nippon Telegraph and Telephone Corporation) and Mitsubishi Electric Corporation in 2000. Camellia algorithm support 128 bits block key which is same with AES (Advanced Encryption Standard) algorithm [3]. AES and Camellia algorithm can be concluded that the length of character input and key length is proportional to the process time of encryption and decryption [4]. Also Camellia algorithm is also known for its suitability in terms of the implementation of both software and hardware as well as a high level of safety [5].

The digital image is an image f (x, y) which having the spatial coordinates, and brightness levels are discrete [6]. Unlike text messages, the image data has special features such as high redundancy and a high correlation between pixels [7]. Digital image can be quickly moved and copied without any loss of information or image quality [8].

This paper proposes implementation of Camelia Algorithm to understand the performance of the algorithm.

2. Methods

Research method in this study can be explained as follows:

2.1. Camellia Algorithm

Camellia algorithm is a symmetric key cryptography algorithm that works on a block size of 128 bits with a key length of 128 bits, 192 bits or 256 bits [5]. Phases of Camellia Algorithm in this research are described as follows:

2.1.1. Encryption Process.

a) Separating the original image into 3 layers (Red, Green, Blue).
b) Insert 128 bits key (16 characters) and do the key scheduling process until produce subkeys which will be used in encryption process.
c) Initializes long rows & columns from original image every 128 bits (16 pixels, 4x4 size).
d) Change the shape of block data becoming array.
e) Encrypting block data from original image every 128 bits (16 pixels) until maximum size from the original image with the 128 bits key from the key scheduling process.
f) Change the shape of array from encryption process becoming block data again.
g) Repeat step 3 until 6 at each of image layer (Red, Green, Blue).
h) Merge 3 layers (Red, Green, Blue) which will be knwon as encrypted image.

2.1.2. Decryption Process.

a) Separating the encrypted image into 3 layers (Red, Green, Blue).
b) Insert 128 bits key (16 characters) and do the key scheduling process until produce subkeys which is opposite in encryption process.
c) Initializes long rows & columns from encrypted image every 128 bits (16 pixels, 4x4 size).
d) Change the shape of block data becoming array.
e) Decrypting block data from encrypted image every 128 bits (16 pixels) until maximum size from the encrypted image with the 128 bits key from the key scheduling process.
f) Change the shape of array from encryption process becoming block data again.
g) Repeat step 3 until 6 at each of image layer (Red, Green, Blue).
h) Merge 3 layers (Red, Green, Blue) which will be known as decrypted image (it should be look like original image).

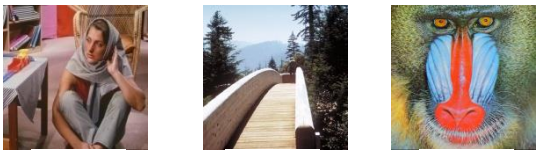
2.2. Key used

The key which was used in this research have 16 characters or 128 bits long. The key selected was '123456789abcdefg'.

2.3. Data used

Digital image which is intended in this research was 3 images with a still image formats. bmp, png and. jpg. The size of the image used is square which mean that is the length and width of the image should be the same. The maximum size used in this research was 512 x 512 pixels.

The imagery used is high-frequency image such as the image of Barbara (a) [9], image that contain high-quality and low-cost as image of Bridge (b) [10], and complex image such as the image of Mandrill (c) [11]. Figure 1 show three digital images which was used in this research.



(a) (b) (c)

Figure 1. Images used for testing

2.4. System Design

General overview of the encryption or decryption process used in this research as in Figure 2 and Figure 3. Figure 2 explained that Camellia algorithm encrypted the original image simultaneously with the help of 128 bits encryption key which was mentioned before. When finished, the image of the encryption process called the encrypted image. While Figure 3 explained that the encrypted image can be decrypted with 128 bits key which was exactly the same when the encryption process. After the decryption process completed the encrypted image turned back to original image.

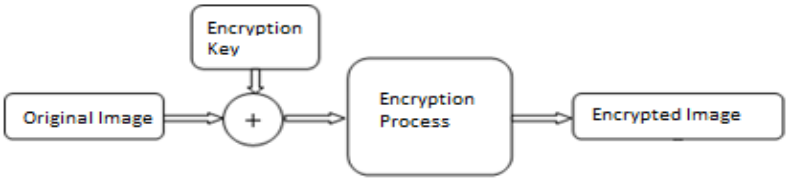


Figure 2. Encryption Process

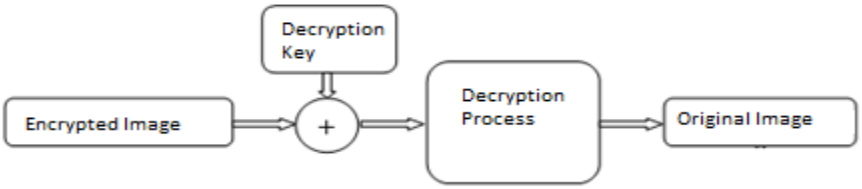


Figure 3. Decryption Process

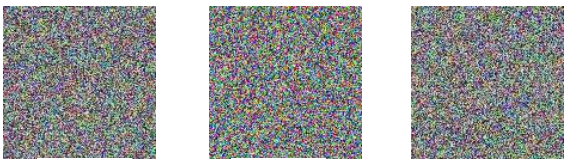
2.5. Image similarity measurement

To show how much exactly the same original image was, this research used euclidean distance measurement method. This method was chosen because image similarity measurement can be done partly by using euclidean distance calculation [12].

3. Results and Discussion

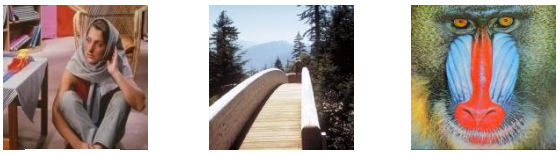
3.1. Shape of encrypted image

The image results are shown in the encryption process when testing was similar in every format (a,b,c). In Figure 4 shows the results from the encryption process of Camellia algorithm against the format. bmp,. jpg,. png. While in Figure 5 shows the results from the decryption process of Camellia algorithm with exactly the same 128 bits key at encryption process against the format .bmp, .jpg, .png.



(a) (b) (c)

Figure 4. Encryption process results for .bmp , jpg and png format



(a) (b) (c)

Figure 5. Decryption process results for .bmp , jpg and png format

Figure 5 shows that .bmp, .jpg and .png format which have been encrypted was turned back exactly the same with original images without any loss or faulty condition. Based on Table 1 all images were calculated using the euclidean distance method and the results reveal that every single image has distance close to 0. This means that getting close to 0 implies the more similar the images are.

Table 1. Results of euclidean distance calculation

No	Image Name	Format		
		BMP	JPG	PNG
1	Barbara	0,534	0,921	0,620
2	Bridge	0,511	0,901	0,609
3	Mandrill	0,523	0,914	0,632

4. Conclusion

Based on the research and discussion that has been done, it is concluded that:

a) Camellia cryptographic algorithms in digital image can successfully produce encrypted images.
b) Every encrypted image was back to original image when decryption process.
c) BMP format was more getting close to 0 than PNG and JPG which mean more similar than others.

References

[1] B.S.W. Poetro, et al, "Kriptografi Citra Digital dengan Algoritma Rijndael dan Transformasi Wavelet Diskrit Haar," S.Kom. undergraduate thesis, Dept., Informatics., Diponegoro Univ., Semarang, Central Java, Indonesia, 2010.
[2] W. Mao, Modern Cryptography : Theory and Practice, Prentice Hall PTR, New Jersey, USA, 2003.
[3] Specification of Camellia – a 128-bit Block Cipher, NTT and Mitsubishi Electric Corporation, 2000.
[4] Sabriyanto, "Analisis Perbandingan Performansi Algoritma Camellia dan AES Pada Blok Cipher," ST. undergraduate thesis, Dept., Elect and Telco, Telkom Institute, Bandung, West Java, Indonesia, 2009.
[5] M. Matsui et al., "A Description of the Camellia Encryption Algorithm, Request for Comments : 3713", 2004.
[6] S. Nugroho, "Sistem Pendeteksi Wajah Manusia pada Citra Digital," M.Cs thesis, Dept., Computer Science, Gadjah Mada University, Yogyakarta, Indonesia, 2004.
[7] E.I.F. El-Ashry, "Digital Image Encryption," M.Sc thesis, Dept., Electronic Engineering, El Monofeya, Menofia University, Egypt, 2010.
[8] S.D. Anderson, "Digital Image Analysis : Analytical Framework for Authenticating Digital Images," M.S thesis, Dept., Engineering and Applied Science, University of Colorado Denver, Denver, USA, 2001.
[9] H. Elkamchouchi and M.A. Makar, "Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR block ciphers,", Proceedings Twenty second National Radio Science Conference (NRSC 2005), pp. C11, Cairo, Egypt, 2005.
[10] E.C. Larson and D.M. Chandler, "Most Apparent Distortion : Full Reference Image Quality Assesment and the Role of Strategy," Journal of Electronic Imaging, Vol 19, Issue 1, USA,

2010.
[11] L.P. Dung, "Perception Based Quality Measure for Image Compression and Transmission," M.IT thesis, Dept. Computer Science and Engineering, Monash University, Australia, 1998.
[12] B.S.W. Poetro and A. Labellapansa, "Pengelompokan Gejala Penderita Kolesterol melalui Pola Iris Mata menggunakan Moment Invarian dan Euclidean Distance," Prosiding Seminar Nasional Ilmu Komputer Universitas Diponegoro 2012, pp 117, Publisher : Graha Ilmu, 2012.