International Journal of Engineering & Technology, 8 (1.9) (2019) 67-73

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Modified AES with Matrices Selective Block Cipher on Image Encryption

Muhammad Barja Sanjaya[1*], Patrick Adolf Telnoni[2]

D3 Manajemen Informatika, Fakultas Ilmu Terapan – Telkom University, Bandung, Jawa Barat, Indonesia
**Corresponding author E-mail: mbarja@tass.telkomuniversity.ac.id*

Abstract

Advanced Encryption Standard (AES) is one of symmetric cryptography which its operation is conducted in cipher block mode. Meanwhile the computation operation is in cipher block mode, AES takes high cost of computation to process the data. Moreover nowadays the data size to process has been bigger, such as image. Because of this, it appears several questions for AES cryptography performance to implement. Several designs of methods that have been studied and conducted namely selective bit plane in 2002 and partially encryption in 2013 were still in high cost for computation. Thus, a new design or method is proposed to cut off the high cost of computation in time processing and memory consumption. In this study, it is proposed matrices selective block cipher which its process operates the object of area in an image to be encrypted exactly. The operation which is conducted while encrypting the selected area in image is only on one of the layers, it also involves random number Blum-Blum-Shub and Chaotic Function for initializating the key. Based on the data result of experimental tests, it is achieved an optimization for the proposed method as big as 28.61197 times faster instead of applying combination partially encryption and selective bit plane in a usual method and it also takes an additional memory comsumption as big as 0.168545%.

Keywords: *AES, random number, chaotic function, selective bit plane, partially encryption.*

1. Introduction

One of fields of study in informatics that studies about method for securing the data as well as giving limitation for the access to the data from unauthorized party is known as cryptography. The implementation of cryptography is full of algebraic computation in its operation and it also operates mathematical formula which in each iteration of the computation there is a newly process so that the readable plaintext that can be understood is transformed into a ciphertext. Cryptography can be presented into asymmetric and symmetric based on the key used to encrypt. Whereas the other type of cryptography is one way function called hash which is only be able to do encrypting into message digest but it cannot be decrypted back into plaintext.

AES is one of symmetric cryptography which in its operation either encrypting or decrypting uses a same key [12]. In its operations, AES applies in cipher block mode, namely it operates encrypting the data such as image in block by block with the size of each block is 4x4 bytes and it is presented in 4 rows and 4 columns as a square matrice [11]. This exactly affects the computation performance of AES while it is being conducted.

As for the data plaintext which can be processed using cryptography is not only in format text but also as an audio, image or video that is rich and full of data or information. That's why very high cost of computation is needed to conduct encrypting an image which also has three layers using AES cryptography. The time for processing and memory consumption will also increase as the file size of plaintext gets bigger [5][6]. Several methods to cut off these high computations to do cryptography process on image or video had been conducted in previous study [1], [3], [9]. However the data result of those studies were still in minimum performance yet. Due to the unnecessary data on selected area on image was also processed so that the time processing and memory consumption needed were so high.

Thus, it is proposed a new method which is also involving edge detection algorithm to get the selected area of object on image to encrypt. Besides, the proposed method also applies combination of selective bit plane operation and partially encryption as well as it only operates the encryption on one of layers to get the optimal computing performance.

2. Related Research

As for the related researches that had been conducted previously, namely:

Martina Podesser, Hans−Peter Schmidt, Andreas Uhl (2002)
In this research, there was a proposed implementation of a design for processing cryptography on image by processing only on several bits of every selected pixels as plaintext. The bits which are processed are only Most Significant Bit (MSB). As for the numbers of bit

Copyright © 2019 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

MSB that were encrypted begin from the first one bit, the first two bits, or four bits firstly. Based on the experiment, it was concluded that using four bits MSB firstly can represent the operation on entire eight bits in each byte of plaintext [1].

Soleymani, Ali. Md Ali, Zulkarnain. Nordin, Md Jan (2012)
In this research, it was explained about the important objectivity of cryptography, namely confidentiality, data integrity, authentication, and non repuditation [8]. Based on the parameters mentioned, authentication had been more paid attention to study. Authentication is the same as digital signature, and it is studied into two concepts namely entity authentication and message authentication.

I Putu Arya Dharmadi (2013)
In this research, it was conducted the implementation of RC4 on image with several objects which were achieved by selecting the area or the entire of image. The applied process of cryptography was combined to Chaotic Function to select the bits to use to produce the key needed. Based on the result, it was achieved that using Chaotic Function on computation could facilitate the process and it took the same size of memory consumption.

M. Barja Sanjaya, Patrick Adolf Telnoni (2015)
In this research, it was conducted the implementation the combination between random number Blum-Blum-Shub (BBS) and Chaotic Function on Advanced Encryption Standard (AES) cryptographic algorithm. As for the plaintext was text file in Notepad file format, and the size of each plaintext was various starting from 10 Kilo bytes till 10 Mega bytes. However, the additional combination process implemented on AES, it was achieved that there was a cut off the processing time as big as 21% and it also took the same size of memory consumption. Beside, the value of avalenche effect (AE) produced was categorized in optimal criteria as big as 49% [10].

3. The Proposed Method

Generally, the process which was conducted in this research is described in block diagram as follows:

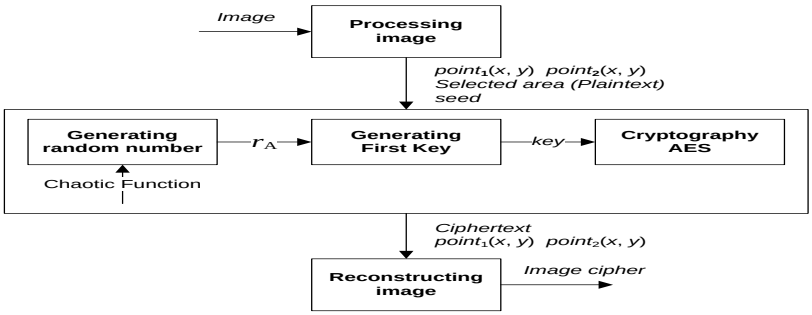


Fig 1: Block Diagram of Proposed Method

Based on the Figure 1, it was depicted that the main process which was conducted on proposed system includes three processes, namely image processing, computation of cryptography and reconstructing the cipher. For the first step, it consists of several sub processes namely cropping, segmentation and reconstructing the plaintext. In the second step, it is conducted generating random number using BBS combined to Chaotic Function to select the bits to use. Furthermore, the inialization for key was generated as the first key to do the next process. And the last step, the process reconstructs the cipher into the image.

For the sub process of reconstructing the data plaintext described in block diagram, it is described in figure 2:

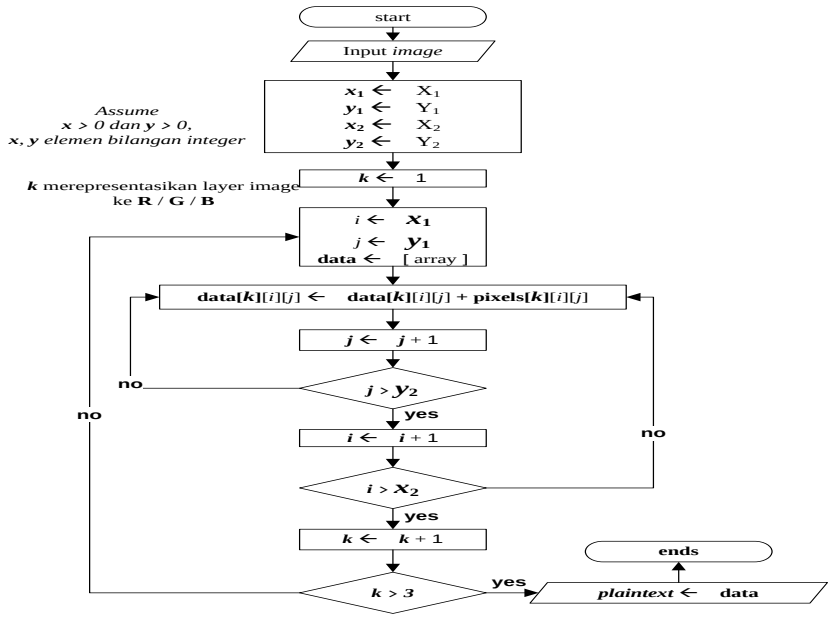


Fig 2: The reconstructing of plaintext (based on selected area)

Figure 2 explains that the first step in processing of image which was conducted is cropping process on area closely to the object selected. The area selected from cropping the image covers to points, starting point as (x1,y1) and it ends in point (x2,y2). These points are used to calculate the area of the object to encrypt. So the further process will focus on the selected area. The next process to be conducted is to apply edge detection using Sobel operator on selected cropped area by determining the background color of the object which is white as presented in black-white color. The purpose of this process is to make easier in copying the data into temporary variable.

In the process of copying the data into a variable, it is also proceeded in conducting the process of reconstructing the data plaintext by still maintaining the position of each layer. Further, the process of selective bit plane is conducted into the new copied variable. As for the selective bit plane process is described in flowchart as follows:

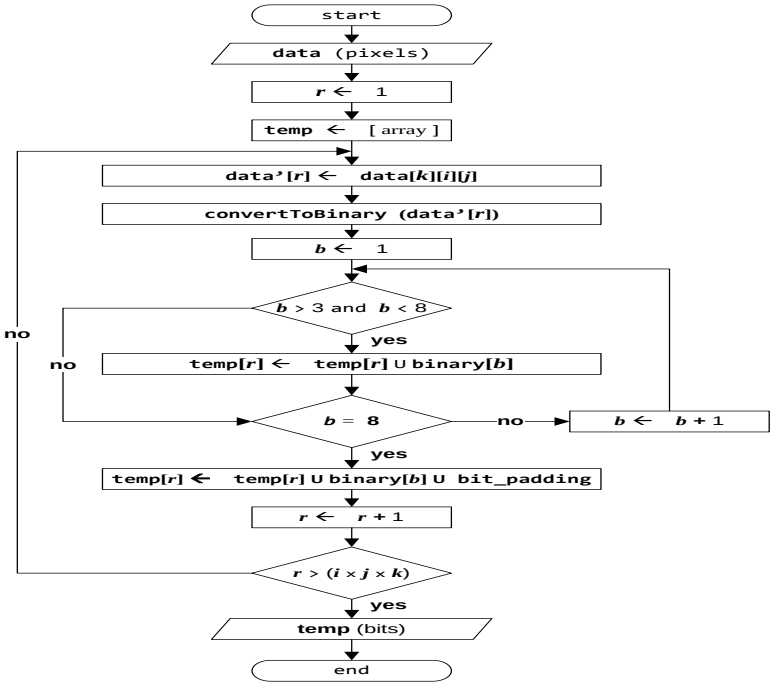


Fig 3: The process of selective bit plane on plaintext

After the process to reconstruct data plaintext has been conducted and saved into temporary variable in one dimensional of an array, the process of selective bit plane as previously explained is conducted.

Figure 3 explains taht the selective bit plane process is begun in the first pixel in the array that has been created. Each of bits on pixels is conducted bit selection process, it starts one bit from the first bit of MSB, two first bits of MSB or four bits of MSB. The result of reconstructing the plaintext is saved into an array variable that has also the same size in one dimension. The number of bit MSB which will be proceeded into new plaintext depends on our criteria. Those MSB bits which are already in new format is transformed into bytes of pixels.

This process is conducted until to the last pixel, if there is uncompleted byte of pixel to process in the next step, then bit padding is also conducted. This last variable containing the data with selected bits have been composed is ready to proceed conducting the process of cryptography.

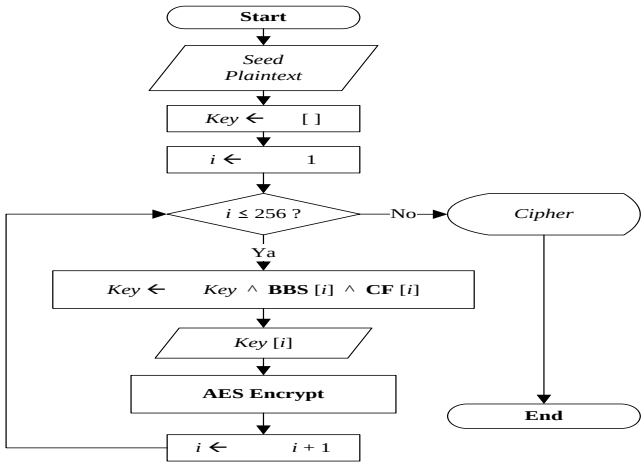


Fig 4: The process of encrypting/decrypting using AES

The explaination of flowchart in figure 4:

a. Input seed as a positive integer number and plaintext as data which will be processed. Seed is an integer in domain 0 < seed < 28.

b. Create an array to load the key generated in each of iteration of computation. The length of bit to produce key is 256-bits.

c. Conduct the AES cryptography, it starts form the first round using the key generated by doing XOR operation to bits which are produced from the combination of random number BBS and Chaotic Function. It is for to randomize the order of bits producing the key in each of iteration.

d. Do the process in step C in the next iteration on other blocks of plaintext until the last byte. Then, conduct the process AES cryptography.

4. Implementation, Testing and Analysis

The sub chapter which will be explained includes: implementation, testing, and analysis.

4.1. Implementation

As for the implementation concerning to proposed design which is conducted testing on image file by simulating several objects with various patterns. It is for demonstrating the objectivity and showing the performance parameters. The image which will be processed in simulation has some criterions, namely in dimensional of 50x50 pixels for the object, whereas the dimension of the entire of image is in dimensional of 400x400 pixels.

4.2. Testing and Analysis

Whereas based on the result of testing after the implementation conducted, namely:

1. The result of image cipher which is achieved from testing

Belows, it shows the data result of image cipher which is achieved from testing:

Table 1: The result of image cipher

Plaintext	Encrypt 1 bit	Encrypt 2 bits	Encrypt 4 bits
			
			
			
			
			
			
			
			
			
			

Based on Table 1 namely the data result of encryption process using proposed method and the criteria of the number of MSB bit to process, it is shown that cipher produced using one bit or evenmore four bits is still in minimum performance on the level of readability on cipher due to the randomized data produced using proposed design is only processed on one of layers on the object of image selected

eventhough the pattern in each of objects is various. It also only involves two kinds of color, namely black and white color so that it affects to the level of readability on cipher. However, the proposed method has still better performance if it is compared to the other way by blurring the image that ruins the byte of pixel on it so that it cannot be conducted process of decrypting the cipher into original plaintext.

Based on the testing result of proposed method, below the evaluation of the comparation of performance between the two methods tested, as follows:

4.3. Performance of computation processing time

As for the comparation of performance which has been achieved is presented as follows:

1. The curve (bar chart) of comparation concerning to the time for processing computation to encrypt using AES between selective bit plane in ordinary and proposed design, as follows:

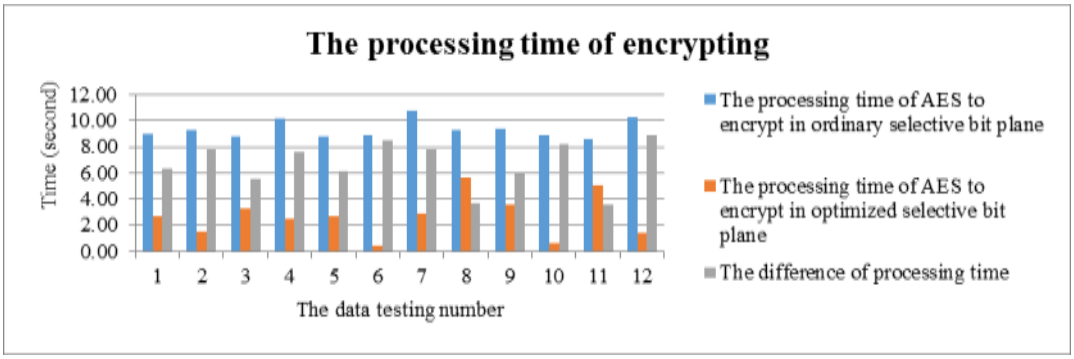


Fig 5: The result of processing time of encrypting

Based on Figure 5, it is shown that the comparation between computation AES using selective bit plane ordinary and proposed design which operates only on one of layers has a high difference on each file plaintext to encrypt. Another significant result is also shown on the green bar chart which explains the difference of processing time of computation between the method in [1] and proposed one. Though there is a minimum additional computing process that has been conducted while generating key scheduling by implementing the calculation of newly changing prime relativity, it is noticed that the processing time gets faster as big as 28.61197 times than the performance in method [1]. Moreover, it is noticed on the sixth and tenth testing, the proposed method has better performance at most than method [1].

2. The curve of the processing time comparation during conducting the simulation of decrypting between the proposed method and the previous method in [1], as follows:

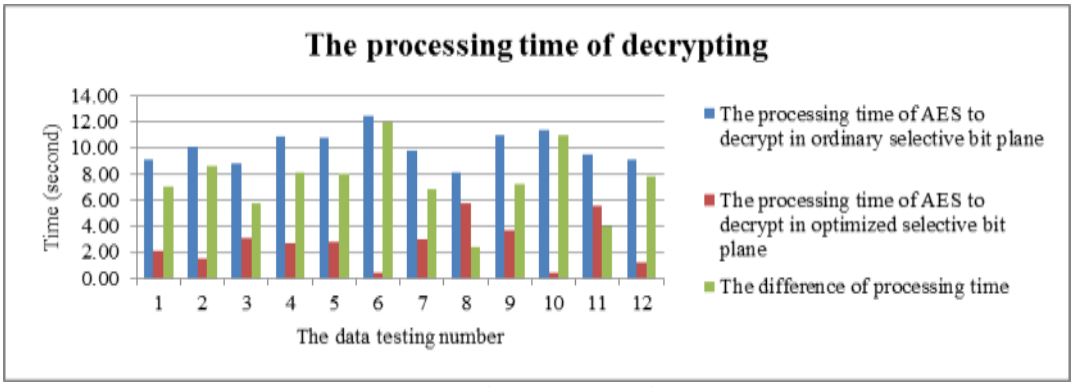


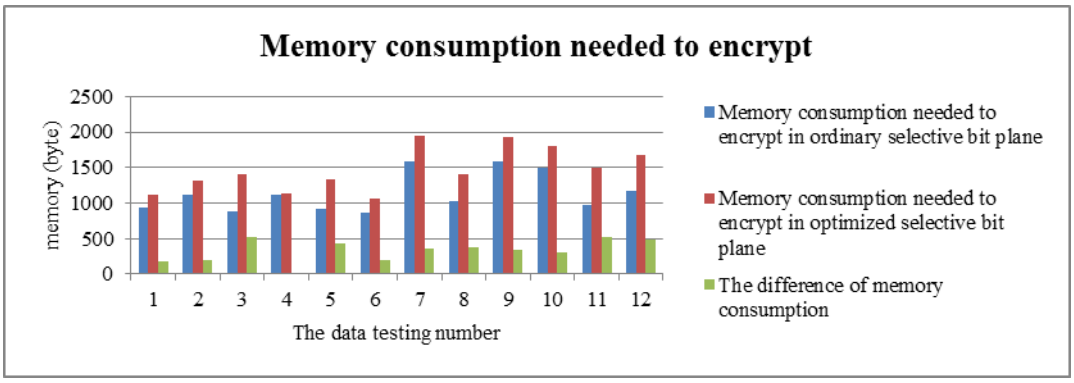
Fig 6: The result of processing time of decrypting

Another the same result related to the testing on simulation is shown in Figure 6, that is indicated while processing of decrypting the ciphertext is conducted. Based on the Figure 6, it is shown that there is relatively big difference of processing time consumption between proposed method and [1] which is shown in the sixth testing, it only takes 0.42268 seconds and in the tenth testing takes only 0.41285 seconds to process the proposed method whereas the method in [1], it takes 12.438009 seconds to process in the sixth testing and 11.380129 seconds in the tenth. This result occurs due to the process is conducted in only one of layers of selected area on image eventhough there is additional process of generating key conducted in the proposed method.

4.4. Performance of memory consumption

As for the memory consumption which has been achieved is presented as follows:

1. The curve of memory consumption comparation during the process computation of encrypting is conducted, as follows:



Based on Figure 7, it is shown that there is enhancement of memory consumption needed to conduct the computation process in the proposed method. As for the factor affecting the memory consumption gets increased while conducting the proposed method is because of an additional process especially while reconstructing the plaintext. However, the average of difference of memory consumption between method in [1] and the proposed one which has an optimization on performance is as big as 329 bytes additional memory on encrypting process and 243 bytes on decrypting. The optimal performance is shown in the fourth testing which has difference as big as 10 bytes. The total average on memory consumption while conducting the proposed method compared to method in [1] is 0,168545%, and this percentage value of memory consumption is categorized as minimum.

2. The curve of memory consumption comparation during the computation of decrypting as follows:

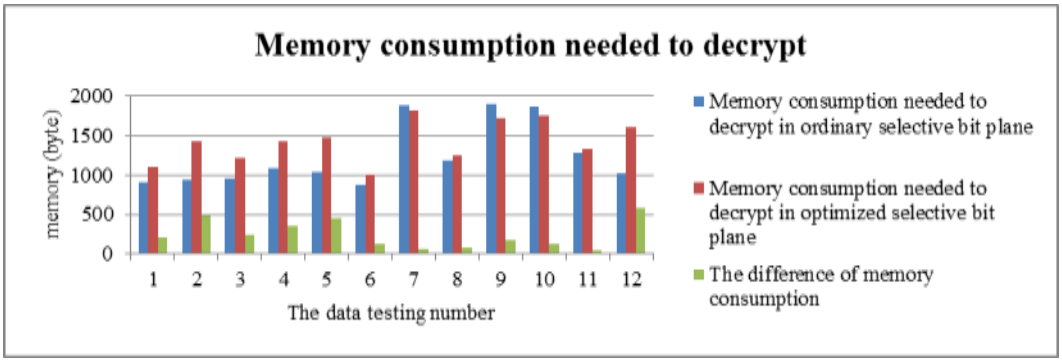


Fig 8: The result of memory consumption of decrypting

The same results based on testing which has been conducted, Figure 8 shows that also occurs a difference of memory consumption. Moreover, in the seventh, eighth, and tenth result of testing, it is shown that there is minimum difference of memory consumption needed in processing, especially in the seventh testing takes only an additional memory as big as 57 bytes. Whereas the total average of all data processed is as big as 0.134096%, and this value is also categorized as minimum. So it is determined that the expected optimization of performance on proposed method has been achieved.

Meanwhile, another analysis that can be discussed is shown in the Figure 7 and 8, there is an obvious inconcistency of memory consumption while conducting the computation. The inconcistency occurs due to several main factors, namely the different pattern of each object on image so that AES operations which is in cipher block mode does the different bit padding in encrypting process. This different value of bit padding added in reconstructing each object affects the enhancement or reduction in consumpting memory while conducting the process. However, the number of the difference is still categorized as minimum if the proposed method is implemented nowadays.

Based on the proposed design and noticed on data testing results, it can be also transformed into a simple formula which determines in Mathematics concerning to the reduced processing time and memory consumption needed to conduct the proposed method. Assume all the numbers N calculated here are in positive integer and $N > 0$. Whereas the number of processing time T needed is in positive real domain.

Let T represents the total of processing time to conduct encrypting the entire of image as width W x height H pixels, T' represents the total of processing time to conduct the method in [9] which encrypted partially image so that the performance produced in method [9] could cut off the area to encrypt as big as W' x H' pixels, where $W' \leq W$ and $H' \leq H$. T'' represents the total of processing time to conduct the method in [1] which encrypted partially image as well as encrypted only on selective bit plane on several numbers of MSB so that it had better performance than method in [9] which method in [1] could cut off the computation of encrypting process as big as half of each byte on selected pixels. And T''' represents the total of processing time to conduct the proposed method which processes on only one of layers on selected pixel so it can cut off the computation cost better than method in [1] and [9]. Thus, it can be written as $T''' \leq T'' \leq T' \leq T$ and $T, T', T'', T''' > 0$.

Beside, the memory consumption needed while conducting the computation can be also written in a simple Mathematics as the formula written for processing time. Due to there is also additional memory consumption in conducting the computation on the proposed method then it can be written as $M''' \geq M'' \geq M' \geq M$ and $M, M', M'', M''' > 0$, where M represents the total of memory consumption to conduct encrypting the whole of image, M' represents the total of memory consumption in method [9], M'' represents for method in [1] and M''' represents the total of memory consumption for conducting the proposed method.

5. Conclusion

The conclusions which are achieved and based on the proposed method conducted are below:

a.The acceleration of time complexity in computing the AES cryptography using proposed method is as big as 28.61197 times faster that method in [1].

b.There is an instability shown in memory consumption needed while conducting the process of computation, either on proposed method or [1]. The thing takes places due to the different pattern of object on image so it also affects in AES operation which does in cipher block mode by implementing bit padding while reconstructing the plaintext.

c.The image cipher resulted based on proposed method is lower than previous method in [1]. It is noticed that the image encrypted produced using proposed method is still readable. However, it has better performance if it is compared to process of blurring or ruining the pixel data on image that the proposed method can be decrypted to original plaintext.

d.The additional percentage of memory consumption needed to conduct the proposed method is as big as 0.168545% than the previous method in [1].

Whereas the further research domain which is also be able to be conducted is below:

a.The plaintext data which is concern for object to process in modified AES cryptography is in format of audio, either it has been compressed or not.

b.The proposed modified AES cryptogragphy for image encryption can be conducted as well as involving watermarking or steganography.

c.The optimization of algorithm for producing the selected area of object exactly on image.

d.The object of area to encrypt on image can be also experimented on facial pattern of people.

References

[1] Podesser, Martina. Schmidt, Hans-Peter, and Andreas Uhl. 2002. “Selective bit plane Encryption for Secure Transmission of Image Data in Mobile Environments”. School of Telematics & Network Engineering. Carinthia Tech Institute, Klagenfurt, Austria.

[2] Parikh C., Patel P. 2007. “Performance Evaluation of AES Algorithm on Various Development Platforms”. IEEE, ISBN: 078-1-4244-1109-2, June 22-23, 2007.

[3] Barmawi, Ari Moesriami. Syakrani, Nurjanah. Faren. Budianto, Heru. 2008. “Modifikasi Video Encryption Algorithm Untuk Meningkatkan Untuk Tingkat Keamanannya”. Jurusan Teknik Komputer Politeknik Negeri Bandung. Gematika Jurnal Manajemen Informatika, Volume 9 Nomor 2, Juni 2008.

[4] Li-Chang Lo, Johnny. Bishop, Judith. Eloff, J.H.P. 2010. “SMSSec: an End-to-End Protocol for Secure SMS”. Computer Science, University of Petrocia, South Africa.

[5] Mohan, H. Raji, R. 2011. “Performance Analysis of AES and AES Encryption Algorithms”. International Journal of Computer Science Issues (IJCSI). Vol. 8, Issue 4.

[6] Singhal, Nidhi. JPS Raina. 2011. “Comparative Analysis of AES and RC4 Algorithms for Better Utilization”. Department of Electronic & Communication, BBSB Engineering College. Fatehgarh Sahib, Punjabi. India. International Journal of Computer Trends and Technology – July to August Issue 2011.

[7] Shah, Jolly and Saxena, Vikas. 2011. “Performance Study on Image Encryption Schemes”. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No. 1, July 2011. ISSN (Online): 1694-0814. Department of CS & IT, Jaypee Institute of Information Technology. Nodia, Uttar Pradesh 201307, India.

[8] Soleymani, Ali. Md Ali, Zulkarnaen and Nordin, Md Jan. 2012. “A Survey on Principal Aspect of Secure Image Transmission”. World Academy of Science, Engineering and Technology 66.

[9] Arya, I Putu Dharmadi. Ari M, Barmawi. Gandeva BS. 2013. “Enkripsi Gambar Parsial Dengan Kombinasi Metode Stream Cipher RC4 dan Chaotic Function”. Fakultas Informartika, Institut Teknologi Telkom, Bandung.

[10] Barja Sanjaya, Muhammad. Adolf Telnoni, Patrick. 2015. “Implementasi Blum-Blum-Shub dan Chaotic Function Untuk Modifikasi Key Generating pada AES”. Jurnal Elektro Telekomunikasi Terapan, Vol. 2, No. 2. ISSN (p): 2407-1320. ISSN (e): 2442-4400. Desember 2015.

[11] Meyer, Carl H., Matyas Stephen M. 1982. “Cryptography: A New Dimension in Computer Data Security”. New York: John Wiley & Sons.

[12] Forouzan, Behrouz. A. 2008. "Cryptography and Network Security". International Edition. New York. MacGraw-Hill Companies, Inc.