

Image Encryption on Mobile Phone using Super Encryption Algorithm

Emy Setyaningsih^{*1}, Catur Iswahyudi², Naniek Widyastuti³

¹Computer System Department of Institute of Science & Technology AKPRIND Yogyakarta
^{2,3}Informatic Engineering Department of Institute of Science & Technology AKPRIND Yogyakarta
Jl. Kalisahak No 28 Komplek Balapan, Yogyakarta, Telp. +62-274-563029
e-mail: emypurnomo@akprind.ac.id^{*1}, catur@akprind.ac.id², naniek_wid@yahoo.com³

Abstrak

Telepon seluler memiliki keterbatasan memory dan sumberdaya komputasi. Algoritma enkripsi modern seperti DES, AES, IDEA menggunakan algoritma yang rumit dan kompleks sehingga tidak cocok untuk enkripsi citra pada telepon seluler. Oleh sebab itu, diperlukan tradeoff antara kecepatan, keamanan, dan fleksibilitas. Problem yang akan diteliti dan diselesaikan adalah bagaimana mendapatkan algoritma enkripsi citra yang sederhana namun aman, dengan proses komputasi yang ringan dan efisien. Algoritma yang diusulkan adalah super enkripsi yang menggabungkan Playfair cipher dan Vigenere cipher. Hasil percobaan menunjukkan histogram cipher image memiliki distribusi keragaman dan perbedaan yang signifikan dengan histogram plain image, serta frekuensi kemunculan masing-masing nilai intensitas pada histogram cipher image juga merata yang berarti tidak dapat memberikan petunjuk untuk dilakukan statistical attack. Hasil percobaan juga menunjukkan korelasi antar elemen citra setelah dilakukan enkripsi mengalami penurunan signifikan. Rata-rata kualitas enkripsi yang tinggi menunjukkan bahwa tingkat perubahan piksel cukup tinggi sehingga citra hasil enkripsi sulit dikenali. Pengujian pada telepon seluler menunjukkan bahwa algoritma ini hanya membutuhkan sumber daya komputasi yang kecil. Hal ini menunjukkan bahwa algoritma ini cukup efektif untuk enkripsi citra pada telepon seluler.

Kata kunci: enkripsi citra, keamanan, playfair cipher, vigenere cipher

Abstract

Mobile phones have limited memory and computational resources. Modern encryption algorithms such as DES, AES, IDEA uses a complicated and complex algorithm, that are not suitable for image encryption on mobile phones. Necessary, it is tradeoff between speed, security, and flexibility. Problem to be investigated and resolved is how to get the image encryption algorithm which is simple yet safe, with the lightweight and efficient computing. The algorithm developed in this study was super-encryption algorithm that combines Playfair cipher and the Vigenere cipher. The experimental results show the cipher image histogram has a distribution of diversity and a significant difference to the plain image histogram, and frequency of occurrence of each intensity value in the histogram of cipher image is also uneven, which means can not provide clues to do statistical attack. The experimental results also showed a correlation between the elements of the image after encryption has decreased significantly. The average of quality encryption showed that the rate of change of image pixels is high enough so that cipher image difficult to identify. Tests on a cell phone showed that this algorithm requires only small computational resources. This shows that the algorithm is quite effective for image encryption on mobile phones.

Keywords: image encryption, playfair cipher, security test, vigenere cipher

1. Introduction

Mobile communications technology has been developing very quickly, as well as the development of service features that support the Global System for Mobile Communications (GSM). One service offered is MMS (Multimedia Messaging Service) which is the development of SMS (Short Message Service) which allows for the delivery of image data.

The message's sent via MMS media does not directly reach the receiver, but through the server of mobile operator. In its implementation, even there are encryption engines in the cellular network architecture, but the operator as an MMS service provider can still find the content of messages sent by the customer. Other problems arise from the occurrence of human error is an error writing the message destination number. These things cause lack of

confidentiality of the messages. So, it required a security system to protect data transmitted over a communications network by using cryptographic techniques.

However, encryption can't prevent the interception and modification of data on communication channels. Encryption is not capable to protect confidential communications from the audience (eavesdropper) to extract confidential data [1]. On the other hand, mobile devices has a number of limitations, including small memory, limited computing power and diversity of platforms so that the necessary of proper design in order to ensure compatibility and interoperability of the various devices. Computational complexity becomes an important concern in the development of cryptographic techniques in the middle of the limited bandwidth in wireless networking, limitations of processors, memory, and time. Therefore, we need tradeoff between speed, safety, and flexibility [2].

In line with the increase in importance of encryption, many methods are found and expanded its use. Among these methods there is a method that requires only simple mathematical operations, but also there is a method which involves the theory of complex and difficult implementation. Some research has been done to obtain a reliable algorithm to secure digital image by several researchers [1-9], but the digital image encoding which implemented on cell phones are still very few. Research on digital image and its application also has been widely applied, for example by [10-12].

This study aims to get the digital image encryption algorithm with a simple but secure process, fast and efficient computing resources. The algorithms developed in this study were super-encryption algorithm that combines two of cipher called Playfair cipher and the Vigenere cipher. The selection of algorithm is due to Super Encryption does not require a lot of resources, making it suitable for application on mobile phones that have limited memory capacity. To enhance security, the key generation process modifications done on the Vigenere cipher using keystream generator concept with vigenere key value early taken from the key of Playfair corresponds to the value at position (1, 1).

2. The Proposed Algorithm

2.1. Encryption Process

The proposed encryption process can be seen in Figure 1. The key that kept secret and has been agreed between the sender and the recipient is used for encryption using the Playfair cipher as described in the Playfair cipher algorithm.

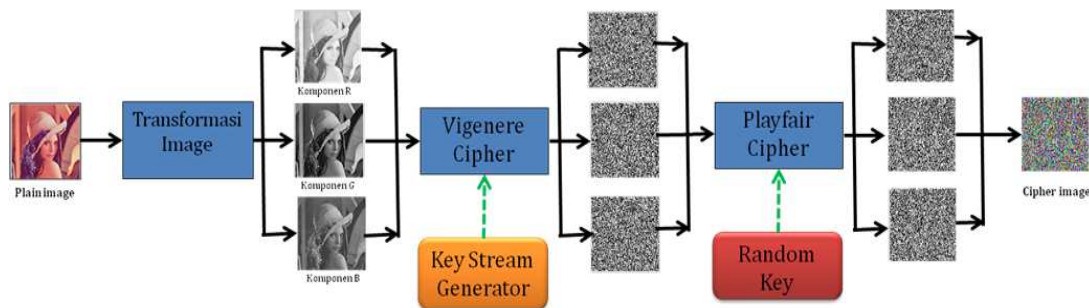


Figure 1. The encryption scheme

Vigenere cipher can still be solved by the method of exhaustive search when the key length is known as the next key is the repetition of the key when the key length is not equal to the length of plaintext. To overcome these drawbacks, the method used to randomize the sequence of next key using keystream generators. The formula used to generate a key using the i -th keystream is [3]:

$$k_i = (k_{i-1} + k_{i-m}) \bmod 256 \quad (1)$$

For example, if the plaintext is known as image with the intensity of 73 78 70 79 82 77 and the key used is 73 83 84, then the key used for encryption should be added 3 key elements to a key length equal to the length of the plaintext. The 4th up to 6th key obtained as follows:

$$k_4 = (k_3 + k_1) \bmod 256 = (84 + 73) \bmod 256 = 157$$

$$k_5 = (k_4 + k_2) \bmod 256 = (157 + 83) \bmod 256 = 240$$

$$k_6 = (k_5 + k_3) \bmod 256 = (240 + 84) \bmod 256 = 68$$

While the key used for encryption using vigenere cipher generated from keys along the next $n+1$ to n keys with key $m \times n$ using the keystream generator in equation (1).

Image encryption steps as follows:

- (i) Select the Playfair key agreed between the sender and the recipient.
- (ii) Generating vigenere key with steps:
 - a. Take the value of playfair key element of the matrix at position (1,1), e.g. is worth 82.
 - b. Playfair key along 82 elements drawn from Playfair key element of the position (1,1) to position (5,2). Key value at position 83 to the n -th ($n = \text{number of rows} * \text{number of columns}$ of the matrix image that will be encrypted) generated by the method of keystream generators in equation (1).
- (iii) Insert the image that will be encrypted
- (iv) Perform a color transformation to separate the RGB color (for color images) into 3 pieces of matrix (Figure 1). For grayscale images do not need the color transformation.
- (v) Perform encryption using a vigenere key for each color component matrix
- (vi) The results of step 5 encrypted using the vigenere encryption algorithm performed using the Playfair key.
- (vii) The vector result of encryption is returned as the value using the RGB color transformation in order to produce a new image that has been encoded as shown in Figure 1.

2.2. Decryption Process

Decryption process performed in this study can be seen in Figure 2.

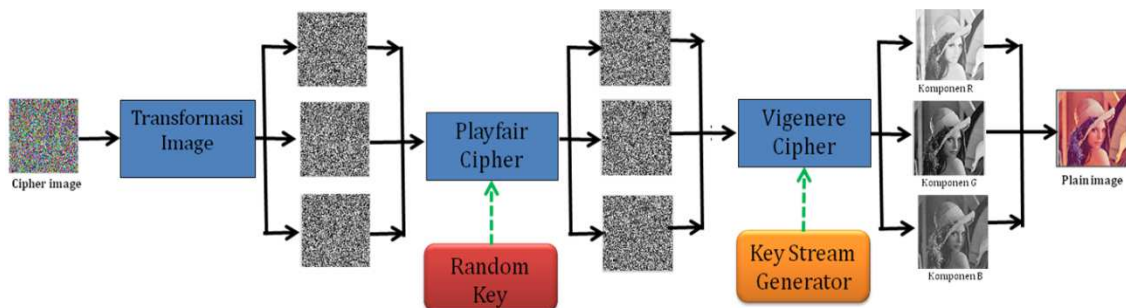


Figure 2. Decryption process scheme

Image decryption steps as follows:

- (i) Insert the image that will be decrypted
- (ii) Select a key that will be used to decrypt the image using the method of Playfair, then generate a key to decrypt the image using the method of vigenere on image in the same way with the encryption process.
- (iii) Perform color transformation so that the RGB color components of the image that has been encoded separated as in the encryption process
- (iv) Perform decryption process using Playfair method with similar step in the encryption process for each color matrix.
- (v) Furthermore, each color component of the ciphertext results of decryption process performed by Playfair method decrypted using vigenere cipher, in ways ciphertext decryption results using vigenere method subtracted with a vigenere key by using the concept of reduction modulo 256 for all color matrix.

- (vi) Vector of the decryption result is returned as the value of RGB using the color transformation to produce the same image with the original image.

3. Research Method

This study is generally divided into two phases. The first stage is the design and analysis of the proposed encryption algorithm. Algorithm analysis was performed using Matlab software. The second stage is the encryption algorithm implementation on mobile phones using the JME programming language.

Super Encryption is one of the character-based cryptography that combines two ciphers. It aims to gain a stronger cipher so it is not easy to solve, and also to address the use of a single cipher which comparatively weak. In this study, the process of encryption and decryption on both Vigenere ciphers and Playfair cipher were performed with one-time process for each cipher.

To determine whether the proposed encryption algorithm is safe enough to be implemented, performed analysis and testing of the encryption algorithm uses several parameters, namely:

3.1. Correlation

Calculation of correlation and entropy performed to assess the quality of the image of the encryption. The lower correlation between pixels and the higher of entropy value, so that the encryption system can be said to be safe. To calculate the correlations used the formula [2], [5]:

$$r = \frac{n \sum (xy) - \sum x \sum y}{\sqrt{[n \sum (x^2) - (\sum x)^2][n \sum (y^2) - (\sum y)^2]}} \quad (2)$$

where:

- r : correlation value
- n : the amount of data
- $\sum xy$: the number of multiplication of x and y
- $\sum x$: the number of data x
- $\sum y$: the number of data y
- $\sum x^2$: the number of x squared
- $\sum y^2$: the number of y squared

3.2. Entropy

Information theory is a mathematical theory of data communication data presented by Shannon in 1949 [13]. Modern information theory matter in terms of error correction, data compression, cryptography, and communication systems. Entropy of a message can be calculated by the formula [5]:

$$H_e = - \sum_{k=0}^{G-1} P(k) \log_2(P(k)) \quad (3)$$

where:

- H_e : entropy
- G : gray value of the image (0..255)
- $P(k)$: incidence probability of k symbol

Practically, if an information is encrypted and in scrambled conditions, the ideal entropy value is 7.99902 (≈ 8). Thus the encryption system designed safe from entropy attack. However, if the entropy value is smaller than 8, it can be said still be able to guess the encryption system [2].

3.3. Histogram Analysis

Color histogram analysis technique is used to view the suitability of the color distribution between plain image and cipher image. If the histogram value has a significant distribution of diversity of cipher image and also have significant differences with plain image histogram, it can be said that cipher image does not give any clues to perform statistical attack on the encryption algorithm.

3.4. Quality of Encryption

Measurement of the encryption quality is done by comparing the pixel values before and after the encrypted image. The higher rate of change of pixels, then the image encryption is said to be more effective and more secure [1], [2], [5]. The size of the encryption quality is expressed as the deviation between the plain image and cipher image. Encryption quality represents the average number of changes per degree of gray. To measure the quality of the encryption used the formula: [1], [2].

$$EQ = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256} \quad (4)$$

where:

- EQ : quality of encryption
- P : plain image
- C : cipher image
- L : gray scale
- $H_L(P)$: number of occurrences for each L in a plain image
- $H_L(C)$: number of occurrences for each L in a cipher image

4. Results and Discussion

To determine the strength of the proposed algorithms, perform by testing and analysis on some examples of images by using a few parameters that have been described in section 3 using Matlab application. Testing was also conducted on cell phones to find out compatibility, memory requirements and speed of encryption and decryption process.

4.1. Visual Test and Histogram Analysis

From the results of visual testing of two different groups of image brightness level and image contrast level using the same key, can be seen in Table 1.

Table 1 shows that the original image can not be seen after the encryption process. The results showed that randomization of color and changes of color intensity are significant. These indicate that the encryption process works well for all groups tested image.

Color histogram analysis is used to view the suitability of the color distribution between plain image and cipher image. The results are shown in Table 2 and 3. Based on visual observation of the plain image and cipher image histogram looks to have the significant diversity and differences distribution with his plain image histogram. Visual test results on the cipher image histogram are also shown the frequency of occurrence of each image intensity values evenly. This suggests that the encryption algorithm used can not provide any clues to do statistical attack by kriptanalysis.

4.2. Statistical Tests

Statistical tests used to measure whether the proposed encryption algorithm is safe enough to be implemented on cell phone. Parameters of statistical tests used for testing are correlation, entropy, quality of encryption, and processing time. Results of statistical tests can be seen in Table 4. Table 4 shows the average value for the two groups of the tested images that the average value of entropy (H_e) was 7.9984. Based on the theory advanced by Jolfae and Mirghadri [7] that if information is encrypted and scrambled so the ideal entropy value is ≈ 8 . Based on that theory, the proposed encryption algorithm is said to be secure from entropy attack or difficult to guess by kriptanalysis because its value is

very close to 8. The strength of an encryption algorithm other than the value measured by the entropy also measured by the correlation value (I_c).

Table 1. Results of visual test






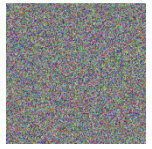

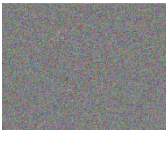

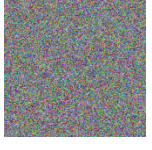



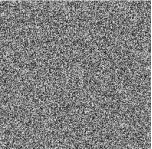






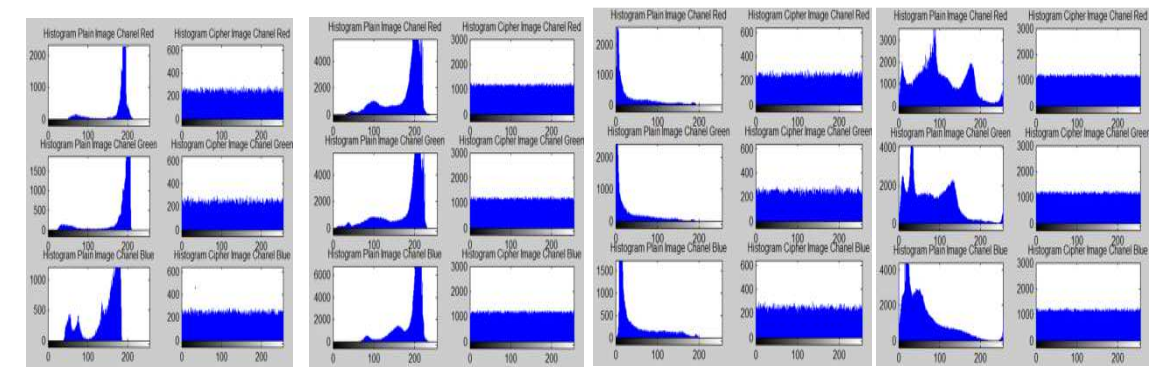
Group of images	256 x 256 pixel		640 x 480 pixel	
	Plain Image	Cipher Image	Plain Image	Cipher Image
Bright	 Jelly.bmp (source:hlevkin.com)		 Airplane.jpg (source:hlevkin.com)	
Dark	 Androm.bmp (source:home.honolulu.hawaii.edu)		 Matador.jpg (source:wikipedia.org)	
Low Contrast	 Baboon.bmp (source:hlevkin.com)		 Kudaponi.jpg (source:kidnesia.com)	
High Contrast	 Crowded.bmp (source:hlevkin.com)		 (personal collection)	

Table 2. Histogram analysis based on differences in image brightness

Bright Image		Dark Image	
			
256 x 256 pixel	640 x 480 pixel	256 x 256 pixel	640 x 480 pixel



This correlation measurement is useful to measure the strength of the relationship between two variables with a scale of 0 to 1. Variables referred to in this study are the image intensity at the plaintext of ciphertext. If the correlation is zero (0), then there is no relationship between two variables. Table 4 shows that the average value of correlation between plain image and cipher image is 0.000254. Since the average correlation value close to zero then the connectedness between plain image and cipher image does not exist. This indicates that the proposed encryption system according to the theory of perfect secrecy suggested by Shannon, i.e the lower correlation between pixels and the higher of entropy value, so that the encryption system is said to be secure [9].

Table 3. Histogram analysis based on differences in image contrast

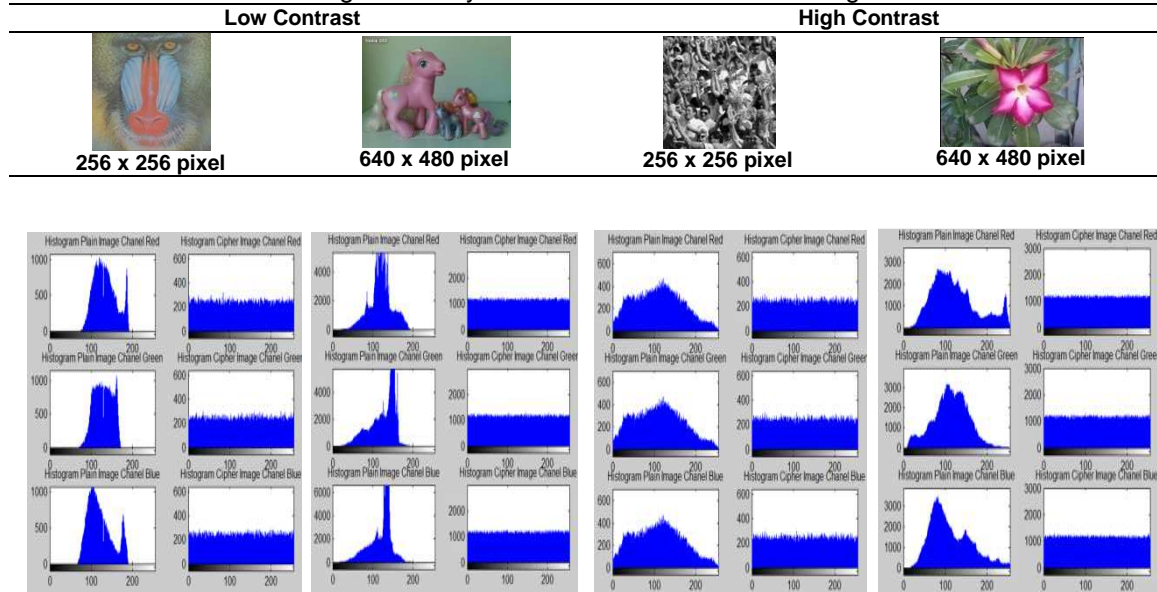


Table 4. Statistical test results

Filename	Pixel size	Filesize (Kb)	Measurement Results			Time (second)	
			He	Eq	Ic	Encrypt	Decrypt
A. airplane.jpg	480 x 640	59	7.9994	1294.87	-0.000091	486.08	485.60
B. Kuda Poni.jpg	480 x 640	34	7.9995	1275.26	0.000219	459.19	473.03
C. Kamboja.jpg	480 x 640	58	7.9994	827.429	-0.000319	461.49	474.34
D. Matador.jpg	480 x 640	63	7.9994	802.156	0.000232	462.18	475.23
Average			7.9994	1049.9288	0.000010	467.24	477.05
E. Androm.bmp	256 x 256	193	7.9975	292.422	0.002759	4.17	6.68
F. Baboon.bmp	256 x 256	192	7.9973	308.966	-0.000119	4.18	6.88
G. Crowded.bmp	256 x 256	193	7.9973	103.984	-0.000671	4.27	6.49
H. Jelly.bmp	256 x 256	193	7.9976	341.294	0.000021	4.18	6.89
Average			7.9974	261.667	0.000497	4.20	6.73
Grand Average			7.9984	655.7976	0.000254		

Description:

- He : Histogram equalization
- Eq : Encryption quality
- Ic : Image correlation

To measure the quality of image encryption is done by comparing the pixel values before and after encrypted, expressed as a deviation between the plain image and cipher image [1]. From the results obtained by testing two groups of image, average quality of the encryption is 655.7976.

Table 4 also shows that the value of encryption quality is high enough which means that its rate of pixels change were high enough so that these systems can be effective and safe. The

results graph of statistical tests which include Histogram Equalization (He), Encryption Quality (Eq), and Image Correlation (Ic) is presented in Figure 3.

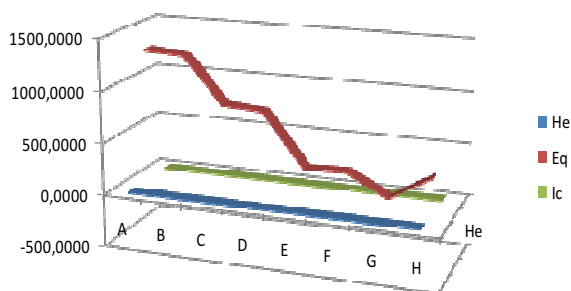


Figure 3. Graph of statistical test results

Table 5. Encryption quality of super encryption, playfair cipher, and vigenere cipher algorithm

Filename	Super Encryption	Playfair Cipher	Vigenere cipher
A	1294,87	871,737	1295,93
B	1275,26	651,753	1278,03
C	827,429	765,156	829,742
D	802,156	690,646	802,201
E	292,422	251,839	293,987
F	308,966	310,029	309,029
G	103,984	108,680	104,891
H	341,294	243,107	341,727

From Table 5 shows that the comparison between the three quality encryption algorithm, which are super encryption algorithm, Playfaircipher, and cipher vigenere relatively the same. Although the quality of the super encryption and vigenere cipher relatively the same, but the level of difficulty to break the encryption becomes increasingly difficult. This was caused by a key randomization using keystream generator.

The next test results are shown in Table 6, which shows a comparison of the encryption quality using super encryption algorithm, by changing the key length. Test results on eight images with a variety of key length suggests that the key length has no significant effect on the quality of encryption. The same relative quality caused by the use of keystream generator to randomize the encryption key. So that regardless of the length of the key, the result will be very random. The best results were obtained on 128 key lengths.

4.3. Testing on Cell Phone

The results of the testing process of encryption and decryption on a cellular phone is shown in Table 5. From Table 5 note the average time for image encryption is 3763.74 milliseconds (\approx 3.76 seconds). While the average time for decryption was 971.625 milliseconds (\approx 0.97 seconds).

Table 6. Relationship between quality encryption and key length

Key length	Encryption Quality (Eq) of image							
	A	B	C	D	E	F	G	H
8	1293,32	1281,1	830,828	804,094	292,604	163,169	103,945	341,406
16	1294,67	1276,01	827,258	804,094	292,328	161,628	104,203	341,122
32	1296,64	1276	830,646	800,284	293,609	161,857	102,242	341,469
64	1295,41	1277,2	825,388	806,159	293,375	162,305	105,078	339,878
128	1295,03	1278,45	827,914	806,414	292,747	163,409	103,906	340,909
256	1293	1277,6	830,992	803,198	292,880	161,013	105,547	340,273

Table 7. Time analysis on cell phone testing

Image	Filename	Pixel size	Filesize (Kbytes)	Process time (milisecond)	
				Encryption	Decryption
A	airplane.jpg	480 x 640	59	1157	1027
B	Kuda Poni.jpg	480 x 640	34	1073	969
C	Kamboja.jpg	480 x 640	58	1001	969
D	Matador.jpg	480 x 640	63	1059	966
E	androm.bmp	256 x 256	193	6688	965
F	baboon.bmp	256 x 256	192	6421	962
G	rowded.bmp	256 x 256	193	6849	965
H	jelly.bmp	256 x 256	193	6662	950
Average time				3763,74	971,625

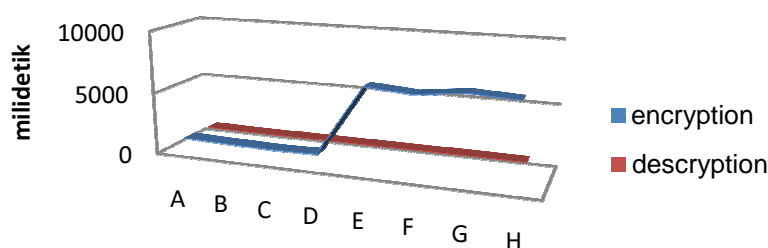


Figure 4. Graph of encryption and decryption time

Graph of encryption and decryption process time in detail is presented in Figure 7. From these results it can be stated that the algorithm is quite effective for the encoding of color image data and can be implemented on mobile phones with Symbian and Bada operating system because it does not require a long processing time.

5. Conclusion

The test results show that visually the encrypted image is not visible anymore due to color randomization and color intensity changes significantly. From the color histogram of plain image and cipher image was seen a significant difference between both of them. So that the proposed encryption algorithm is secure because the value of entropy is very close to 8 which average is 7.9984. The average correlation values between the plain image and cipher image is 0.000254. This indicates that the proposed encryption system according to the theory of perfect secrecy advanced by Shannon because the correlation values near zero. The average quality of the encryption of 655.7976 indicates that the rate of pixels change is high enough so that this system can be said to be effective and safe.

The application also successfully implemented on mobile phone devices with relatively small size (88 Kb) with the JAR file format. The average time required by the image encryption process is 3.76 seconds. While the average time of decryption is 0.97 seconds. It states that the proposed algorithm is quite effective for the encoding of color image data and can be implemented on mobile phones because require less computational resources.

Acknowledgements

This work was supported by the Directorate General of Higher Education, Ministry of National Education, which has funded research activities in accordance with the Letter Agreement Research Assignment Number: 117/SP2H/PL/Dit.Litabmas/IV/2011, through Research Competitive Grant funds.

References

- [1] Gupta K, Silakari S. Choase Based Image Encryption Using Block-Based Transformation Algorithm. *International Journal of Computer and Network Security*. 2009
- [2] Jolfaei A, Mirghadri A. Image Encryption Using Chaos and Block Cipher. *Computer and Information Science*. 2011.
- [3] Abrihama D. Keystream Vigenere Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator. Program Studi Informatika ITB. Bandung. 2008
- [4] Ismail I A, Mohammed A, Hossam D. How To Repair The Hill Cipher. *Journal of Zhejiang University SCIENCE A*. <http://www.zju.edu.cn/jzus>. 2006.
- [5] Krikor L, Baba S, Arif T, Shaaban Z. Image Encryption Using DCT and Stream Cipher. *European Journal of Scientific Research*. <http://www.eurojournals.com/ejsr.htm>. 2009: 47-57.
- [6] Setyaningsih E. Penyandian Citra Menggunakan Metode Playfair Cipher. *Jurnal Ilmiah Nasional Jurnal Teknologi*. 2009; 2(2): 213-217.
- [7] Setyaningsih E. Konsep Superenkripsi Untuk Penyandian Citra Warna Menggunakan Kombinasi Hill Cipher dan Playfair Cipher. *Jurnal Ilmiah Nasional SITRORIKA*. 2010: 38-48.

-
- [8] Suhartana I K G. Pengamanan Image True Color 24 Bit Menggunakan Algoritma Vigenere Cipher Dengan Penggunaan Kunci Bersama. *Ejurnal. Universitas Udayana Bali*. 2008.
 - [9] Younes M A B , Jantan A. Image Encryption Using Block-Based Transformation Algorithm. *IAENG International Journal of Computer Science*. 2008.
 - [10] Sun J., Wang Y., Wu X., Zhang X., Gao H. A New Image Segmentation Algorithm and It's Application in lettuce object segmentation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(3).
 - [11] Akram U. Retinal Image Preprocessing: Background and Noise Segmentation. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(3).
 - [12] Feng W., Bao W. An Improved Technology of Remote Sensing Image Fusion Based Wavelet Packet and Pulse Coupled Neural Net. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(3).
 - [13] Stinson R Douglas. *Cryptography Theory and Practice*, London: CRC Press. Inc.1995