International Journal of Engineering & Technology, 7 (2.2) (2018) 62-64

International Journal of Engineering & Technology

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

Research Paper

Image encryption using vigenere cipher with bit circular shift

Arief Susanto[1], Tutik Khotimah[1], Muhammad Taufik Sumadi[2], Joko Warsito[2], Rihartanto[2]*

[1]Faculty of Engineering, Muria Kudus University, Kudus, Indonesia
[2]Department of Information Technology, State Polytechnic of Samarinda, East Kalimantan, Indonesia
**Corresponding author E-mail: rihart.c@gmail.com*

Abstract

Cryptography is a method of securing text data, images and sound in order to secure its confidentiality and to minimize data stealing, attack, etc. The purpose of this study is to improve classic Vigenere cipher using bit circular shift on image encryption. This experiment uses both RGB and grayscale images as samples and shows that Vigenere cipher with bit circular shift has better performance when encrypting an image both visually and its randomness. It is obtained the MAE values of images of final encryption process are 81.702637 of RGB and 73.678756 of grayscale, and the final decryption process of 0 for both images. The randomness of images of the final encryption process is shown by its correlation coefficient values; it is 0.033857 of RGB and -0.058501 of grayscale.

Keywords: *Vigenere chipper; bit circular shift; image encryption.*

1. Introduction

Data and information are important commodities both for individual and organizational. Information can be presented in form of text, image, audio, video or mix of it. Some information is available and accessible to the public where some are secrets. In order to secure information, cryptography can be applied. Cryptography is the science of keeping secrets secret [1], [2]. It is the science of secret writing with the goal of hiding the meaning of a message[3].

While securing information, cryptography can be divided into two processes. It is encryption and decryption. Encryption is a process of hiding the information and decryption is the process of extracting the information from encrypted information. To implement encryption and decryption, it needs an appropriate encryption and decryption algorithm[4]. In this paper, Vigenere cipher will be used for image encryption and decryption. Vigenere cipher is a classic cryptography implemented symmetric keys. It is a polyalphabetic substitution that works based on Caesar cipher implementing Vigenere Square[5].

In this digital world, an image is a collection of the pixel which has different intensity values[6]. Each image consists of $n*m$ number of pixel, where n is the number of rows and m is the number of columns. A pixel (**pic**ture **el**ement) is a small block that represents the amount of gray intensity to be displayed for that particular portion of the image. For most images, pixel values are integers that range from 0 (black) to 255 (white). For example, an enlarged image with 15 x 15 pixels shown in Figure 1 that shows its gray intensities and Figure 2 that show its corresponding intensity values.

An RGB image or a true color image is an image in which each pixel has three components value[7]. These components are red (R), green (G) and blue (B), so that the RGB image are *m-by-n-by*-3 array of class uint8, uint16, single, or double whose pixel values specify intensity values. The multiple values may correspond to different color intensities as shown in Figure 3.

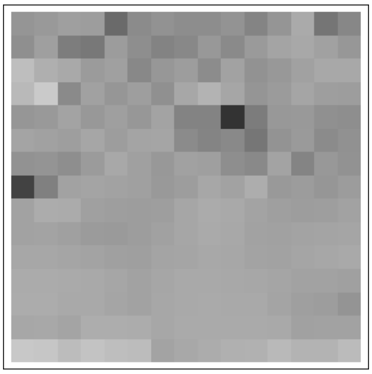
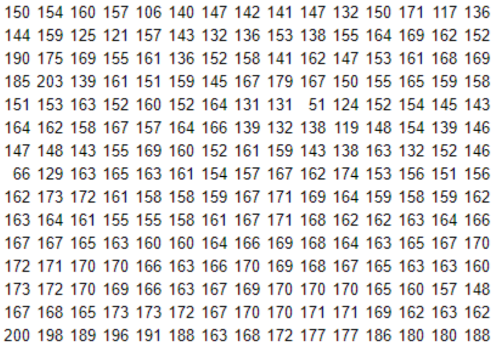


Fig. 1: The 15 x 15 pixel of an enlarged image



```
150 154 160 157 106 140 147 142 141 147 132 150 171 117 136
144 159 125 121 157 143 132 136 153 138 155 164 169 162 152
190 175 169 155 161 136 152 158 141 162 147 153 161 168 169
185 203 139 161 151 159 145 167 179 167 150 155 165 159 158
151 153 163 152 160 152 164 131 131  51 124 152 154 145 143
164 162 158 167 157 164 166 139 132 138 119 148 154 139 146
147 148 143 155 169 160 152 161 159 143 138 163 132 152 146
 66 129 163 165 163 161 154 157 167 162 174 153 156 151 156
162 173 172 161 158 158 159 167 171 169 164 159 158 159 162
163 164 161 155 155 158 161 167 171 168 162 162 163 164 166
167 167 165 163 160 160 164 166 169 168 164 163 165 167 170
172 171 170 170 166 163 166 170 169 168 167 165 163 163 160
173 172 170 169 166 163 167 169 170 170 170 165 160 157 148
167 168 165 173 173 172 167 170 170 171 171 169 162 163 162
200 198 189 196 191 188 163 168 172 177 177 186 180 180 188
```

Fig. 2: The intensity values of 15x15 pixel of an enlarged image

According to its compression algorithm, the image can be classified into lossless type and lossy type. A lossless type stores an exact representation of the original image in a smaller number of bytes that can be expanded back to its uncompressed form using a corresponding decompression algorithm. Meanwhile, a lossy type stores an approximation representation of the original image and while it expanded back to its uncompressed form, it is slightly different but visually is the same. PNG and BMP are samples for lossless type while JPG is a sample of lossy type.

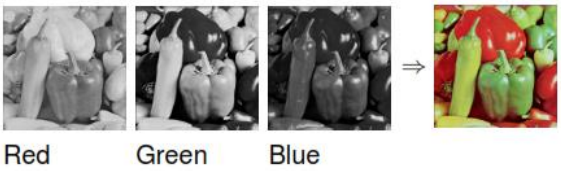


Fig. 3: Three components of an RGB image

Many studies have implemented in order to secure image. For example, implementing Rubik's Cube Principle that scrambling the original image then applied an XOR operator using two secret keys[8]. Sajid[6] divides the original image into some smaller images, encrypted and sent part by part. Meanwhile, Vigenere with Playfair cipher has been exploited for image encryption on a mobile phone[9], [11]. The aim of this paper is to show that the addition of bits circular shift on Vigenere cipher can produce a good result on image encryption.

2. Experimental details

In this study, an image that used as input can be lossless type or lossy type, but lossless type will be used to store the encryption output. As samples for encryption and decryption purpose is lena.jpg with 225x225 pixels in size, both RGB and grayscale. The original formula of Vigenere cipher for encryption and decryption is [10]

$$C = (P + K) \bmod 26 \quad (1)$$
$$P = (C - K) \bmod 26 \quad (2)$$

The value of 26 is the representation of the number of letter from A to Z, which is then represented by the numbers 0-25 which indicate the position of the letters in alphabetical order

Since the pixel intensity is a number value of 0-255, then the original Vigenere formula need to modify to accommodate these new value range. The modified formula for encryption purpose[9] is

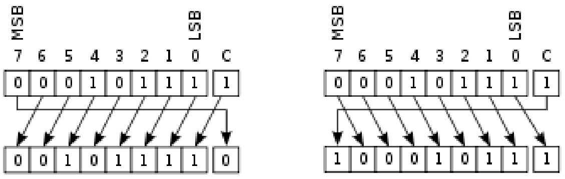
$$C = (P + K) \bmod 256 \quad (3)$$

and for decryption purpose[9] is

$$P = (C - K) \bmod 256 \quad (4)$$

These encryption and decryption process is applied to all intensity values in each pixel.

Furthermore, bit circular shift is applied to improve the encryption result of Vigenere cipher. This step is needed since the encryption result of Vigenere cipher visually still showing the original image, although mathematically has shown a different data. The circular method that used for bit shifting process is rotated no carry as illustrated in Figure 4. In this operation, a bit is rotated as if the left and right ends of the register are joined. Any value on the right ends is taken and placed to the left ends of the register (Figure 4b), and vice versa.



(a). The left circular (b). The right circular

Fig. 4: Rotate No Carry

Implementation of Vigenere cipher and bit circular shift for encryption and decryption purpose is shown in Figure 5.

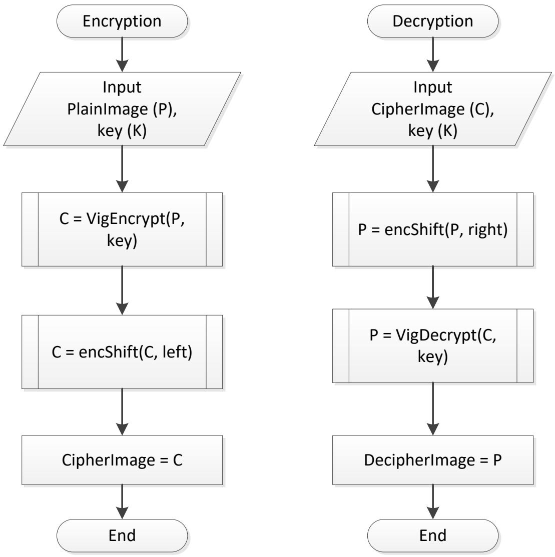


Fig. 5: Flowchart for encryption and decryption

Mean Absolute Error (MAE) and correlation coefficient were used to measure the performance of Vigenere cipher and Vigenere cipher with bit circular shift on images. MAE is used to assess how accurate the result of the decryption is compared with its original image, while correlation coefficient is used to assess how the randomness of cipher image compares to its original.

The correlation coefficient is calculated using the equation

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\ \sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (5)$$

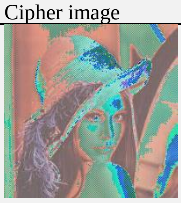
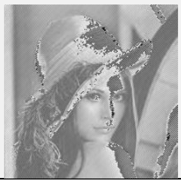
Mean Absolute Error is calculated using the formula

$$MAE = \frac{1}{n}\sum_{i=0}^{n}|x_i - y_i| \quad (6)$$

3. Results and discussion

In this study, the program for the encryption-decryption process is created using Python programming implementing OpenCV and numPy. Encryption conducted on intensity values on each color component in RGB image or grayscale intensity values in the grayscale image. The encryption result using Vigenere cipher is shown in Table 1 while it using Vigenere cipher with bit circular shift in Table 2. As the key to encrypt and decrypt is 'a1b2c3d4e5'.

Table 1. Encryption Result Using Vigenere Cipher

Plain image	Cipher image	MAE	Corr. Coef
		82.233468	0.127643
		73.028997	0.478397

It can be seen from Table 1 that pixel intensity change on RGB image is bigger than that grayscale image, which is indicated by a larger MAE value. Similarly, the randomness of the encryption results of RGB image is much better than the grayscale image, indicated by the coefficient of correlation value that is smaller, i.e. 0.127643. Both encryption results are visually still easy to refer to its originals.

Differ from Vigenere cipher, encryption using Vigenere cipher with bit circular shift gives better results, both visually and data randomness. Visually the encrypted results have not shown the characteristics of the original image. The better randomness is showed by correlation coefficient value of 0.033857 compared to 0.127643 for RGB images and -0.058501 compared to 0.478397 for grayscales.

Table 2. Encryption Result Using Vigenere Cipher with Bit Circular Shift

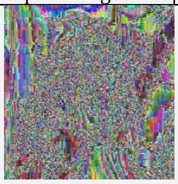
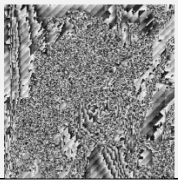
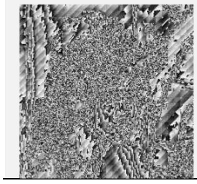
Plain image	Cipher image	MAE	Corr. Coef
		81.702637	0.033857
		73.678756	-0.058501

Table 3. Decryption Result Using Vigenere Cipher with Bit Circular Shift

Cipher image	Decrypted image	MAE	Corr. Coef
		0	1.0
		0	1.0

The decryption result is shown in Table 3. It shows that the MAE value is 0 and correlation coefficient value is 1.0 for both images, indicating that the decrypted images are perfectly matched to its originals.

4. Conclusion

In conclusion, this study has presented the performance of classic Vigenere cipher with or without bit circular shift. The MAE and correlation coefficient are computed on each result and compared to its original. Based on the result obtained image encryption using Vigenere cipher with bit circular shift give a better result than that Vigenere cipher only. A vigenere cipher with bit circular shift produces better randomness image that yields images that are difficult to recognize. Optimizing the circular shift such as pixel-level circular shift is one of the future works that can be conducted in order to investigate a better implementation of encryption-decryption in Vigenere cipher on the image.

References

[1] H. Delfs, K. Paterson, and R. Cramer, *Introduction to Cryptography: Principles and Application*, Third Edit. Berlin: Springer-Verlag GmnH, 2015.

[2] B. Schneier, *Applied Cryptography*, 20th Anniv. Indianapolis: John Wiley & Sons, Inc, 2015.

[3] C. Paar and J. Pelzl, *Understanding Cryptography*. 2010.

[4] R. Dixit and K. Ravindranath, "Encryption techniques & access control models for data security : A survey," *Int. J. Eng. Technol.*, vol. 7, no. 1.5, pp. 107–110, 2018.

[5] A. Saraswat, C. Khatri, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," *Procedia - Procedia Comput. Sci.*, vol. 92, pp. 355–360, 2016.

[6] M. Sajid, Q. Khizrai, and P. S. T. Bodkhe, "Image Encryption using Different Techniques for High-Security Transmission over a Network," *Int. J. Eng. Res. Gen. Sci.*, vol. 2, no. 4, pp. 299–306, 2014.

[7] T. Kumar and K. Verma, "A Theory Based on Conversion of RGB image to Gray image," *Int. J. Comput. Appl.*, vol. 7, no. 2, pp. 5–12, 2010.

[8] K. Loukhaoukha, J. Chouinard, and A. Berdai, "A Secure Image Encryption Algorithm Based on Rubik ' s Cube Principle," *J. Electron. Comput. Eng.*, vol. 2012, 2012.

[9] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Image Encryption on Mobile Phone using Super Encryption Algorithm," *Telkomnika*, vol. 10, no. 4, pp. 835–843, 2012.

[10] N. Sinha, "Improving Security of Vigenère Cipher by Double Columnar Transposition," *Int. J. Comput. Appl.*, vol. 100, no. 14, pp. 6–10, 2014.

[11] A. Jawahir and H. Haviluddin, "An audio encryption using transposition method," International Journal of Advances in Intelligent Informatics, vol. 1, No 2, July 2015, pp. 98-106, 2015.