JTEC

by Andik Setyono

Submission date: 14-May-2019 02:56PM (UTC+0700)
Submission ID: 1130218109
File name: International_Journal_3_JTEC.pdf (1.09M)
Word count: 3749
Character count: 19384

Dual Encryption Techniques for Secure Image Transmission

And[8] Setyono, De Rosal Ignatius Moses Setiadi, and Muljono
Faculty of Computer Science, Dian Nuswantoro University,
207 Imam Bonjol Street, Semarang, Indonesia
andik.setyono@dsn.dinus.ac.id

***Abstract*—Security is the most important thing in [7]nding secret messages through internet media. Cryptography is one of the techniques used for securing the messages by encoding so it cannot be read directly. This research proposes a cryptographic method by combining two cryptographic algorithms namely RSA and Vernam Cipher. The RSA algorithm[19]rength depends on the quality of the key, which is generated by the formulation of two prime numbers *p* and *q*. The result of the formulation can encrypt the image pixel values beyond the boundary. RSA algorithm is modified to work better on the image and to accommodate encryption results with a larger range. For more robust image secu[23], RSA is combined with Vernam Cipher algorithm. To test the performance of the proposed method, the histogram analysis, measuring entropy, and correlation coefficient, and the time required for the computation process were performed. Based on the combined results of both techniques proved that image security has improved because all measuring devices produced satisfactory values.**

***Index Terms*—Image Cryptography; Image Security; Encryption; RSA; Vernam Cipher**

I. INTRODUCTION

The messaging security is of the utmost importance, especially to private and confidential messages. Currently, message delivery can be[7] various forms such as text, image, audio, or video [1] [2]. The Internet is a public network that can be accessed by everyone connected to it [3]. However, not all internet users use the internet properly. There are users who abuse the Internet to commit criminal acts such as data theft.

There are various[4]chniques for securing data transmission on the internet, such as cryptography, st[15]nography, watermarking and digital signatures [4] [5] [6]. Cryptography is a technique for encrypting data [7], steganography is a technique for hiding data [8], watermarking is a technique used to provide copyright protection to the data [1], while digital signatures are used to perform data identification [9].

This research focuses on developing cryptographic methods on digital image. Cryptography has two main processes namely the encryption and decryption [10] [11]. Encryption refers to the process of changing the image to appear random or even damaged, so it has a differ[3]t meaning from the original image. In contrast, decryption is a process to restore the digital im[25]e into its original form. A key is required for performing encryption and decryption processes. [6] Cryptographic algorithm can be symmetric or asymmetric. Symmetric cryptography uses the private key, while asymmetric cryptography uses both private and public keys [8]. The cryptographic process for image is different from text and not all the cryptographic techniques on text can be used in digital image [12]. There are many cryptographic methods on digital image that have been used, such as Achterbahn [4], one-time pad [5] [13], RSA [6] [7], Scrambling System [10] [11] [14], even a combination of two methods or more to create super encryption [15]. Whereby, each method has its own differences and advantages respectively.

RSA is a popular asymmetric cryptography technique. The RSA security level depends on the time it takes to find the private key. To maximize the security, RSA requires a large range of numbers [7]. However, the image pixel values are limited i.e 0 to 255, this will certainly make the RSA variation keys to be limited. This limitation requires modification for R[5] to work more optimal for image encryption.

One-time pad is a symmetrical cryptography technique that uses the Vernam Cipher method. This method is difficult to solve if the used key is at the same length as the message, ra[18]m, and only used once [1] [5].

This study proposed a combination of two cryptographic techniques with double keys to improve the imag[11]ecurity. This research is divided into several sections: Section II presents related works. Section III discusses the literature review. Section IV describes the proposed solution. Section V presents implementation and testing. Finally, Section VI concludes the study.

II. RELATED WORKS

Anane et al. study [7] the performance of RSA algorithm was tested on medical image with sizes of 512 * 512, 256 * 256, and 128 * 128. They used MATLAB and Maple tools applications. Based on the testing results, RSA algorithm works well for encryption process of medical image as it takes less than one second to encrypt an Image. Whereby, the decryption process takes a longer time about 22 seconds for image size of 512 * 512.

Shukla et al. [13] conducted cryptographic research using one-time pads algorithm (Vernam Cipher). They used text messages with sizes 100, 1000, 10000 and 100000 characters. The key is generated randomly with key length equal to the message length. The testing results showed that the proposed algorithm works well and it is very difficult to decrypt the text message without knowing the keys used.

The RSA algorithm was proposed in [16]. It was combined with wavelet transform watermarking techniques to improve the security of medical i[22]es. The used medical images were of grayscale type with size 512 * 512 while the watermark was a grayscale image with size 64 * 64. The RSA algorithm was applied to the watermark image for improving its security. The combined methods can improve the security

in unsafe networks.

Nkapkop et al. [6] proposed a combination of chaos and RSA cryptographic methods on digital images to improve their security. The tested Image size is 512 * 512 with grayscale type. RSA algorithm was applied first on the image followed by the chaos algorithm. However, the combination of two encryption algorithms requires two types of keys, namely RSA key and chaos lock. The testing results used the 2.2Ghz i5 processor took about two seconds to process key pairing, encryption, and decryption. This shows that the combination of methods runs fast enough.

In this research, RSA and Vernam Cipher algorithms are combined for securing digital images as they are difficult to solve. RSA is chosen because it is a popular and reliable asymmetric algorithm, while Vernam is chosen because it has the power on random key.

III. Literature Review

A. Rivest Shamir Adleman (RSA)

RSA is a cryptographic technique that involves two kinds of keys, namely private and public keys [17]. RSA stands for Rivest Shamir and Adleman and it is a popular asymmetric cryptographic algorithm for securing data [16]. Data security depends on the key used, because the use of strong key makes it more difficult to decrypt the data. Public key used in RSA is not secret, but the private key must be kept secret so the encrypted message cannot be decrypted [6]. Both keys values must be different with large range of values to make the decryption process more complicated. RSA keys can be generated by mathematical formulas as described in the following steps.

1. Choose two random primes defined as p and q. The prime numbers used should be large numbers for a higher level of security.

2. Calculate value of n by multiplying p and q, using (1).

$$n = p \times q \tag{1}$$

3. Calculate the equivalent value of n using (2).

$$\emptyset(n) = (p-1) \times (q-1) \tag{2}$$

4. Choose a prime number randomly between 1 to $\emptyset(n)$ which has no divisor factor of $\emptyset(n)$ to get e i.e. the public key.

5. Calculate d private key using (3).

$$(e \times d) mod\ \emptyset(n) = 1 \tag{3}$$

From the above formula, the variable pair(e, n), to obtain the public key and a pair of variables (d, n) to obtain the private key.

Furthermore, the encryption process can use (4), while the decryption process can use (5).

$$C = P^e mod\ n \tag{4}$$

$$P = C^d mod\ n \tag{5}$$

where C is ciphertext and P is plaintext.

B. Vernam Cipher

Vernam Cipher is part of a block cipher in classical cryptography using XOR operation. It can be unsolved algorithm if it qualifies these terms a) the key length must be same as the length of the plaintext, b) the used key must be random and c) should be used only once [13]. Cryptographic techniques can also be imposed on digital image [5] and [1]. The Vernam cipher algorithm is quite simple but with the key strength of cryptography makes it so difficult to solve [8]. Moreover, to perform the encryption process use (6) and for the decryption process use (7).

$$E(x) = (P(x) + K(x))\ mod\ z \tag{6}$$

$$D(x) = (C(x) - K(x))\ mod\ z \tag{7}$$

IV. Proposed Solution

A. Proposed Encryption Scheme

To provide layered security to the message image, the proposed method requires three inputs i.e. message image, RSA key, and Vernam key. Figure 1 illustrates the process of image encryption.

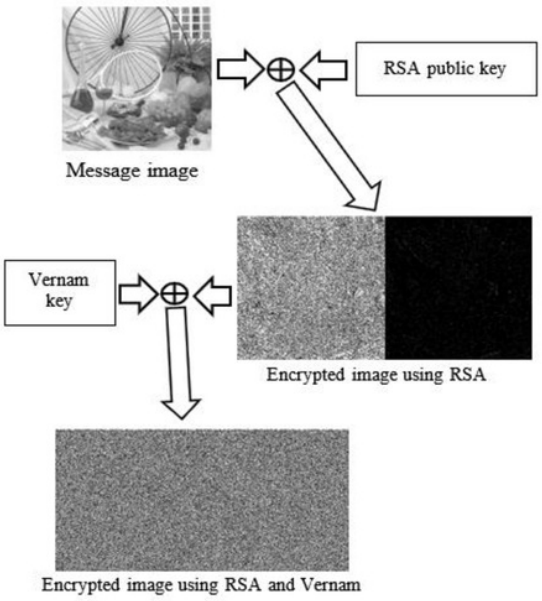

Figure 1: Proposed Encryption Scheme

The proposed message encoding scheme is as follows:

1. Create RSA keys using formulas (1), (2) and (3).
2. Read the message image of m * n size.
3. Encrypt the message image using (4). When performing this encryption, the pixel values will exceed 255 or $2^8 - 1$, so that the values will not be lost when stored. The encrypted values are divided and stored into two image pixels.
4. With the use of two image pixels for storage, the encrypted values can accommodate up to $2^{16} - 1$. The encryption result will produce an image size 2 m * n.
5. Create a Vernam key with a random function and a key

size same as image size after being encrypted with RSA. This is done to make the decryption process more difficult, because the key size is larger than the original image size.

6. Perform the Vernam encryption process by using the formula (6).

B. Proposed Decryption Scheme

The image decryption process requires three inputs including an encrypted message image, RSA private key, and Vernam key. Similar to the encryption process, the image decryption process is done with two algorithms. Vernam algorithm is done first followed by RSA algorithm. Following is a detailed step of the decryption process.

1. Read the encrypted message image and the Vernam key.
2. Perform Vernam decryption process first with the Equation (7).
3. Take the value of two pixels Vernam decryption image, then do the decryption process RSA using the Equation (5).
4. From the decryption of two pixels obtained pixel reconstruction image value with the range 0-255. Save the decryption on a new pixel so that the image size m * n matches the original image.

Figure 2 illustrates the process of decrypting the message image.

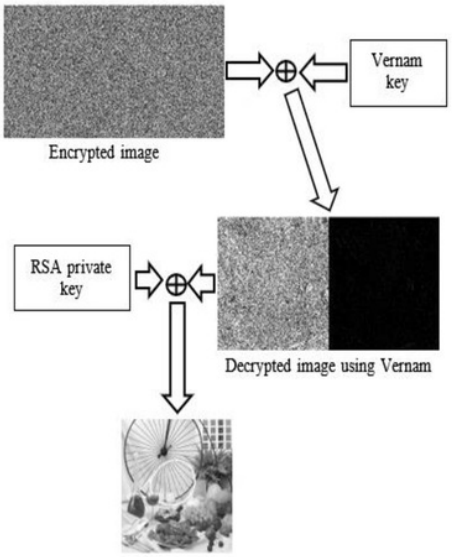

Figure 2: Proposed Decryption Scheme

V. IMPLEMENTATION AND TESTING

In this study, the image encryption method will be implemented on a grayscale image with a size of m * n, where m and n = 256. The image message used is standard image that is used in image processing research. This research can be as reference to other researches. Figure 3 shows the images messages that are tested in this research. It also shows an image histogram; the histogram is used to perform analysis and comparison with the encrypted image histogram.

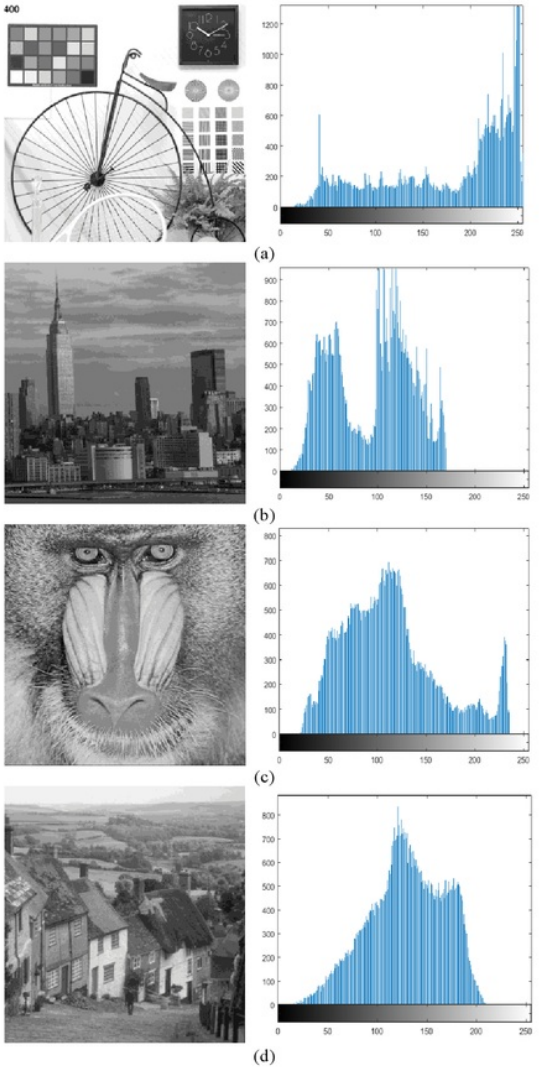

Figure 3: Message image used with this histogram {(a) bicycle; (b) city; (c) mandrill; (d) gold hill}

The next stage is the encryption process in accordance with the proposed method, namely RSA encryption followed by Vernam encryption. For example, the implementation of encryption of bicycle image message made RSA key with value p = 19 and q = 23, then got value n = 437, Ø (n) = 396. The public key used (103, 437) and the private key used (223, 437). Then, we get the result of image encryption with size 2m * n, as shown in Figure 4. Based on the image encryption results by using modified RSA algorithm, it appears that the image seemed like multiplied by two. On the left side, the image is brighter and on the right side, the image appears darker. This is because one image pixel is split into two pixels. This is applied by RSA encryption values with relatively larger p and q values for accommodated purposes. The larger p and q values affect the number of RSA key variations; thus, RSA encryption becomes more robust.

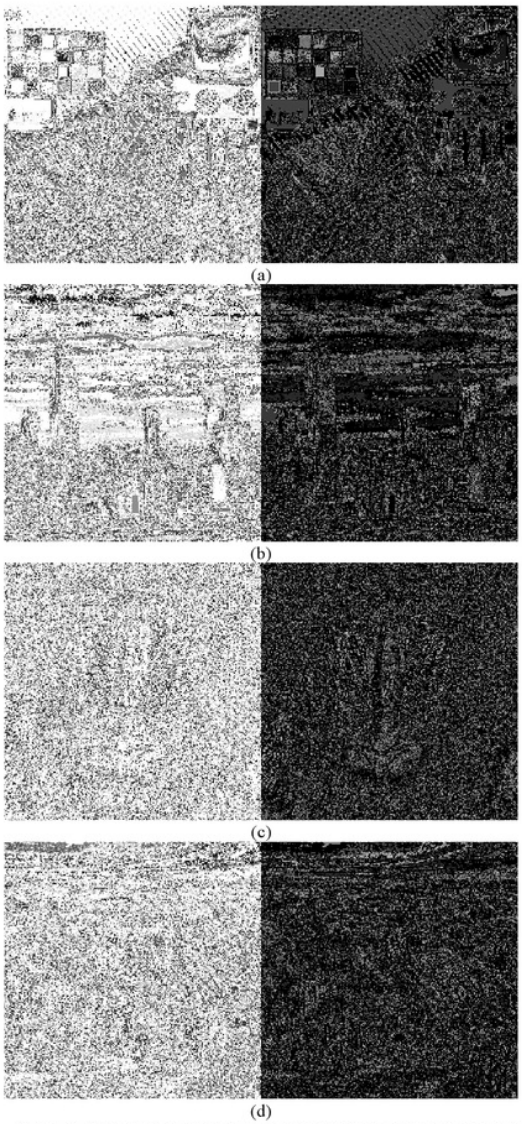

Figure 4: Encrypted image using modified RSA algorithm {(a) bicycle; (b) city; (c) mandrill; (d) gold hill}

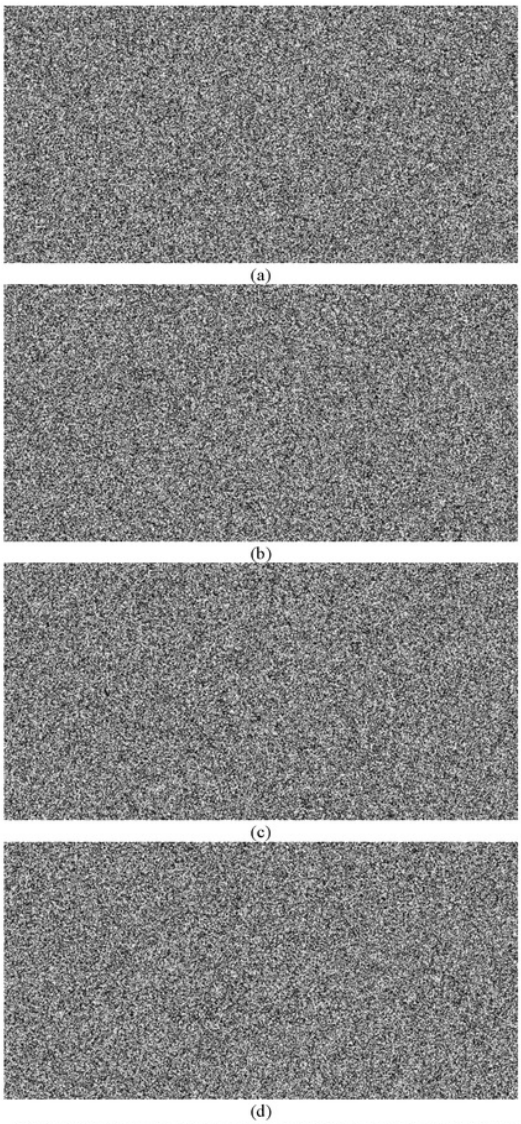

Figure 5: Encrypted image using modified RSA algorithm and Vernam Cipher {(a) bicycle; (b) city; (c) mandrill; (d) gold hill}

The Vernam algorithm is then performed to provide double encryption to the image. Why is Vernam encryption done after RSA encryption and not vice versa? This is due to the nature of Vernam encryption that can randomize the image better than RSA. So that, the image of RSA encryption which consists of two images can be mixed into one encrypted image. This technique can deceive the unauthorized party to decrypt the image. The Vernam algorithm will be more secure if the used key is the same as the message size, random, and only once used. Key and message size also greatly affect encryption and decryption processes. A large key and message size will make the decryption process longer and more complicated. However, if the key is known, the encryption and decryption processes using Vernam algorithm can be computed very quickly. This is the second reason why Vernam algorithm is done after the RSA algorithm. Figure 5 shows the image encryption results by using a combination of both algorithms.

Quality of the encryption results can be measured by MSE and PSNR. The value of the MSE is generated by comparing the original image with the encrypted image provided that the size of the two images must be the same, while the value of PSNR is obtained with logarithm values from MSE. The smaller value of PSNR and the greater value of MSE indicate the encryption quality is better. But, the encryption result of the proposed solution makes the image form changing, where the original size of m * n changes to be 2m * n, so it cannot be measured with MSE and PSNR. Another way to measure the quality of encryption results is by analyzing the histogram and measuring the entropy values. Computational performance should also be measured to determine how long time it takes to perform the encryption process. Time taken to get the encrypted image is measured by tic toc function, while histogram analysis is done by using the imhist function in Matlab. Figure 6 shows the histogram results of the original message image and the encrypted message image.

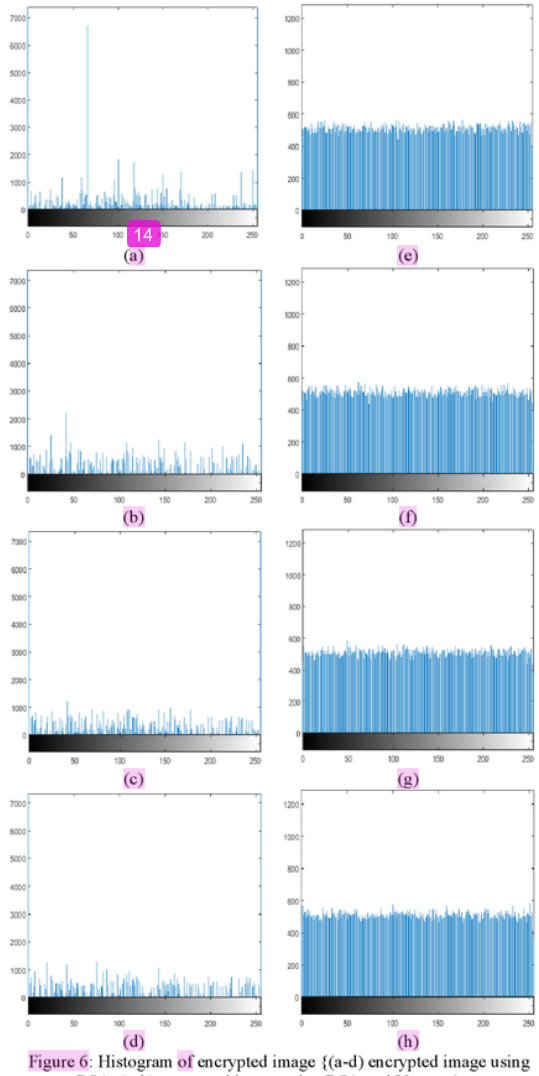

Figure 6: Histogram of encrypted image {(a-d) encrypted image using RSA; (e-h) encrypted image using RSA and Vernam}

Based on Figure 6, the image histogram after encryption changes drastically. Statistically, there is a striking difference between image messages and RSA encryption images, however, the distribution of pixel values is relatively not uniform. The distribution of pixel values appears relatively uniform after Vernam encryption performed, as shown in Figure 6 (e-h). Uniform distribution of pixel values in RSA and Vernam encryption histograms proves that the propos 2 method has good quality. Measurement of the quality of encryption is also calculated by entropy. Entropy is a possible probability that the encrypted image contains information about the key so that the encrypted image can be mathematically decrypted. Entropy can be calculated by the Equation (8).

$$E = -\sum_{x=0}^{G=255} p(x)\, log_2(p(x)) \qquad (8)$$

where: E = Entropy
G = range of pixel value
$p(x)$= incidence probability

The perfect entropy value is 13 good encryption should yield an entropy value close to 8. Table 1 shows the results of entropy on the proposed method.

Table 1
Entropy of Encrypted Message Image

Image	RSA Only	RSA and Vernam
Bicycle	4.8888	7.9984
City	4.8814	7.9982
Mandrill	4.9772	7.9982
Gold hill	5.0536	7.9983
Average	4.9503	7.9983

Based on Table 1 it appears that the average result of entropy is 7.99, the value is very close to 8, so it will minimize the probability of encrypted image can be decrypted by the irresponsible party. On the computing performance side, the proposed method is measured by the tic toc function of Matlab, table 2 shows the results of the time required for the computation of the encryption process

Table 2
Time Taken to get Encrypted Message Image (in seconds)

Image	RSA	Vernam	Total Time
Bicycle	1.27572	0.00164	1.27736
City	1.19524	0.00784	1.20308
Mandrill	1.38496	0.00214	1.38710
Goldhill	1.31119	0.00279	1.31398
Average	1.29178	0.00360	1.29538

The used processor for computing process in this research is Intel Core i3 with the memory of 4 GB. Based on Table 2, the required encryption time is only 1.29 seconds, it proves that the proposed method has a fast computing performance. The next test is done in the decryption process. To measure the decryption quality used correlation coefficient which can be calculated by the Equation (9).

$$cc = \frac{\sum_m \sum_n (M_a - \overline{M_a})(M_b - \overline{M_b})}{\sqrt{(\sum_m \sum_n (M_a - \overline{M_a})\,(\sum_m \sum_n M_b - \overline{M_b})}} \qquad (9)$$

where: $\sum_m \sum_n$ = sum of matrix value with size m*n
M_a = Matrix of message image
M_b = Matrix of recover message image

16 he correlation coefficient is a formula to calculate the correlation between the original and the decrypted image. The perfect correlation coefficient value is 1 whereas the worst value is 0. Table 3 shows the correlation coefficient of the decryption of all image messages tested in this study.

Table 3
Correlation Coefficient of Recover Message Image

Image	Correlation Coefficient
Bicycle	1
City	1
Mandrill	1
Gold hill	1

Based on Table 3, it can be concluded that all images can be decrypted perfectly. While the time required to perform the image, decryption is shown in Table 4.

Table 4
Time taken to get Decrypted Message Image (in seconds)

Image	RSA	Vernam	Total Time
Bicycle	1.20885	0.00089	1.20974
City	1.14935	0.00123	1.15058
Mandrill	1.24785	0.00089	1.24874
Gold hill	1.16773	0.00102	1.16875
Average	1.19344	0.00101	1.19445

Table 4 shows that the required decryption time in the proposed method for the tested image is very fast with an average value of 1.19 seconds.

VI. CONCLUSION

This research combines improved RSA algorithm and Vernam algorithm. The improved RSA algorithm can increase the variation of public and private keys values during the encryption process, as well as changing the image shape making the message more difficult to guess. These results are combined with the Vernam algorithm and a large random key size. The result makes the encryption more complicated as evidenced by the uniform distribution values in the histogram and the excellent entropy value of 7.99. Moreover, reasonable fast computing time and light calculation process allow this method to be implemented on mobile devices.

REFERENCES

[1] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 15, no. 4, pp. 1987-1995, 2017.

[2] S. Liu, C. Chen, Y. Chen and H. Wang, "Hybrid Encryption Algorithm Based on Spatial and Gray Level Information," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 15, no. 3, pp. 569 - 575, 2015.

[3] A. Setyono, D. R. I. M. Setiadi, and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in *International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Semarang, 2017.

[4] A. Belmeguenai, O. Berrak and K. Mansouri, "Image Encryption using Improved Keystream Generator of Achterbahn-128," in *Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, 2016, Rome.

[5] M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari and S. Astuti, "An Improved Secure Image Hiding Technique using PN-Sequence based on DCT-OTP," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[6] J. D. D. Nkapkop, J. Y. Effa, A. Toma, F. Cociota and M. Borda, "Chaos-based Image Encryption using the RSA keys Management for an Efficient Web Communication," in *IEEE International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, 2016.

[7] N. Anane, M. Anane, H. Bessalah, M. Issad and K. Messaoudi, "RSA based Encryption Decryption of Medical Images," in *International Multi-Conference on Systems Signals and Devices (SSD)*, Amman, 2010.

[8] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[9] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in *International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)*, Yogyakarta, 2017.

[10] P. Takkar, A. Girdhar, and V. Singh, "Image Encryption Algorithm using Chaotic Sequences and Flipping," in *International Conference on Computing, Communication, and Automation (ICCCA)*, Greater Noida, 2017.

[11] Y. Zhang, "A Chaotic System Based Image Encryption Scheme with Identical Encryption and Decryption Algorithm," *Chinese Journal of Electronics,* vol. 26, no. 5, pp. 1022 - 1031, 2017.

[12] H. Shuangshuang and L.-Q. Min, "A Color Image Encryption Scheme Based on Generalized Synchronization Theorem," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 12, no. 1, pp. 685 - 692, 2014.

[13] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman and G. Varadan, "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem," in *International Conference on Machine Intelligence and Research Advancement (ICMIRA)*, Katra, 2013.

[14] Z. Yunpeng, S. Peng, X. Jing and H. Yunting, "Color Image Encryption Solution based on The Chaotic System of Logistic and Henon," in *International Conference on Software and Data Technologies*, Piraeus, 2010.

[15] E. Setyaningsih and C. Iswahyudi, "Image Encryption on Mobile Phone Using Super Encryption Algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 10, no. 4, pp. 835-843, 2012.

[16] P. Kishore, N. Venkatram, C. Sarvya and L. Reddy, "Medical Image Watermarking using RSA Encryption in Wavelet Domain," in *International Conference on Networks & Soft Computing (ICNSC)*, Guntur, 2014.

[17] P. V. Nadiya and B. M. Imran, "Image Steganography in DWT Domain using Double-Stegging with RSA Encryption," in *International Conference on Signal Processing Image Processing & Pattern Recognition (ICSIPR)*, Coimbatore, 2013.

JTEC

ORIGINALITY REPORT

12%	3%	7%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Brawijaya Student Paper	2%
2	Eko Hari Rachmawanto, Rofi' Syaiful Amin, De Rosal Ignatius Moses Setiadi, Christy Atika Sari. "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size", 2017 International Seminar on Application for Technology of Information and Communication (iSemantic), 2017 Publication	1%
3	Submitted to National Institute of Technology, Silchar Student Paper	1%
4	Yani Parti Astuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari. "Simple and secure image steganography using LSB and triple XOR operation on MSB", 2018 International Conference on Information and Communications Technology (ICOIACT), 2018 Publication	1%

5	Submitted to Universitas Diponegoro Student Paper	1%
6	Submitted to (school name not available) Student Paper	1%
7	De Rosal Ignatius Moses Setiadi, Heru Agus Santoso, Eko Hari Rachmawanto, Christy Atika Sari. "An improved message capacity and security using divide and modulus function in spatial domain steganography", 2018 International Conference on Information and Communications Technology (ICOIACT), 2018 Publication	1%
8	Andik Setyono, Siti Nur Aeni. "Development of Decision Support System for Ordering Goods using Fuzzy Tsukamoto", International Journal of Electrical and Computer Engineering (IJECE), 2018 Publication	1%
9	www.kidpsy.ru Internet Source	<1%
10	Submitted to Indiana University Student Paper	<1%
11	Submitted to Higher Education Commission Pakistan Student Paper	<1%

12	Yuuki Watanabe, Yuhei Takahashi, Hiroshi Numazawa. "Graphics processing unit accelerated intensity-based optical coherence tomography angiography using differential frames with real-time motion correction", Journal of Biomedical Optics, 2013 Publication	<1%
13	Lecture Notes in Computer Science, 2015. Publication	<1%
14	www.icrwhale.org Internet Source	<1%
15	kinetik.umm.ac.id Internet Source	<1%
16	Boukhatem Mohammed Belkaid, Lahdir Mourad, Cherifi Mehdi, Ameur Soltane. "Secure transfer of medical images using hybrid encryption: Authentication, confidentiality, integrity", International Conference on Computer Vision and Image Analysis Applications, 2015 Publication	<1%
17	Rizky Damara Ardy, Oktaviana Rena Indriani, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto. "Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)", 2017 International	<1%

Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), 2017
Publication

---

18 Giovani Ardiansyah, Christy Atika Sari, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto. "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm", 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2017 <1%
Publication

---

19 Kuang Tsan Lin, Sheng Lih Yeh. "Hiding a Covert Digital Image by Assembling the RSA Encryption Method and the Binary Encoding Method", Mathematical Problems in Engineering, 2014 <1%
Publication

---

20 www.iraseat.com <1%
Internet Source

---

21 Yong Zhang, Yingjun Tang. "A plaintext-related image encryption algorithm based on chaos", Multimedia Tools and Applications, 2017 <1%
Publication

---

22 Submitted to School of Business and Management ITB <1%

Student Paper

23	media.neliti.com Internet Source	<1%
24	Submitted to University of Johannsburg Student Paper	<1%
25	Submitted to BATANGAS STATE UNIVERSITY Student Paper	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		