International Journal of Engineering & Technology, 7 (2.5) (2018) 65-68

International Journal of Engineering & Technology

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

Research Paper

Visual Cryptography with RSA Algorithm for Color Image

Ratnadewi[1]*, Benny Santoso Sugiharto[1], Nuning Kurniasih[2], Dahlan Abdullah[3], Ida Bagus Ary Indra Iswara[4], Darmawan Napitupulu[5], Selfianus Laritmas[6], Erland Mouw[6], Ansari Saleh Ahmar[7], Nanik Kurniawati[8], Robbi Rahim[9]

[1]*Department of Electrical Engineering, Universitas Kristen Maranatha, Bandung, Indonesia*
[2]*Faculty of Communication Sciences, Library and Information Science Program, Universitas Padjadjaran, Bandung, 45363, Indonesia*
[3]*Department of Informatics, Universitas Malikussaleh, Aceh, Indonesia*
[4]*STMIK STIKOM Indonesia, Indonesia*
[5]*Research Center for Quality System and Testing Technology, Indonesian Institute of Sciences*
[6]*Universitas Halmahera, Halmahera Utara, Maluku Utara, Indonesia*
[7]*Department of Statistics, Universitas Negeri Makassar, Makassar, Indonesia*
[8]*The National Archive of The Republic of Indonesia (ANRI), Indonesia*
[9]*Universiti Malaysia Perlis, School of Computer and Communication Engineering, Perlis, Malaysia*
**Corresponding author E-mail:ratnadewi.bandung@gmail.com*

Abstract

RSA algorithm founded by Rivest, Shamir and Adleman is an algorithm that based on the use of factorization of a significant number to its factor, and the element must be the prime number. Factorization used to find the private key. In this paper, the RSA algorithm will be used in a visual cryptographic to encrypt and decrypt a color image. The test will conduct with five different photos. Assessment performed using Structural similarity (SSIM) to compare the matrix value of the initial image with the decrypted image. SSIM generates a value of 1 on all pictures. The proves that the Matrix Value in the initial and after decoded images has the same amount. The image decryption will worsen; can be seen from the smaller SSIM value.

Keywords: *Decryption, Encryption, RSA Algorithm, Visual Cryptography.*

1. Introduction

In recent years, the process of sharing information and data transfer between users has increased greatly[1]–[3]. Therefore threats from third parties who want to access confidential information are of concern to experts[4]–[8]. With the advancement of communication networks, information is transmitted easily over the Internet and many confidential data (images, texts etc) are transmitted. Issues that need to be considered are security, because of the opportunity to steal confidential information by hackers because of weak security in the public network. To handle security issues need to be developed algorithm that can secure data sent over the internet[9]–[12]. With the help of Visual Cryptography, visual information systems can be secure through the internet. The method used combines the benefits of Visual Cryptography and Public key cryptography. Combining these two methods will enhance security in maintaining data confidentiality[13]–[15]. Embedded extended Visual Cryptography also develop to image and have a good result [16]–[18]. The improvement of flip (2,2) image in visual cryptography had been done in this paper. The decryption image have a good image like the original image before encryption[19], [20][21]. Visual Cryptography (VC) is an encryption technique; this technique is used to encrypt secret imagery[17]. Visual Cryptography is divided into two stages of encryption and decryption. Encryption is to convert a secret image into a cipher image being decrypted representing the return stage of cipher image into a secret image. To be able to work, cryptographic visuals require algorithms for encryption and decryption processes. There are many algorithm in cryptography i.e.: AES[22], ElGamal[12], [23] algorithm use in visual cryptography. In this paper is used the RSA algorithm[22], [24], [25]. The RSA algorithm was invented by Rivest, Shamir and Adleman in 1977. RSA algorithms use large-scale factoring into its factors and the factor must be a prime number. Factoring is done to get a secret key. As long as there is no algorithm to find the prime factor of large numbers with easy and fast way then RSA security is guaranteed.

2. Method

The workings of the visual cryptographic with the RSA algorithm contain the key search process, the encryption process and the decryption process[26]–[28]. The first process is the generation of keys with the prime number p and q. With the value of p and q is sought n value with the formula $n = p.q$, then select the value e = 5 and find the value d according to the formula obtained value d = 53. The next process is a secret color image and parsed into RGB components of the original image named Component image red, Component image green and Component image blue[29]. The pixel value of the three images is the input of the encryption formula formed from the preconceived public key.

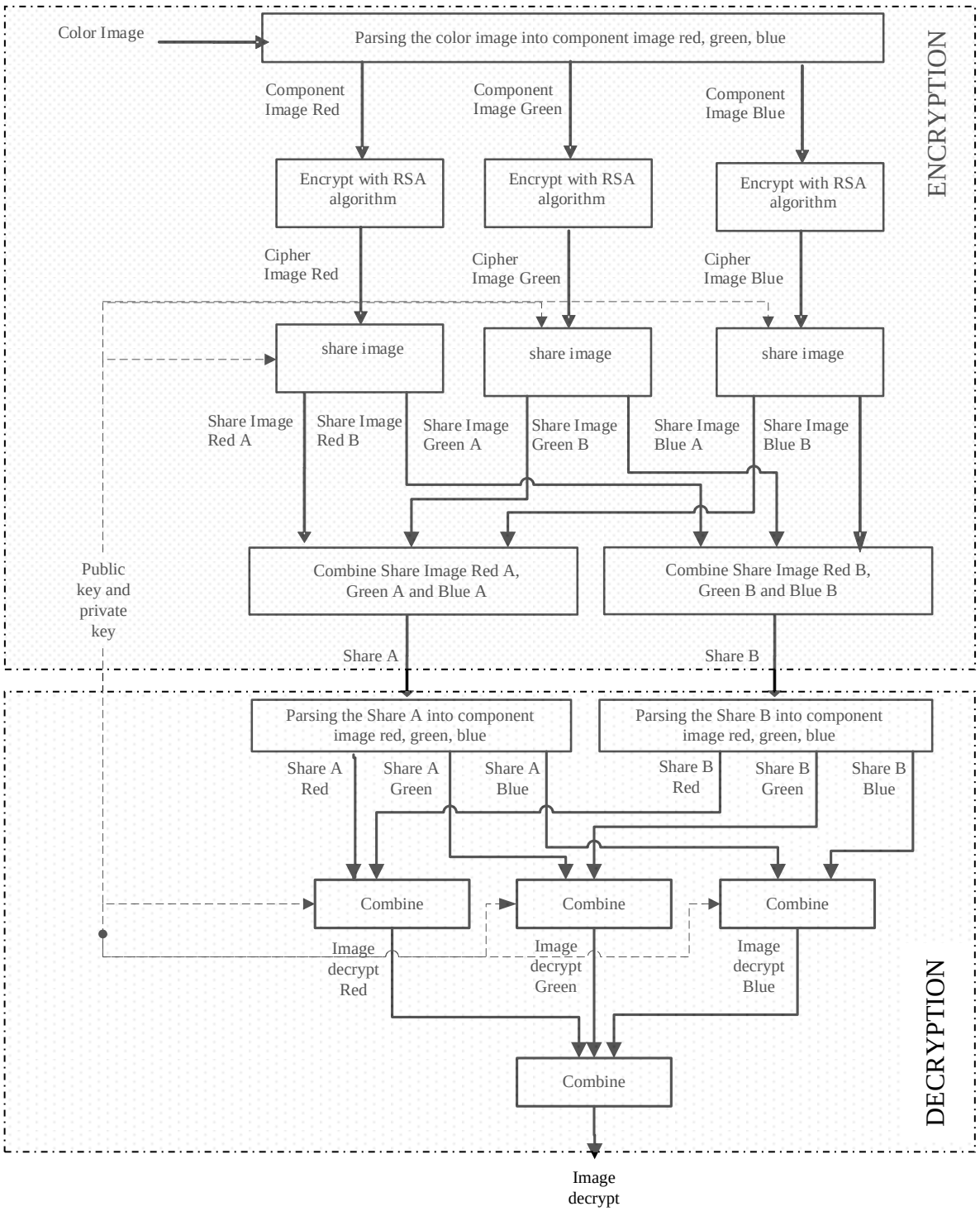

Fig. 1: Block Diagram Visual Cryptography with RSA Algorithm.

In the first encryption process encryption using RSA method with modification method to calculate each cipher image Red, Green, and Blue.[30]

$$cipher\,image = component\,image^{e} \bmod n \quad (1)$$

In the visual cryptography process is sought to share image red A, share image red B, share image green A, share image green B, share image blue A, share image blue B. Combine the share image red A, share image green A, and share image blue A to have image share A. Combine the share image red B, share image green B, and share image blue B to have share image B. Share key is only formed by public key so that it is independent of the effect of pixel value of original image. The decryption process begin by parse the RGB component of share A to share A Red, share A Green, share A Blue, and parsing the RGB component of share B to share B Red, share B Green, share B Blue. The last process is combine share A Red with Share B Red to have image decrypt Red, combine share A green with Share B green to have image decrypt green, and combine share A blue with Share B blue to have image decrypt blue. By combining image decrypt red, image decrypt green, and image decrypt blue, will generate an image decrypt. This process can be seen in Fig. 1.

3. Result and Discussion

In Fig. 2 we describe initial image bird. We need 1.191455 seconds to process the initial image until we have share image A and share image B. The decryption image can be seen in Fig. 3, that we accepted when share image A and share image B combined. This decryption process take 0.723392 seconds and SSIM value is 1. This value SSIM means that between initial image and decryption image is the same. The share image A in Fig. 4 and the share image B in Fig. 5. The decryption image if only one share image A use in process decryption can be seen in Fig. 6. The SSIM value is 0.0454 and decryption time is 0.71384 seconds. In Fig. 7 the decryption image if only one share image B use in process decryption. The SSIM value is 0.0767 and decryption time is 0.710301 seconds. The SSIM value approaching zero means the image does not resemble the original image.

Fig. 2: The original image bird.

Fig.3: The decryption image.

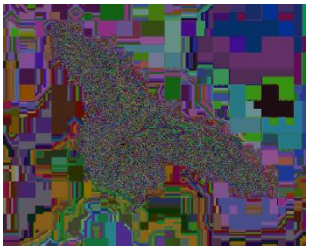

Fig.4: The share image A.

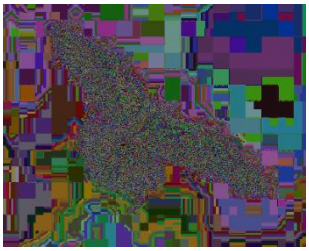

Fig.5: The share image B.

Fig.6: The decryption image if only share image A is accepted.

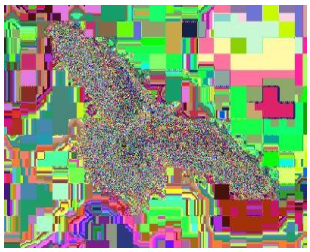

Fig.7: The decryption image if only share image B is accepted.

In this experiment we use 5 images that are bird, scenery, sea, mountain, and leaf. We can count the SSIM from this image decryption. If SSIM value is one then the decryption image is same with the initial image, if SSIM value less than one then the decryption image not as same as the initial image. If the value of SSIM more close to zero, that means the decryption image is more different from the original image. Fig. 8 is the graphics of processing time of encryption and decryption with two share image and decryption with one share image. We can see that encryption process take a long time than decryption time. Fig.9 is the graphics of SSIM decryption with two share image and SSIM decryption with only one share image A or share image B. This proves that the matrix value in the initial image with the decrypted image with two share image has the same value.

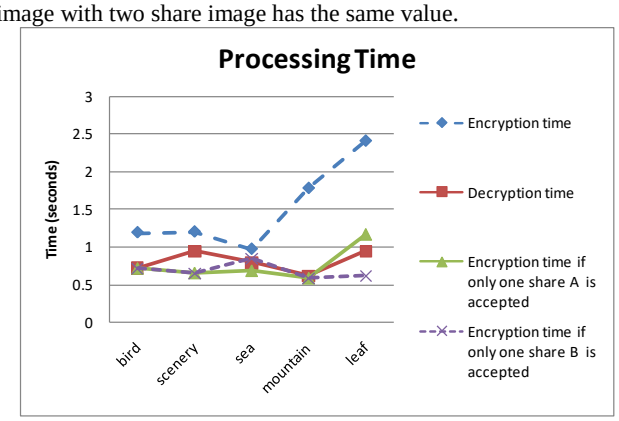

Fig.8: The graphics of processing encryption time and decryption time.

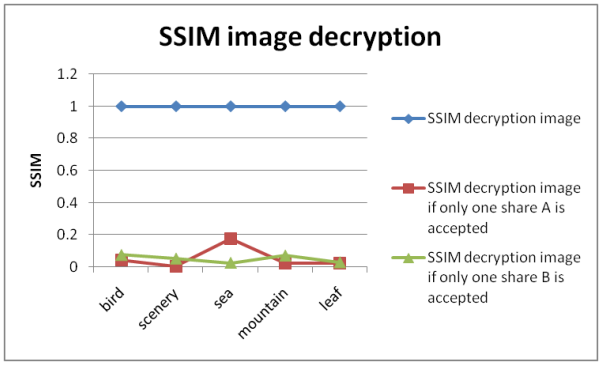

Fig.9: The graphics of SSIM image decryption.

4. Conclusion

Visual cryptographic experiments on color digital imagery with RSA algorithm are successfully implemented. The image quality of the decrypted image is the same as the image before it is encrypted (can be seen from the SSIM testing that is worth 1). If only received one share and decrypted looks very bad results (can be seen the value of SSIM close to 0).

References

[1] D. Abdullah, S. Suwilo, Tulus, H. Mawengkang, and S. Efendi, "Data envelopment analysis with upper bound on output to measure efficiency performance of departments in Malaikulsaleh University,"

J. Phys. Conf. Ser., vol. 890, no. 1, p. 012102, Sep. 2017.
[2] D. Abdullah *et al.*, "A Slack-Based Measures for Improving the Efficiency Performance of Departments in Universitas Malikussaleh," *Int. J. Eng. Technol.*, vol. 7, no. 2, pp. 491–494, Apr. 2018.
[3] H. Hartono, D. Abdullah, and A. S. Ahmar, "A New Diversity Technique for Imbalance Learning Ensembles," *Int. J. Eng. Technol.*, vol. 7, no. 2, pp. 478–483, Apr. 2018.
[4] A. Putera, U. Siahaan, and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016.
[5] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.
[6] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, p. 012003, Apr. 2018.
[7] R. Rahim, N. Kurniasih, M. Mustamam, L. Andriany, U. Nasution, and A. H. Mu-, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.
[8] D. Abdullah, Tulus, S. Suwilo, S. Effendi, and Hartono, "DEA Optimization with Neural Network in Benchmarking Process," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 288, no. 1, p. 012041, Jan. 2018.
[9] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, pp. 366–371.
[10] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012005, Dec. 2017.
[11] M. Blumenthal, "Encryption: Strengths and Weaknesses of Public-key Cryptography," *CSRS 2007*, pp. 1–7, 2007.
[12] A. E. S. Kacaribu and Ratnadewi, "Multiplying cipher images on visual cryptography with ElGamal algorithm," in *2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2015, pp. 159–162.
[13] F. Liu and C. Wu, "Embedded Extended Visual Cryptography Schemes," vol. 2, no. 2, pp. 30–37, 2010.
[14] E. Kartikadarma, T. Listyorini, and R. Rahim, "An Android mobile RC4 simulation for education," *World Trans. Eng. Technol. Educ.*, vol. 16, no. 1, pp. 75–79, 2018.
[15] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, "Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression," *World Trans. Eng. Technol. Educ.*, vol. 15, no. 3, pp. 292–297, 2017.
[16] R. Ratnadewi and P. K. Sari, "ComTech," *Comput. Math. Eng. Apllications*, vol. 7, no. 3, pp. 213–223, 2016.
[17] A. P. Utama Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," *Int. J. Comput. Sci. Eng.*, vol. 3, no. 7, pp. 1–6, Jul. 2016.
[18] Q. Kester, "A Visual Cryptographic Encryption Technique for Securing Medical Images," *arXiv Prepr. arXiv1307.7791*, vol. 3, no. 6, pp. 3–7, 2013.
[19] M. A. M. Maeref, F. Alghali, and K. Abied, "An Advance Visual Model for Animating Behavior of Cryptographic Protocols," *J. Comput.*, vol. 10, no. 5, pp. 336–346, 2015.
[20] R. I. Al-Khalid, R. A. Al-Dallah, A. M. Al-Anani, R. M. Barham, and S. I. Hajir, "A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes," *J. Softw. Eng. Appl.*, vol. 10, no. 01, pp. 1–10, Jan. 2017.
[21] M. Naor and A. Shamir, "Visual Cryptography," in *Proc. Adv. Cryptol.: Eurprocrypt'94, LNCS, 1994, vol. 950, pp. 1–12.*, 1994, pp. 1–12.
[22] G. Singh and Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 6, no. 19, pp. 33–38, 2013.
[23] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985.
[24] T. Cao, D. Lin, and R. Xue, "A randomized RSA-based partially blind signature scheme for electronic cash," *Comput. Secur.*, vol. 24, no. 1, pp. 44–49, Feb. 2005.
[25] S. Garg and M. K. Rana, "A Review on RSA Encryption Algorithm," *Int. J. Eng. Comput. Sci.*, vol. 5, no. 7, pp. 17148–17151, 2016.
[26] S. Bruce, *Applied cryptography*. 1996.
[27] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition," *Network*. pp. 623–631, 1996.
[28] D. Chandravathi and P. V. Lakshmi, "Advanced Homomorphic Encryption for Cloud Data Security," *JOIV Int. J. Informatics Vis.*, vol. 1, no. 4, p. 1, Mar. 2017.
[29] M. Ramalingam and N. A. M. Isa, "A steganography approach over video images to improve security," *Indian J. Sci. Technol.*, vol. 8, no. 1, pp. 79–86, 2015.
[30] H. Delfs and H. Knebl, *Information Security and Cryptography*, vol. 19. 2007.