Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish

Masumeh Damrudi, Kamal Jadidy Aval

Abstract*: *In today's world, confidential information is growing due to various areas of works. Internet is the main area of transmission of digital data, so security must be more considered. Two common ways of providing security is cryptography and steganography. Employing a hybrid of cryptography and steganography enhances the security of data. This paper employs LSB (Least significant Bit) as the steganography algorithm and AES, RSA, DES, 3DES, and Blowfish algorithms as cryptographic algorithms to encrypt a message that should be hidden in a cover image. The results are represented in the form of execution time, PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and the histogram of main and covered image. The experimental results reveal that all the algorithms achieve appropriate quality of stego image. They can be used as cryptographic algorithms to encrypt a message before applying steganography algorithms.

***Index Terms*: Steganography, LSB, AES, RSA**

I. INTRODUCTION

Two main techniques of security area are Cryptography and Steganography. Cryptography converts original information (plaintext) into encrypted information (cipher text) while in steganography, the message which should be secret is hidden into the cover medium which can be image. Steganography is a Greek word which means "covered writing". Cryptography is also a Greek word which means "secret writing"[1].

While the applications on insecure communication environments are increasing by the time, Cryptography has become one of the most important aspect of digital word [2]. There are two common way of cryptography including symmetric key and asymmetric key (public key). Symmetric key uses the same key for encryption and decryption. Asymmetric key employs two keys. Public key for encryption and private key for decryption [3].

Steganography is an effective way to hide data. It can be used in various applications including social, scientific and governmental applications [4]. Steganography is classified into three categories [5]-[8], pure steganography which has no key, secret key steganography with the key which communicating parties exchange the key and public key steganography with a public key and a private key.

Various techniques are available for cryptography and steganography. In this paper, five different algorithms including AES, RSA, DES, 3DES, and BLOWFISH as cryptography technique and LSB as steganography are employed. Using LSB as steganography algorithm, human cannot realize the small changes in patterns visually [9]. Different works on the selected algorithms as cryptographic algorithms and LSB as steganography algorithm are done but there is no work which employs all these algorithms at the same time and on the same environment to compare them on different factors including encryption and decryption time, SNR (Signal to Noise Ratio), PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error) and the histogram. AES, DES, 3DES, and BLOWFISH are employed as symmetric algorithms and RSA is employed as asymmetric algorithm while it is secure using greater key length [10]. The papers including [1], [11]-[19] are based on AES and LSB as their approach. Authors of [15], [19], [20]-[22] employed DES and LSB to hide their information. Researchers of [23-24] worked on 3DES and LSB. The authors of [25]-[27] issued implementations of Blowfish and LSB to have secure data. RSA is used as cryptographic algorithm in [14], [19], [20], [24], [28]-[31]. Nazeh Abdul Wahid et al. only compared DES, 3DES, AES, RSA, and Blowfish based on Guessing Attacks Prevention. Their experimental results show that the perfect choices are: blowfish algorithm in case of time and memory, AES algorithm for confidentiality and integrity, DES as the demand of the application for the network [32].
In this paper, first encryption of data is done by using AES, RSA, DES, 3DES, and Blowfish algorithms which are the most common techniques. Thence the encrypted message is hidden using LSB approach. This method provides two layers of security and it gets harder for the intruders to figure out the original message. Combination of steganography and cryptography enhance the guarantee of protecting data. The Experimental results reveals appropriate quality of stego image.

II. PROPOSED METHOD

In this paper the cryptographic algorithms are the java programs that are imported in MATLAB area. First, the message is converted to ASCII code.

Revised Manuscript Received on September 22, 2019.

Masumeh Damrudi, Computer Science Department, Islamic Azad University, Firoozkooh Branch, 3981838381, Iran.
Kamal Jadidy Aval, Computer Science Department, Islamic Azad University, Firoozkooh Branch, 3981838381, Iran.

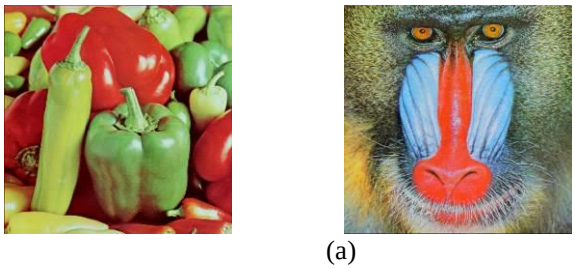
Then the key is generated based on the algorithm that is considered. The key generation of RSA is different from AES, RSA, DES, 3DES, and Blowfish. The RSA is a public key algorithm and needs two different keys; one for encryption and the other one for decryption. Thence the message is encrypted with the mentioned algorithm which is based on java and is imported in MATLAB. The cover image is converted to grayscale and the encrypted message (cipher text) is fed into the LSB algorithm employing the image. The LSB algorithm is implemented in MATLAB. The results of LSB algorithm are converted to an image to be visible. The result is the hidden of encrypted data in the cover image. LSB stands for Least Significant Bit. LSB is the easiest way of image steganography [28]. In this algorithm, the least significant bit of each pixel which is the 8th bit is considered for the encrypted message. The changes in image are not realizable by eyes of human. The following procedure shows the flow of method.

1. Convert the message to ASCII code
2. Key generation
3. Encryption of message (AES, RSA, DES, 3DES, Blowfish)
4. LSB algorithm (encrypted message, cover image)
5. Convert the result to a visible image

III. Experimental Results

In this paper, the cover images are from USC-SIPI [33] dataset for experiments. Two images are selected as cover images which are shown in Fig. 1.

The images are considered to be 512×512 pixels. The message which is considered to be encrypted with the five mentioned algorithm is around 1Kbits. The plaintext is the same for all five cryptographic algorithms. The first comparison is based on encryption time including key generation which are depicted in Table I. These implementations are on MATLAB(R2016a) which import java programs of five algorithms. The implementations of five algorithms are performed on the same environment



(a) (b)

Fig. 1. (a) Peppers (b)Baboon cover images.

Table I. Encryption time of AES, RSA, DES, 3DES, and Blowfish

Algorithm	Key length bits	Encryption time seconds(s)
AES	128	0.003851
DES	56	0.003064
3DES	168	0.003734
Blowfish	128	0.003357
RSA	2048	0.095579

The key length for each algorithm is considered as the most common key length that are still secure and employed in applications. The results represent that the worst encryption time including key generation is for RSA cryptographic algorithm. It is a public key algorithm and needs two key for operation. In the following, the time of decryption of algorithms are shown in Table II.

Table II. Decryption time of AES, RSA, DES, 3DES, and Blowfish

Algorithm	Key length bits	Decryption time seconds(s)
AES	128	0.000691
DES	56	0.000650
3DES	168	0.001036
Blowfish	128	0.000766
RSA	2048	0.001203

The decryption time is less than encryption time due to the key generation is not considered in these times.

The other quality metrics used to evaluate the steganography employing the five cryptographic algorithms and the LSB technique are the signal-to-noise ratio (SNR), peak signal-to-noise ratio (PSNR) and Mean Square Error (MSE). PSNR value defines the image quality. The more the PSNR value is, the higher quality the image has. The PSNR value should not be less than 30dB in decibels [15].

MSE indicates the degree of differences or similarity between original image and steganography image. The less the MSE value of an image is, the better the quality and distortion from the original is [18].

$$MSE = \frac{\sum_{M,N}\left(T(r,c) - T'(r,c)\right)^2}{M*N} \quad (1)$$

Where, M is the total number of rows, N is total number of columns, (r,c) are rows and columns respectively, T is original image T' is the changed image.

Peak Signal to Noise Ratio (PSNR) is the ratio between maximum possible power and corrupting noise that corrupts the representation of the image. Higher is the value, better is the quality of the image [12].

$$PSNR = 10*\log_{10}\left[\frac{R^2}{MSE}\right] \quad (2)$$

R is the maximum fluctuation in the input image data type. Table III depicted The SNR, PSNR and MSE values of AES, RSA, DES, 3DES and Blowfish algorithms and peppers image as the cover image.

Table III. The SNR, PSNR and MSE values of AES, RSA, DES, 3DES, and Blowfish and Peppers as cover image

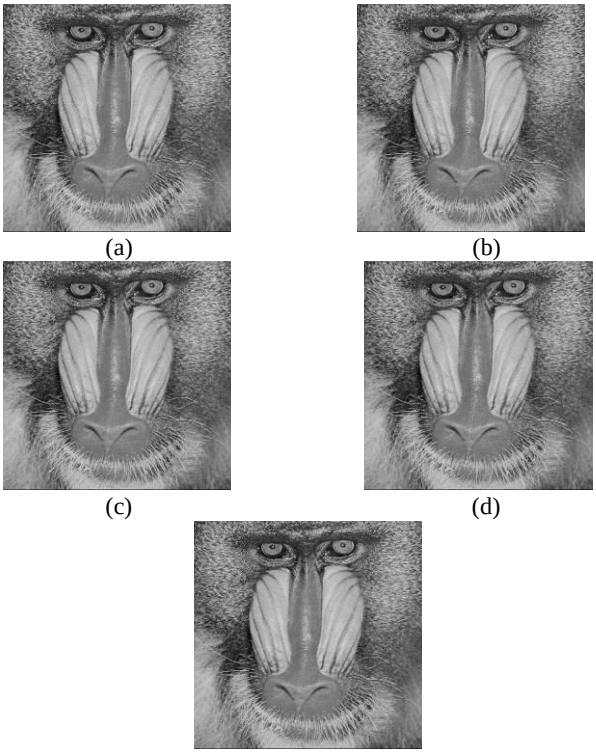
Algorithm	SNR	PSNR	MSE
AES	66.4513	72.1878	0.0039
DES	66.5623	72.2989	0.0038
3DES	66.5623	72.2989	0.0038
Blowfish	66.4555	72.1920	0.0039
RSA	66.4724	72.2090	0.0039

Table IV. The SNR, PSNR and MSE values of AES, RSA, DES, 3DES, and Blowfish and Baboon as cover image

Algorithm	SNR	PSNR	MSE
AES	66.8265	72.2644	0.0039
DES	66.7753	72.2132	0.0039
3DES	66.8870	72.3249	0.0038
Blowfish	67.0465	72.4845	0.0037
RSA	66.7838	72.2217	0.0039

The best results are obtained by high PSNR and less MSE. Table IV depicted The SNR, PSNR and MSE values of AES, RSA, DES, 3DES, and Blowfish algorithms and Baboon image as the cover image.

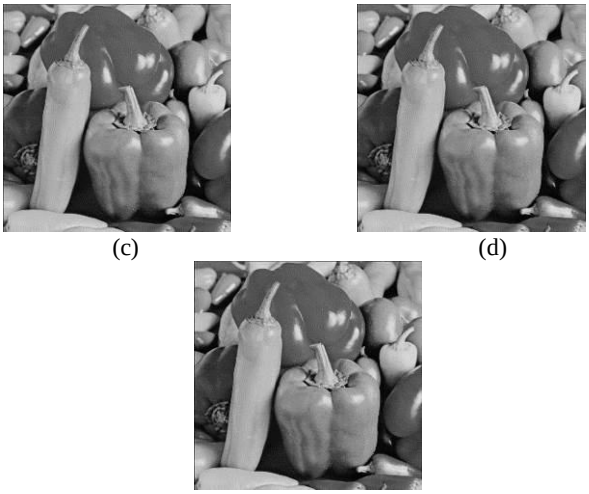
The results using of AES, RSA, DES, 3DES, and Blowfish algorithms as cryptographic algorithms and LSB as steganography algorithm using Peppers and Baboon images as cover images illustrates perfect values. The Stego images of using Peppers and Baboon are shown in Fig. 2 and Fig. 3 respectively.



(a) (b) (c) (d) (e)

Fig. 2 Stego images of employing (a) AES (b) DES(c) 3DES (d) Blowfish (e) RSA, and Peppers as cover image

(a) (b)



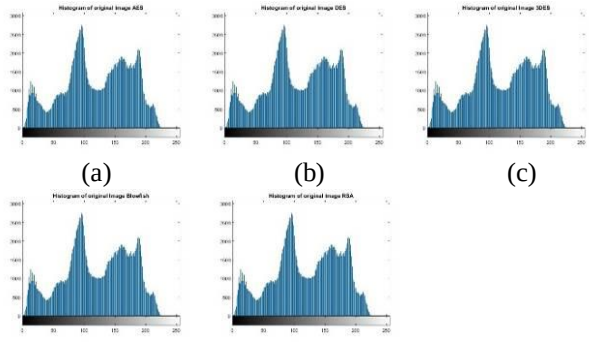
(c) (d) (e)

Fig. 3 Stego images of employing (a) AES (b) DES(c) 3DES (d) Blowfish (e) RSA, and Baboon as cover image

Fig. 1 shows the input cover images of size 512 × 512 whereas Fig. 2 and Fig. 3 illustrates the resulting stego images employing AES, RSA, DES, 3DES, and Blowfish algorithms.

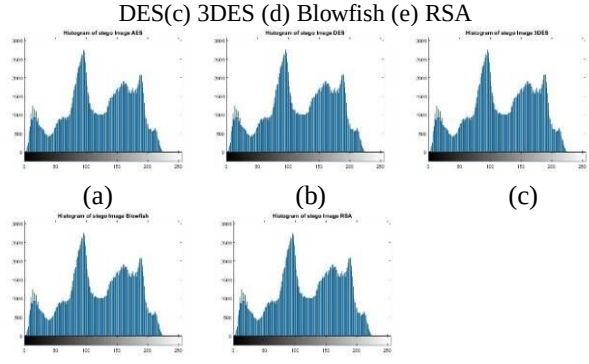
Histogram analysis between the cover image and stego image are illustrated to measure robustness against common statistical attacks [34]. The histogram of stego images and the histogram of cover image are compared in Fig. 4 and Fig. 5.

The analysis results represent that there is no significant difference in histograms of the cover and stego images.



(a) (b) (c) (d) (e)

Fig. 4 Histogram of Peppers cover image employing (a) AES (b) DES(c) 3DES (d) Blowfish (e) RSA



(a) (b) (c) (d) (e)

Fig. 5 Histogram of Peppers stego image employing (a) AES (b) DES(c) 3DES (d) Blowfish (e) RSA

IV. CONCLUSION

In this paper, cryptography and steganography are combined to achieve higher security. The cryptographic algorithms are AES, RSA, DES, 3DES and Blowfish algorithms and the steganography technique is LSB. First, the data is encrypted via the mentioned algorithms. Then the secret message is embedded into the LSB algorithm to be hidden in a cover image. The experimental outcome of the method is performed on MATLAB. The execution time of RSA is more than the other algorithms due to it is a public key algorithm. Two error metrics are employed to compare the quality of cover image and the stego image. The high PSNR and low MSE represent the satisfaction of employing these algorithms for the first step of the method. The encrypted message is also not easily detected by the difference histogram analysis while employing cryptographic algorithms for the first step of steganography.

REFERENCES

1. S. Panwar, S. Damani, and M. Kumar, "Digital image steganography using modified lsb and aes cryptography", *International Journal of Recent Engineering Research and Development (IJRERD)*, ISSN: 2455-8761, vol. 3(6), June 2018, pp. 18-27
2. M. Damrudi, Masumeh, and N. Ithnin, "Parallel RSA encryption based on tree architecture." *Journal of the Chinese Institute of Engineers*, vol. 36, no. 5, 2013, pp. 658-666.
3. M. Damrudi, Masumeh, and N. Ithnin, "State of the art practical parallel cryptographic approaches", *Australian Journal of Basic and Applied Sciences*, 2011, pp. 660-677.
4. A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A comparative study of recent steganography techniques for multiple image formats", *International Journal of Computer Network and Information Security*, vol. 11, no. 1, 2019, p. 11.
5. M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, IEEE, 2014, pp. 1-6.
6. A. Saha, S. Halder, and S. Kollya, "Image steganography using 24-bit bitmap images", *14th International Conference on Computer and Information Technology (ICCIT 2011*), IEEE, 2011, pp. 56-60.
7. S. M. Karim, Masud, M. S. Rahman, and M. I. Hossain, "A new approach for LSB based image steganography using secret key", *14th international conference on computer and information technology (ICCIT 2011)*, 2011, IEEE, pp. 286-291.
8. P. Wayner, "Disappearing cryptography: information hiding: steganography and watermarking", Morgan Kaufmann, ELSEVIER, 3rd Edition, 2009.
9. U. M. E.Ali, M. Sohrawordi, and M. P. Uddin, "A Robust and secured image steganography using LSB and random bit substitution", *American Journal of Engineering Research (AJER)*, E-ISSN: 2320-0847 p-ISSN: 2320-0936, vol. 8(2), 2019, pp. 39-44.
10. M. Damrudi, K. J. Aval, and N. Ithnin, "A Parallel method for RSA cryptosystem utilizing topological architecture", *Indian Journal of Science and Technology*, vol. 8(30), 2015.
11. N. Banjan, and P. Dalvi, "Medical Data Security using combination of Cryptography and Steganography with AES-LSB algorithm", *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, vol. 7(7), 2018.
12. S. Nagpal, and R. Nagpal, "Collaboration of cryptography and steganography for enhanced security: a review", *International Journal of Innovative Knowledge Concepts*, vol. 6, no. 8, 2018, pp. 124-128.
13. A. Moumen, and H. Sissaoui, "Images encryption method using steganographic LSB method, AES and RSA algorithm", *Nonlinear Engineering*, vol. 6, no. 1, 2017, pp. 53-59.
14. E. Deshmukh1, J. Dangle, S. Ghadi, S. Kewat, and K. Shewale, " Image steganography-hiding data within image", *International Journal of Computer Sciences and Engineering*, vol. 5, Special Issue 1, 2016.
15. A. Pandey, and J. Chopra, "Steganography using AES and LSB techniques", *International Journal of Scientific Research Engineering & Technology (IJSRET)*, vol. 6, no. 6, 2017, pp. 620-623.
16. M. E. Saleh, A. A. Aly, and F. A. Omara. "Data security using cryptography and steganography techniques" *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, 2016, pp. 390-397.
17. F. R Patel, and A. N. Cheeran, "Performance evaluation of steganography and AES encryption based on different formats of the image", *Performance Evaluation*, vol. 4, no. 5, 2015.
18. A. Pandey, and P. Bonde, "Performance evaluation of various cryptography algorithms along with LSB substitution technique", *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 6, 2013, pp. 866-871.
19. Y. Go swami, A. Bhargava, and P. Badal, "improved method for a secure image cryptography based on RSA and des algorithm and LSB steganography technique", *International Journal of Advance Engineering and Research Development Volume*, vol. 4(11), 2017.
20. N. Manwade, , and S. Nigam, "LSB image steganography with DES cryptography", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 7, 2015, pp. 761-764.
21. S. Singh, and A. Singh, "An Information security technique using DES-RSA hybrid and LSB", *International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*, vol. 8, 2014, pp.187-192.
22. A. O. Babatunde, A. J. Taiwo, and E. G. Dada, "Information security in health care centre using cryptography and steganography", arXiv preprint arXiv:1803.05593, 2018.
23. M. Zodape, and P. Shukla, "Analysis of Triple DES and RSA algorithm in securing image steganography", *International Journal of Computer Architecture and Mobility*, ISSN: 2319-9229, vol.1(8), June 2013.
24. C. D. Naidu, S. Koppu, V. M. Viswanatham, and S. L. Aarthy, "Cryptography based medical image security with LSB Blowfish algorithms", *ARPN Journal of Engineering and Applied Sciences*, vol. 9, no. 8, 2014.
25. M. H. Sharma, M. MithleshArya, and M. D. Goyal, "Secure image hiding algorithm using cryptography and steganography", *IOSR Journal of Computer Engineering (IOSR-JCE)*, e-ISSN: 2278-0661, 2013.
26. K. Patel, S. Utareja, and H. Gupta, "Information hiding using least significant bit steganography and blowfish algorithm", *International Journal of Computer Applications*, vol. 63, no. 13, 2013.
27. R. Apau, and C. Adomako, "Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones", *International Journal of Computer Applications*, vol. 164, no. 1, 2017, pp. 0975-8887.
28. R. Halder, S. Sengupta, S. Ghosh, and D. Kundu, "A secure image steganography based on RSA algorithm and hash-LSB technique", *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 18, no. 1.
29. J. K. Alhassan, I. Ismaila, V. O. Waziri, and A. Abdulkadir, "A secure method to hide confidential data using cryptography and steganography", *International Conference on Information and Communication Technology and Its Applications*, 2016.
30. A. Sawant, V. Darji, and A. Shetty, "Data hiding in encrypted images", *International Journal of Computer Science and Information Technologies*, vol. 6(2), 2015.
31. M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish for guessing attacks prevention", *Journal Computer Science Applications and Information Technology*, vol. 3, 2018, pp. 1-7.
32. The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 6 July 2019).
33. G. Swain, "Steganography in digital images using maximum difference of neighboring pixel values", International Journal of Security and Its Applications, vol. 7(6), 2013, pp. 285-294.

AUTHORS PROFILE

Masumeh Damrudi has received her B.Sc and M.Sc in Computer Science (software engineering) from Islamic Azad University, Tehran South branch, Tehran, Iran in 2001 and 2004 respectively. She has received her PhD from Universiti Teknologi Malaysia (UTM), JB, Malaysia in 2013. She is a lecturer in the Islamic Azad University, Firoozkooh branch since 2006. She has more than 30 papers in various journals and conferences. Her research interests are parallel processing, cryptography, and image processing. steganography

Kamal Jadidy Aval has received his B.Sc and M.Sc in Computer Science (software engineering) from Iran University of Science and Technology and Islamic Azad University, Tehran South branch, Tehran, Iran in 2002 and 2004 respectively. He has received his PhD from Universiti Teknologi Malaysia (UTM), JB, Malaysia in 2014. He is a lecturer in the Islamic Azad University, Firoozkooh branch since 2006. He has more than 30 papers in various journals and conferences. His research interests are Image Processing, Evolutionary Algorithms, WSNs, and MANets.