opción

Revista de Antropología, Ciencias de la Comunicación y de la Información, Filosofía, Lingüística y Semiótica, Problemas del Desarrollo, la Ciencia y la Tecnología

Año 35, 2019, Especial N° 20

Revista de Ciencias Humanas y Sociales
ISSN 1012-1587/ ISSNe: 2477-9385
Depósito Legal pp 198402ZU45

Universidad del Zulia
Facultad Experimental de Ciencias
Departamento de Ciencias Humanas
Maracaibo - Venezuela

Opcion, Año 35, Especial Nº 20 (2019):*2899-2921*
ISSN 1012-1587/ISSNe: 2477-9385

A Modified RSA Algorithm for Hiding Text in Colored Images with Random Pixel Selection

Sinan A. Naji[1], Hatem N. Mohaisen[2], Qusay S. Alsaffar[2], Salman H. Omran[3]

[1] Department of Postgraduate Studies, University of Information Technology and Communications, Baghdad, Iraq; dr.sinannaji@uoitc.edu.iq
[2] Ministry of Higher Education and Scientific Research, Minister's Office, Baghdad, Iraq.
[3] Ministry of Higher Education and Scientific Research, Private Higher Education Directorate, Baghdad, Iraq.

Abstract

This study introduces a combination of two techniques: a modified RSA cryptography and image-based steganography to improve the overall system's security level. The system comprises three main steps: message encryption, random traversing path generation, and image-based steganography. We propose to use the addition of factor F along with standard RSA to the make the cryptanalysis task more difficult. Furthermore, LSB image-based steganography technique is used for hiding the message. However, hiding data on a systematic basis subjects the algorithm to many steganalysis techniques. As a result, the attacker is capable of detecting the inclusion of a secret message within the image. As such, it is important to have an additional level of security to enhance the protection of the data. This study proposes to use of random pixel selection. For brute-force attack, the attacker not only needs to find the pixels holding the secret bits, but also must determine the appropriate combination of bits in order to reconstruct the hidden data. Compared to standard RSA and LSB techniques, the proposed system achieves a significant security improvement with high image quality.

Keywords: RSA, LSB, Steganography, Cryptography, Random Pixel Selection.

Algoritmo RSA modificado para ocultar texto en imágenes en color con selección aleatoria de píxeles

Resumen
Este estudio presenta una combinación de dos técnicas: una criptografía RSA modificada y una esteganografía basada en imágenes para mejorar el nivel de seguridad general del sistema. El sistema consta de tres pasos principales: cifrado de mensajes, generación de rutas de recorrido aleatorio y esteganografía basada en imágenes. Proponemos utilizar la adición del factor F junto con el RSA estándar para dificultar la tarea de criptoanálisis. Además, la técnica de esteganografía basada en imágenes LSB se utiliza para ocultar el mensaje. Sin embargo, ocultar datos de forma sistemática somete el algoritmo a muchas técnicas de esteganálisis. Como resultado, el atacante es capaz de detectar la inclusión de un mensaje secreto dentro de la imagen. Como tal, es importante tener un nivel adicional de seguridad para mejorar la protección de los datos. Este estudio propone el uso de la selección aleatoria de píxeles. Para el ataque de fuerza bruta, el atacante no solo necesita encontrar los píxeles que contienen los bits secretos, sino que también debe determinar la combinación adecuada de bits para reconstruir los datos ocultos. En comparación con las técnicas estándar RSA y LSB, el sistema propuesto logra una mejora significativa de seguridad con alta calidad de imagen.

Palabras Clave: RSA, LSB, esteganografía, criptografía, selección aleatoria de píxeles.

Introduction

Colored images play a crucial role of our lives so that the society becomes visually oriented [1]. Therefore, it is not surprising that image-based steganography techniques play an important role in hiding information without arousing the suspicion of the third party. In general, the term steganography can be defined as the discipline that includes techniques for hiding information in a cover media so that the viewer cannot identify the existence of the hidden information [2] [3]. With image-based steganography, some image bits are replaced with bits of the secret message that needs to be hidden [4] . However, the main aim of cryptography is to store and transmit data in a certain format so that only authorized persons can access and process them. To do this, plain text or other types of data are converted into an encoded version. Governments, companies, and individuals typically apply encryption to protect their data and files stored on computers, servers, cloud computing, and mobile devices such as phones or tablets. Although encryption is widely used for protecting data, cipher text could attract the immediate attention of a third party [5]. To strengthen the security level of exchanging secret information, both steganography and cryptography are used alongside by encrypting the data before carrying out steganography [6] [7]. This combination provides double level of information security. In practice, many challenges are associated with these methods that should be carefully considered when designing a secure system. These include [5] [8]: They are undetectable, robust against attacks, embedding capacity, and computational complexity.

Many cryptography techniques are in use today. They may include: DES, RSA, Diffie-Hellman, DSA, ElGamal, ECC, MD5, IDEA, etc. [4] [9]. The RSA technique is one of the most widely-used public key encryption techniques [10] [11]. Currently, RSA seems to be very secure [4] [12]. However, since the main steps of the RSA technique are publically known, many different attacks are possible against this technique to identify a ciphered message and try to retrieve the original message [4] [13].

This study proposes using the addition of factor F along with RSA to the make the cryptanalysis task more difficult. Furthermore, LSB image-based steganography technique is used for hiding the message. To enhance the security level of the standard LSB algorithm, our proposal is to generate a random sequence of points. Applying randomization to hide message bits instead of storing them in a systematic way makes the system more secure. The attacker not only needs to predict which pixels that hide the data, but also must rearrange them in the correct sequence. The suggested system achieves a significant security improvement with high image quality.

The rest of this paper comprises eight sections: Section 2 presents some relevant works. Section 3 introduces the standard RSA technique. Section 4 discusses the modified RSA technique. Section 5 describes Linear Congruential Random Number Generator. Section 6 describes embedding message bits into cover image. Section 7 presents the fidelity measures. Section 8 provides the experimental results of the proposed technique. Lastly, Section 9 presents the conclusions.

Related Works

Uppal et al. developed a system of double layers that combines an enhanced RC6 algorithm for encryption and LSB technique for image steganography [14]. The enhanced RC6 cryptography uses 8 × 32-bit registers. Along with these registers, the inclusion of integer multiplication in this algorithm increases the diffusion per round. The authors show that their system provides a highly secured communication.

In [15], Saraireh proposed the filter bank cipher technique for encryption, where this technique offers high speed and enhanced security level. Message embedding is achieved using the Discrete Wavelet Transform (DWT)-based steganography.

Saleh et al. offered a system that comprising two stages. In the first stage, the secret message is encrypted using a modified version of the AES algorithm that is named AES_MPK algorithm [16]. In the second stage, the PVD-MPK and MSLDIP-MPK techniques are combined and used to hide the encrypted message in gray-scale images

Pujari and Shinde proposed to apply Blowfish encryption algorithm to convert a plain text file into a cipher text file [17]. Then, the produced ciphered text is embedded into a cover image using LSB-based steganography. The Blowfish algorithm is a symmetric block cipher that uses a variable key length.

Kumar and Sharma presented a modified LSB technique, i.e., Hash-LSB alongside the RSA algorithm to provide greater security [18]. The Hash-LSB is based on a hash function to create a pattern for hiding message bits in the cover image. Then, each 8-bits of the message will be embedded in sequence of (3, 3, 2) bits into Red, Green and Blue channels of each pixel within the cover image.

Similar work was presented by Satar et. el. [19]. They proposed using Diffie-Hellman algorithm to generate the traversing path of pixels to be used for hiding message bits.

Dhamija and Dhaka described a secure scheme for exchanging information within cloud servers [20]. The proposed scheme uses one's complement method, that they named SCMACS. It is based on symmetric key principles where both sender and receiver share the same key to encrypt and decrypt data. In the steganography step, they use the standard LSB algorithm.

Pillai et al. presented a method of clusters where the cover image is divided into several segments and then hides the message bits in these segments [21].   Among the numerous methods that have been proposed in the literature, the authors used the K-means clustering technique to produce the clustering results.

In [22], the authors proposed using MP3 files for hiding data. The secret data are encrypted using Advance Encryption Standard (AES) algorithm along with Message Digest (MD5) hash function for key generation and processing. Then, the encrypted data are embedded in the homogeneous frames of the MP3 audio files.

Patel and Meena [23] presented a similar system that uses dynamic key cryptography. The dynamicity of key is based on rotating the key where each rotation step generates a new key. In this scheme, Pseudo Random Number Generator (PRNG) is used for pixel selection.

More related works can be found in [8] [9] [24] [25] [26] and [27] .

Standard RSA Technique

The RSA technique was proposed by three researchers from MIT, Ron Rivest, Adi Shamir and Leonard Adleman in 1977 [4]. It is based on the property of modular exponentiation and presents the structure of public key cryptosystem. The RSA is an asymmetric technique. The advantage of this technique is that it offers high security level when the key is sufficiently large. The same algorithm can be used for encryption and decryption. Nowadays, the RSA method has become one of the most widely-used public key encryption techniques and plays a crucial role in a wide range of information security applications.

Using the RSA technique involves three steps: key generation, encryption, and decryption [4] [13].

3.1 Key Generation

In standard RSA, the sender creates his public and private keys with the following procedure [4]:

1) Choose two prime numbers p and q.
2) Calculate the modulus $n = p \times q$.
3) Calculate $m = (p-1) \times (q-1)$.
4) Choose the public encryption key e, where $1 < e < m$ and $\gcd(m,e) = 1$
5) Determine the private key d. Utilize Euclidean algorithm to get $d \times e$
mod m=1 where d is the multiplicative inverse of e.
6) The public key consists of (e,n)
7) The private key consists of (d,n)

3.2 Encryption

Now, for encrypting a secret plain text message M, the message is converted into an integer number using any padding scheme. Then, the cipher text C is generated using the public key (e,n) as follows:

$$C = M^e mod\, n \qquad (1)$$

3.3 Decryption

The decryption in RSA is also an exponential operation. So, the original plain text M is retrieved using the private key (d,n) as follows:

$$M = C^d\, mod\, n \qquad (2)$$

Modified RSA for cryptography

Although RSA technique offers high security level, many different attacks are possible against this technique. These may include brute-force, guessing, timing attack, and mathematical attack [4] [13]. To provide a strong algorithm and make the task of the cryptanalysis more difficult, one should keep the value of p and q more secure. If the attackers succeed in guessing the values of p and q, the value m and n can be easily computed. If this is achieved, all messages encrypted with the public key can be decrypted.

The main idea of the new approach is that instead of using two prime numbers p and q, we propose using additional factor F that will be used in equation No. (1) using the public key (e,n) as follows:

$$C = (M^e mod\, n\,) \times F \qquad (3)$$

where F is a randomly chosen positive integer. The sender and receiver should agree in advance to use F prior to communication. The multiplication of C by F will make cryptanalysis more confusion because guessing the value of three numbers is much harder than guessing the value of two. Therefore, the factor F is considered as an additional key that makes the search space relatively high and accordingly improves the general security level of the system.

At the receiver end, retrieving the original message of the decrypting equation No. (2) will require the use of the private key (d,n) as follows:

$$M = \left(\frac{C}{F}\right)^d\, mod\, n \qquad (4)$$

Linear Congruential Random Number Generator (LCRNG)

Hiding data on a systematic basis such as sequential pixels, zigzag path, edge points, etc. leaves the system open to many steganalysis techniques. Consequently, the attacker can detect the inclusion of a secret message within the image. Thus, it is important to have an additional level of security to protect the data.

In this work, the Linear Congruential Random Number Generator (LCRNG) is used to generate a random set of pixels (i.e., traversing path). LCRNG was first proposed by Lehmer [28] to generate a sequence of random integers x_0 , x_1 , ….. in range [0, n-1]. Nowadays, the LCRNG is considered one of the most widely-used techniques for the generation of random numbers. The initial value x_0 is called Seed number. Each successive random number $x_{(i+1)}$ is generated as follows [16]:

$$x_{i+1} = a * x_i + b \ mod\ n \qquad (5)$$

where a is constant multiplier, b is the increment, and n is modulus.

Now, the attacker not only needs to find the pixels that hold the secret bits, but also must determine the correct combination of these bits in reconstructing the hidden data.

Selecting the values for a, b, n, and x_0 significantly affects the statistical properties of the traversing path. Changing any of these values leads to complete change in the generated list of points.

Least Significant Bit (LSB)

The purpose of this stage is to embed a ciphered text in an innocent-looking cover image. In computing, digital images are arrays of numbers created from the physical scene picture. These numbers represent the intensity values of the image pixels [1]. For gray-scale image, the most common system used is 8 bits per pixel. Thus, for each pixel there are 256 intensity values. For true-color image such as RGB images, the most common system used is 24 bits per pixel. This implies that each pixel offers $256 \times 256 \times 256 \approx$ 16.7 million colors [29]. A slight alteration in pixel intensity will produce indistinguishable change in pixel appearance and it remains difficult for the Human Vision System (HVS) to detect the slight changes [27]. From our point of view, Least Significant Bit (LSB) algorithm is among the most significant algorithms. It is based on a substitution procedure to replace the least significant bit (i.e., 8th bit) of original pixel's intensity with the secret message-bit directly [12] [10]. This means that the secret message is converted into a bit stream and sequentially overwrites the least significant bit of the image's pixels [3]. The main characteristics of LSB can be summarized as follows: easy to understand, fast processing, and less distortion. In this work, the LSB algorithm is utilized for hiding the cipher text. The general step-by-step algorithm at the sender's end is listed as follows:

Input: Message M, Cover-image of size N×M, Public-key, Seed number S, factor F.
Output: Stego-image.

A. Apply eq. No. (3) to encrypt the Message M using public key (e,n) and the factor F.
B. Compute the size Z of the ciphered text message.
C. Convert the three-dimensional cover-image (i.e., RGB-image) into one-dimension array I with index of each pixel (N×M×3, 1).
D. Generate a traversing path of random points that will hold the message bits using LCRNG techniques as described in Section 5.
E. Convert ciphered text bytes into binary stream bits.
F. Hide the binary stream bits of the ciphered text in I using LSB algorithm at random points generated by Step D.
G. Reconstruct the image by converting the one-dimension array I into three-dimensional colored image (i.e., Stego-image).
H. Output Stego-image

At the receiver end, the receiver will use the stego-image and the above-mentioned parameters to retrieve the original message.
Fidelity Measures
Fidelity measures refer to the type of measures utilized to compute the difference level between the original cover-image and the resulting stego-image after embedding the secret message. The most used fidelity measures are: Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM):

7.1 Mean Square Error (MSE)
The mean square error represents the cumulative squared error (i.e., pixel differences) between the two images. The MSE is calculated as follows [7] [25]:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - S(i,j)]^2 \qquad (6)$$

where m and n are the image dimensions and C(i,j) and S(i,j) are the cover and stego-image pixels respectively.

7.2 Peak Signal to Noise Ratio (PSNR)

The PSNR is a measure of the peak error. A higher PSNR means better quality image [6] [30]:

$$PSNR = 10\ log_{10} \frac{R^2}{MSE} \qquad (7)$$

where R is the maximum possible value of the pixels' intensities.

7.3 Structural Similarity Index Measure (SSIM)

Inclusion of a recent measure such as Structural Similarity Index Metric (SSIM) can provide a fair comparison along with MSE and PSNR. The SSIM is regarded as one of the most powerful methods of assessing the visual closeness of images, which can be calculated as follows [31]:

$$\text{SSIM(x,y)}=\frac{(2\,\mu_x\,\mu_y + C_1)\,(2\,\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1\,)(\sigma_x^2 + \sigma_y^2 + C_2\,)} \qquad (8)$$

where µ is the mean intensity, σ is the standard deviation, C_1 and C_2 are constants > 0 that are included to avoid instability when µ_muyghbv cvx
$\mu_x\,, \mu_y\,, \sigma_{xy}\,,\ \mu_x^2,\ \mu_y^2, \sigma_x^2, \sigma_y^2$ are very close to zero.

8. Experimental Results

The experimental results provided in this section define the performance of the proposed technique. Our system was carried out on Intel (R) Core i7 processor with 8-GB RAM on Windows platform. We used MATLAB R2017b package for the implementation of the modified RSA and standard LSB algorithm. The results showed that the proposed system achieved a significant security improvement with high image quality.

For qualitative evaluation, Figure 1 shows examples of applying the proposed technique. The top row of this figure shows the original cover-image; while the second row shows the corresponding resulting stego-image. As shown in this figure, the original cover-image and the resulting stego-image are visually almost identical. In other words, the stego-image does not contain any detectable defects caused by hiding information.

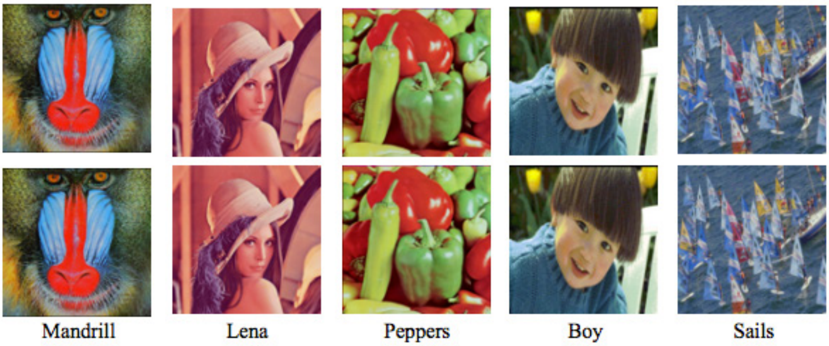

Figure 1: Sample of experimental results. The first row of this figure shows the original cover-image, while the second row shows the corresponding resulting stego-image.

For quantitative evaluation, the lower the value of MSE, the lower the error. The higher PSNR value and SSIM close to 1, i mplies less defects and better visual quality of image. Table 1 shows the calculated PSNR, MSE and SSIM using different lengths of secret message in the five images that are shown in Figure 1. The length of the secret message includes: 52, 105, 158, and 211 characters.

Table 1: The PSNR, MSE and SSIM experimental results

No. of Char.	PSNR					Average PSNR	Average MSE	SSIM
	Mandrill	Lena	Peppers	Boy	Sails			
52	80.9279	82.0359	80.8549	83.3767	83.8446	82.2081	0.000406	1
105	77.9493	78.8527	78.0619	80.536	80.7225	79.2244	0.000802	1
158	76.0906	76.9004	76.1954	78.0599	79.0121	77.2516	0.001230	0.999999
211	74.7906	75.8067	74.7448	77.3285	77.7273	76.0795	0.001668	0.999998

Figure 2 shows the histograms of the three color channels (i.e., Red, Green, and Blue) for the cover- image and its corresponding stego-image. The top row shows the original cover-image; while the second row shows the resulting stego-image. The three histograms of the stego-image are highly similar to their respective original histograms.

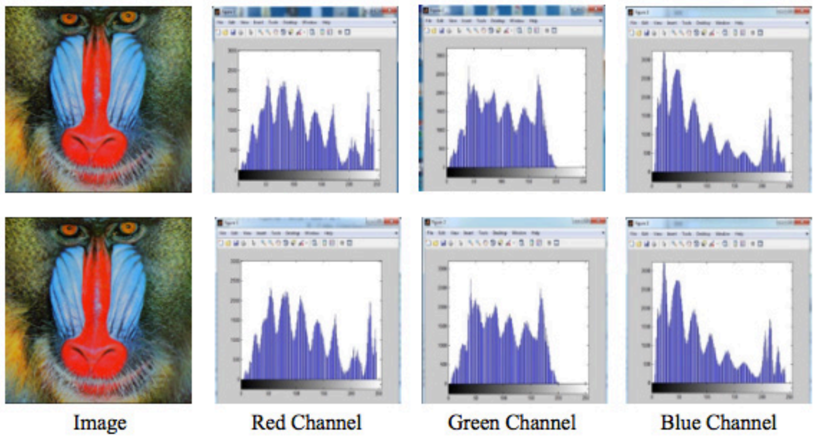

Figure 2: Histograms of the color channels (i.e., Red, Green, and Blue) for the cover-image and its corresponding stego-image. The top row shows the original cover image; while the second row shows the resulting stego-image.

Conclusion

Information security (IS) is an essential issue in the storage and exchange of information between different parties. The main goal of any IS system is to protect the information from various attacks. The IS has attracted much attention and has been studied for decades by mathematicians, information technology specialists, and engineers. Many research demonstrations and commercial applications have been developed from these efforts. It is a challenging field as technology changes literally on a daily basis. A first step of any IS system is to encrypt the information. However, encrypting the plain text could attract the immediate attention of a third party.

This study aims to develop a system that provides an enhanced level of security. The system involves three main steps: message encryption, random traversing path generation, and image-based steganography. We have proposed a modified RSA algorithm to make the cryptanalysis task more difficult. LSB image-based steganography technique is used for hiding the message with a random selection of pixels that hold a secret message. Applying randomization to hide message bits rather than storing them in a systematic basis makes the system more secure. Furthermore, even though that the attacker can locate the pixels that hide data; the retrieved data bits cannot be processed because they are already ciphered. The inclusion of additional factor F along with RSA algorithm makes the search space relatively high. In general, retrieving the original data without knowing the architecture of the proposed technique is really difficult. Compared to standard RSA and LSB techniques, the proposed system achieves a significant security improvement with high image quality.

References

[1] N. Efford, Digital image processing: a practical introduction using java (with CD-ROM): Addison-Wesley Longman Publishing Co., Inc., 2000.

[2] K. Joshi, K. Puniani, and R. Yadav, "A Review on Different Image Steganography Techniques," Digital Image Processing, vol. 8, no. 6, pp. 179-186, 2016.

[3] M. Mishra, G. Tiwari, and A. K. Yadav, "Secret communication using public key steganography," in International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), 2014, pp. 1-5.

[4] V. Pachghare, Cryptography and information security: PHI Learning Pvt. Ltd., 2015.

[5] H. L. Hussein, A. A. Abbass, S. A. Naji, S. Al-augby, and J. H. Lafta, "Hiding text in gray image using mapping technique," in Journal of Physics: Conference Series, 2018, pp. 012032.

[6] A. Y. Tuama, M. A. Mohamed, A. Muhammed, and M. H. Zurina, "Randomized Pixel Selection for Enhancing LSB Algorithm Security against Brute-Force Attack," Journal of Mathematics and Statistics vol. 13, no. (2), pp. 127-138, 2017.

[7] A. Tiwari, S. R. Yadav, and N. Mittal, "A review on different image steganography techniques," International Journal of Engineering and Innovative Technology (IJEIT) Volume, vol. 3, pp. 19-23, 2014.

[8] A. Baby, and H. Krishnan, "Combined Strength of Steganography and Cryptography-A Literature Survey," International Journal

of Advanced Research in Computer Science, vol. 8, no. 3, 2017.

[9] S. Almuhammadi, and A. Al-Shaaby, "A survey on recent approaches combining cryptography and steganography," Computer Science Information Technology (CS IT), 2017.

[10] G. Swain, and S. K. Lenka, "A novel steganography technique by mapping words with LSB array," International Journal of Signal and Imaging Systems Engineering, vol. 8, no. 1-2, pp. 115-122, 2015.

[11] A. K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm," IJISET-International Journal of Innovative Science, Engineering & Technology, vol. 2, no. 1, pp. 858-862, 2015.

[12] A. Senarathne, and K. De Zoysa, "ILSB: Indexing with Least Significant Bit Algorithm for Effective Data Hiding," International Journal of Computer Applications vol. 161, no. 5, 2014.

[13] A. H. Al-Hamami, and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," in Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on, 2012, pp. 402-408.

[14] R. S. Ankit Uppal, Renuka ngapal, Aakash gupta, "Merging Cryptography and Steganography Combination of Cryptography: RC6 Enhanced Ciphering and Steganography: jpeg," International Journal of Advanced Computational Engineering and Networking, vol. 2, no. 10, Oct. 2014.

[15] S. Saraireh, "A Secure Data Communication system using cryptography and steganography," International Journal of Computer Networks & Communications, vol. 5, no. 3, pp. 125, 2013.

[16] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, pp. 390-397, 2016.

[17] A. A. Pujari;, and S. S. Shinde, "Data Security using Cryptography and Steganography," IOSR Journal of Computer Engineering, vol. 18, no. 4, 2016.

[18] A. Kumar, and R. Sharma, "A secure image steganography based on RSA algorithm and hash-LSB Technique," International Journal of Advanced Research in Computer Science and Software

Engineering, vol. 3, no. 7, 2013.

[19] S. D. M. Satar, N. A. Hamid, F. Ghazali, R. Muda, and M. Mamat, "A New Model for Hiding Text in an Image Using Logical Connective," International Journal of Multimedia and Ubiquitous Engineering, vol. 10, no. 6, pp. 195-202, 2015.

[20] A. Dhamija, and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 346-351.

[21] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering and encryption techniques," in 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, pp. 1206-1211.

[22] R. Indrayani, H. A. Nugroho, R. Hidayat, and I. Pratama, "Increasing the security of mp3 steganography using AES Encryption and MD5 hash function," in 2016 2nd International Conference on Science and Technology-Computer (ICST), 2016, pp. 129-132.

[23] N. Patel, and S. Meena, "LSB based image steganography using dynamic key cryptography," in 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), 2016, pp. 1-5.

[24] S. Jindal, and N. Kaur, "Digital image steganography survey and analysis of current methods," International Journal of Computer Science and Information Technology & Security, vol. 6, pp. 10-13, 2016.

[25] K. U. Singh, "A Survey on Image Steganography Techniques," International Journal of Computer Applications, vol. 97, no. 18, 2014.

[26] B. Li;, J. He;, J. Huang;, and Y. Q. Shi;, "A Survey on Image Steganography and Steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, 2011.

[27] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal processing, vol. 90, no. 3, pp. 727-752, 2010.

[28] D. Lehmer, "Proceedings of the Second Symposium on Large-Scale Digital Computing Machinery," Harvard University

Press, Cambridge, Mass, 1951.

[29] R. Zainuddin, S. Naji, and J. Al-Jaafar, “Suppressing False Negatives in Skin Segmentation,” in International Conference on Future Generation Information Technology, 2010, pp. 136-144.

[30] J. Rani, and T. A. Khan, “Performance Optimized DCT Domain Watermarking Technique with JPEG,” International Journal of innovative Technology and Exploring Engineering, vol. 4, no. 2, 2014.

[31] K. Rao, and H. Wu, “Structural similarity based image quality assessment,” Digital Video image quality and perceptual coding, pp. 261-278: CRC Press, 2005.

UNIVERSIDAD
DEL ZULIA

opción
Revista de Ciencias Humanas y Sociales

Año 35, N° 20, (2019)

Esta revista fue editada en formato digital por el personal de la Oficina de Publicaciones Científicas de la Facultad Experimental de Ciencias, Universidad del Zulia.
Maracaibo - Venezuela

www.luz.edu.ve

www.serbi.luz.edu.ve

produccioncientifica.luz.edu.ve