Hybrid cryptography and steganography method to embed encrypted text message within image

Hybrid cryptography and steganography method to embed encrypted text message within image

Khider Nassif Jassim[1]*, Ahmed Khudhur Nsaif[2], Asama Kuder Nseaf[3], Al Hamidy Hazidar[3], Bagus Priambodo[4], Emil Naf'an[5], Mardhiah Masril[5] Inge Handriani[4], And Zico Pratama Putra[6]

[1]Department of Statistics. Faculty of Management and Economics, Wasit University, Al-Kut, Iraq
[2]Department of Electrical, Electronic & Systems Engineering, Faculty of Engineering & Built Environment,Universiti Kebangsaan Malaysia, Malaysia
[3]Institute of Visual Informatics (IVI), Universiti Kebangsaan Malaysia, Malaysia
[4]Information System, Faculty of Computer Science, Universitas Mercu Buana Jl. Raya Meruya Selatan, Kembangan, Jakarta 11650
[5]Universitas Putra Indonesia YPTK, Padang, 25221, Indonesia
[6]School of Electronic Engineering and Computer Science, Queen Mary University of London

*khnsaif@uowasit.edu.iq[1]

Abstract. The businesses in various fields use the online communication application to gather their data and information with local and global sources. The gathered data may sensitive such as the financial and businesses development information. The hackers or online thief try to stole the valuable data i.e. credit card numbers. The organizations looking for secure online channels in order to transfer their data efficiently and avoid the data thieving. One of the most applicable methods that developed to secure the online transferred data is the cryptography which transfers the original data or information to encrypted formulation. Cryptography still has many drawbacks such as stole and decrypts the original texts using automatic decryption counter. The main aim of this research is to improve the cryptography securing level using supportive method which is Steganography. The Steganography is the processes of hide the data or information in media files such as video, images and audio files. There are four stages represent the methodology of this paper; (1) encrypt the original texts using RSA algorithm, (2) hide the encrypted texts in Image files, (3) extract the encrypted texts from Image files, and (4) decrypt the original texts using decryption key of RSA algorithm. It is expected to improve the security level of the online transferred textual data. The performance of the final results will be evaluated through compare the Image files quality before and after hide the data in these files. The quality of the original and stego Image files need to be same or near in order to maximize the difficulty of detect that there data hide in these files.

1. Introduction

This Nowadays, the internet and communication applications pro-vide many advantages such as transfer the data and information at real time and online conferences [11;21]. This wide increasing in the online applications in various fields such as financial, govern-mental and social fields maximize the importance of secure the channels that used to transfer the data through internet network [20; 17]. Therefore, these applications are necessary to improve the businesses of various fields. However, the data and information security is one from the most challenges that face the organizations that need to transfer sensitive or private data online. According to [13;22;23], the number of hackers or online data thief increased rapidly in the last years. The hackers focus on stole the sensitive data such as credit cards numbers and organizations secrets. Thus, the organizations always afraid from the security level of data transferring channels.

Cryptography is playing a major role in data protection in applications running in a network environment that used to secure the online transferred data [18; 2]. The cryptography allows people to do business electronically without worries of deceit and deception in addition to ensuring the integrity of the message and authenticity of the sender [12]. It has become more critical to our day-to day life because thousands of people interact electronically every day; through e mail, e-commerce, ATM machines, cellular phones, etc. This geometric increase of information transmitted electronically has made increased reliance on cryptography and authentication by users [9].

The main weakness of cryptography method is that the hackers can detect the encrypted messages and try to decrypt these messages through many ways such as automatic counters or random tests based on mathematic calculations [4]. Therefore, the cryptography method still has security drawbacks i.e. only depend on decryption keys. The main question is how to improve the cryptography security level of the online transferred texts? According to [7], cryptography method could be improved using supportive another security method such as Steganography method. The Steganography method is one form the most supportive methods that can improve the security level of cryptography method. Both of these methods can be integrated efficiently to provide high level of online data security [7]. The Steganography can be defined as the method of hide the data and information in media files such as images, audio files, or video files [1; 26]. The main aim of Steganography is to maximize the difficulty of detect the encrypted data that transferred online [1]. Therefore, the encrypted data can be hidden in media file before send this file through online application [24]. The receiver can ex-tract the encrypted data from the media file and decrypt the data using the secret keys. Thus, the hackers will face difficulty to discover encrypted data the transferred online. Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively [27]. Steganography is the art of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it can’t be understood; the Steganography hides the message so it can’t be seen. Even though both cryptography and steganography methods provide security, but combine cryptography and steganography in to one system for better security and confidentiality [25].

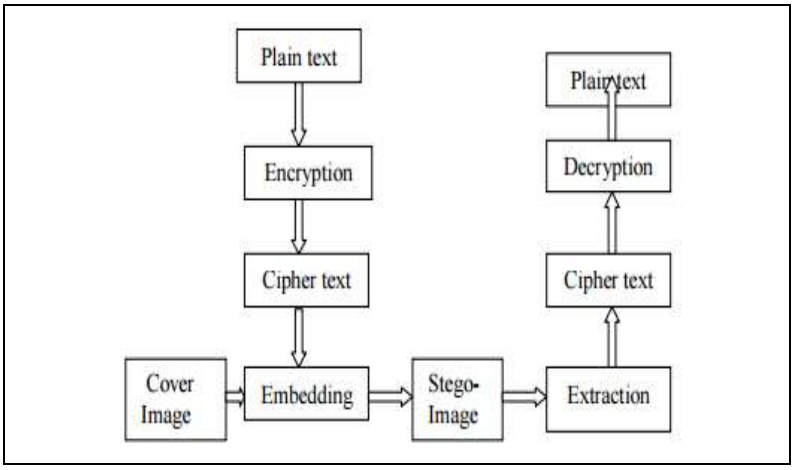

Figure 1. Combination of Cryptography and Steganography.

Therefore, the main objective of this research is to develop hybrid security system using cryptography and Steganography methods through hide the encrypted texts data in Image files that transferred online between two points.

2. Methodology

The main scope of this paper is securing the texts data using cryptography and Steganography methods. The data will be encrypted using RSA Algorithm. On the other hand, the encrypted data will be hided in Image files of (.bmp) extension. Figure 2 illustrates the research paper scope. While, Figure 3 illustrates the research paper model. There are four main stages of the methodology which are as the following (1) Encrypt the text data using RSA through and generate the encryption keys. (2) Hide the encrypted data using Image files. (3) Extract the encrypted data from the Image files. (4) Decrypt the text data using the decryption key.

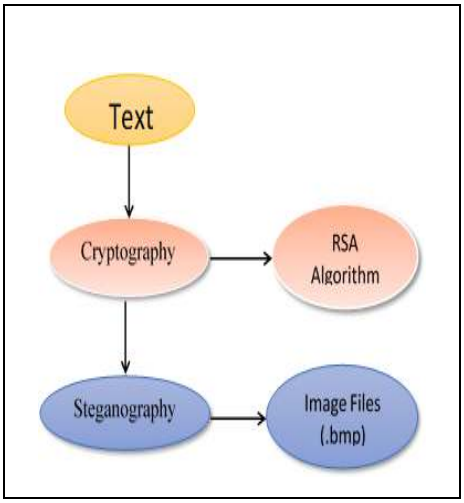

Figure 2. Research Scope.

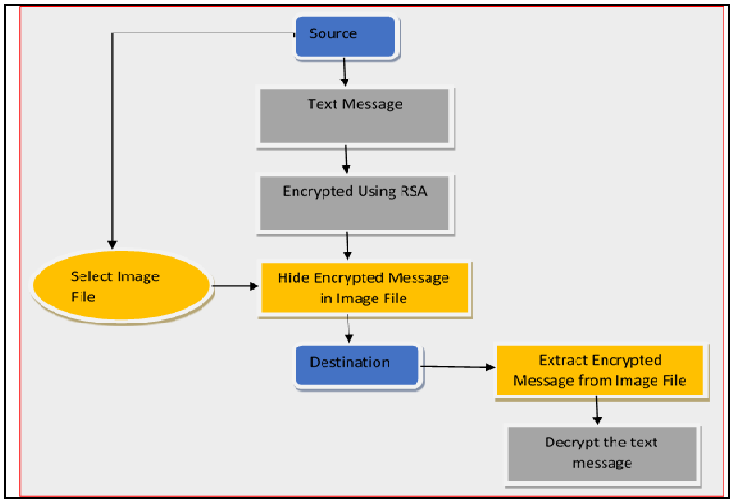

Figure 3. Research paper methodology.

2.1. Cryptography

According [16; 1], cryptography is the method of witting using secret styles or codes. The original text can have transferred to cipher-text using secret keys or codes. Thus the original texts structure and representation will be changed to ambiguous texts. The processes of transfer the original text to cipher-text called encryption. The decryption is the processes of transferring from cipher-text to original texts. Also, the decryption needs secret code or keys to extract the original texts.

2.1.1. RSA Algorithm.

[14] mentioned that, RSA is one from the most popular encryption algorithms. RSA considered as asymmetric cryptography method [14]. Thus, the encryption and decryption processes need independent keys based on RSA. The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward. To create an RSA public and private key pair, the following steps can be used:

- Choose two prime numbers, p and q. From these numbers we can calculate the modulus, n = p*q
- Select a third number, e, that is relatively prime to (i.e. it does not divide evenly into) the product (p −1) *(q −1), the number e is the public exponent.
- Calculate an integer d from the quotient $\frac{(ed-1)}{((p-1)(q-1)}$. The number d is the private exponent.
- The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.
- To encrypt a message, M, with the public key, creates the cipher text, C, using the equation: $C = M^e \text{ Mod } n$
- The receiver then decrypts the cipher-text with the private key using the equation: $M = C^d \text{ Mod } n$

2.2. *Steganography*

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It is the art of concealing a message in a cover without leaving a remarkable track on the original message [15; 3; 19]. Currently, Steganography is the processes of hide the digital data and information in media files such as video, audio, and images files [5]. The sender hide the data using media files and the receiver can extract this data using stego applications to import and export the data in/from the media files [6; 10] Image files lend themselves to exploitation particularly well, which we will explore throughout this project. Focus will primarily be on bitmap formatted images.

2.2.1. Least Significant Bit.

One A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit in other words, the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600-pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the LSB

of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hid-den. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [8].

3. Model Validation/Verification using software

Using hybrid encryption and steganography, provides the user a convenient way to transmit and exchange data from one place to another in a safe manner that prevent an attacker from accessing on the secret information. This software typically makes the task of encrypting/decrypting and data hiding smoothly and reliably, com-pared to the traditional ways. The software should ease the encryption and data hiding activities. It should be user friendly and highly secured. The software will respond to the user commands depending on the types of commands issued by the user. We believe that the developed software will be more reliable, more secured, more robust, attractive and easy for the users. The figure below describes the architecture of the software. This figure is divided into two parts. The first one Figure 4 defines the process from the sender side, which includes specifying the secret message to encrypt and hide within the cover file. The second part Figure 5 represents the recipient side where the recipient attempts to retract and decrypt the secret message.

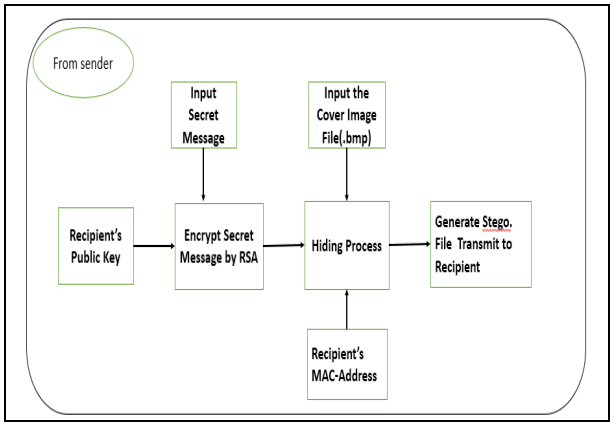

Figure 4. Architecture of the Software at a sender.

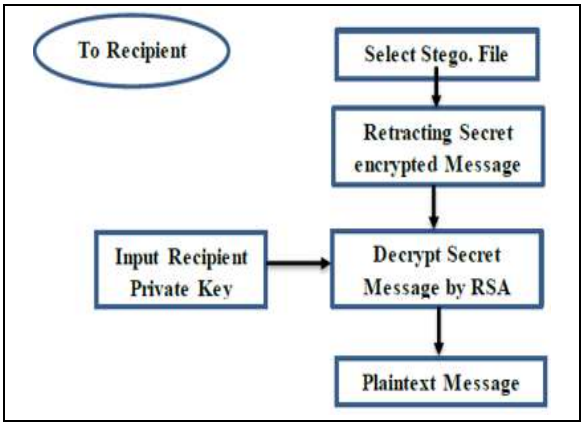

Figure 5. Architecture of the Software at a recipient.

4. Experimental Results

Brief results of the implementation of the various phases of the software: There are two keys that important in this process, namely: public e and private d keys. These created keys depend on the following variable p and q, where the values of these variables consist of prime numbers. The values of p and q have chosen randomly with no need to be entered by the user to be easy and more secure. Generally, through the value of *p* and *q*, the system will compute and show the value of *n*, where this value comes from (p × q) and represent the part of the public key. On the other hand, also calculates the value of phi (φ) through (p-1) × (q-1), where this value represents the number of integers less than *n* and relatively prime to (*n)*. For example, suppose the values of a recipient will be getting after he click on the button of generate keys as illustrated in Figure 6. Where we see the recipient got the values which are; *public key = 18A1*, *n = 4ED, MAC-address= 904CE53E2897* and *private key = 8DEC9*. After the sender receives the public key, n value and MAC address from the recipient becomes able to manage the encrypting and hiding process through available selection Encrypt button on the interface that is prepared for this purpose The sender will determine many inputs that are needed to perform this process by insert the public key *e*, value *n* and MAC-Address of the recipient. The both public key *e* and value *n* of the recipient using to encrypt message by RSA algorithm, but the MAC-Address of the recipient hide in the cover file to verify from the Recipient. After the termination

of insert keys, insert the secret message to encrypt, sender will click on *encrypt button* to execute encrypting of the secret message and can see the cipher text in the encrypted message list box, as shown in Figure 7.

Figure 6. Generation Key Process.

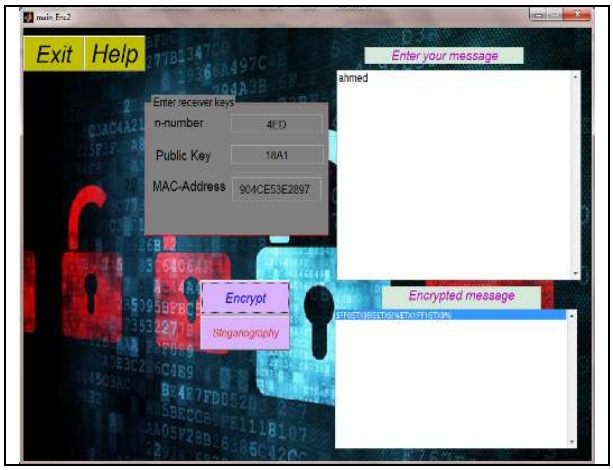

Figure 7. Encrypt Process at a sender.

However, Determine Image file; through the browse option. After the termination of all the above steps, sender will click on steganography button to execute hide cipher text inside the cover file (Image file) after the progress of the processes is completed, a message will be viewed to indicate the success of this process, as shown in Figure 8 describes selecting Image file to hide encrypted message; Figure 9 steganography was completed.

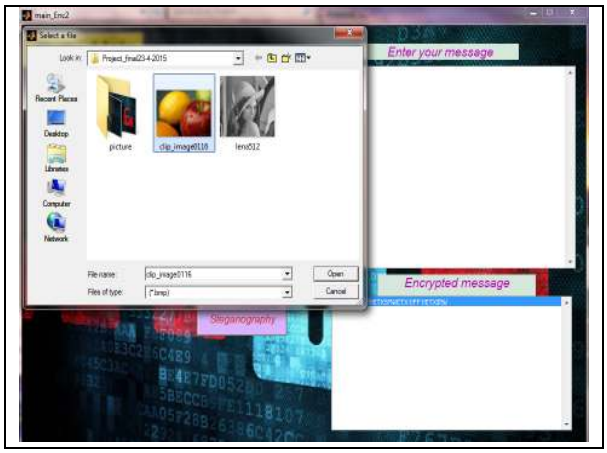

Figure 8. Selecting image file.

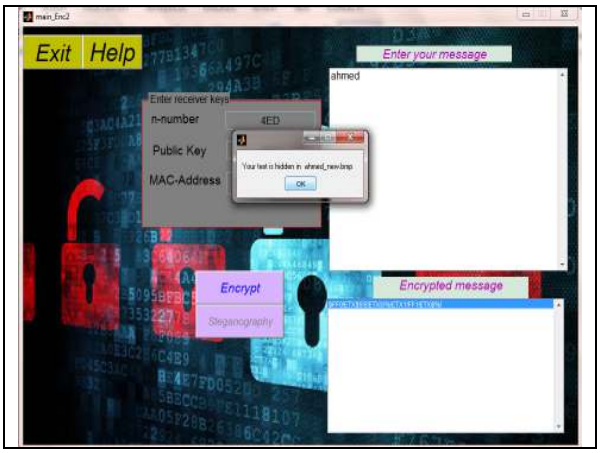

Figure 9. Embedding Process Completed.

Finally, the stego file that is produced which includes the cipher text became ready to be sent to recipient via transmitted channels. How-ever, implement of retracting and decrypting processes at the recipient site after received encrypt-stego file from the sender. The recipient will select decrypt and retract interface that is prepared for this purpose the recipient will determine many inputs to perform this operation, through determining the stego file is by clicking recover text button to choose the desired file, as shown in Figure 10. The software automatically check on the MAC-Address for receiver, if it is true continue process, if not true will be display message no hide message. After that, Insert the private key d to use for decryption the secret message through the use of RSA algorithm, as shown in Figure 11. After the process progress is completed, we will see the secret message after clicking decrypt button.

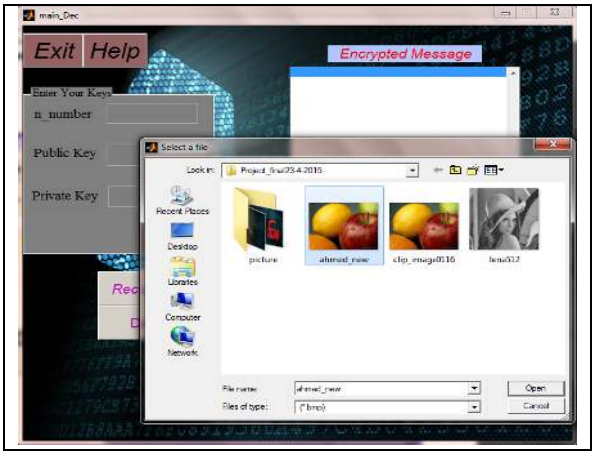

Figure 10. Specify the Stego File.

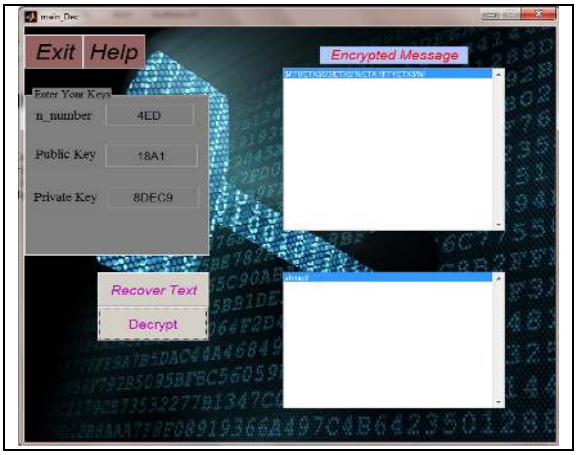

Figure 11. Complete the Decrypt process.

5. Result Discussion

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the stego Image and the original image, whereas PSNR represents a measure of the peak error. result discussion The lower the value of MSE, the lower the error.

$$MSE = \frac{\sum_{M,N}[I_1(M.N) - I_2(M,N)]^2}{M * N} \quad (1)$$

To compute the PSNR, the block first calculates the mean-squared error using the following equation: In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10\, log_{10} \frac{R^2}{MSE} \quad (2)$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating point data type, then R is 1. If it has an 8-bit un-signed integer data type, R is 255, etc.

Figure 12. original image.

Figure 13. steganographic image.

The result of PSNR between original image and steganography image is equal 83.2591. So, the LSB method has been successfully implemented & results are delivered. From the result it is the clear that PSNR is high and MSE is low in LSB based steganography.

6. Conclusion

The Cryptography methods are used widely to secure the online transferred data. However, the Cryptography approaches still have many drawbacks. Thus, the supported security methods are necessary to improve the efficiency of Cryptography. The Steganography approach could be effective method to improve the Cryptography approach. In this our paper, we using hybrid RSA and LSB algorithms the integration between these methods are applicable and reliable. As we are using image as a cover file, high amount of data can be embedded and also provides resistance from external attacks.

References

[1] Adale, D. A. 2011. Hybrid Information Security Models: Crypto-Steg And Steg-Crypto Systems.Tesis HOWARD UNIVERSITY.Washington.,
[2] Al Hasib, A. & A. A. M. M. Haque 2008. A comparative study of the performance and security issues of AES and RSA cryptography. Convergence and Hybrid Information Technology, 2008. ICCIT'08. Third International Conference on. **2** pp. 505-510.
[3] Amin, M. M., M. Salleh, S. Ibrahim, M. R. Katmin & M. Shamsuddin 2003. Information hiding using steganography. Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on. pp. 21-25.
[4] Chang, C.-C. & C.-Y. Lee 2013. A Smart Card-based Authentication Scheme Using User Identify Cryptography. IJ Network Security **15(2)**: 139-147.
[5] Changder, S., N. C. Debnath & D. Ghosh 2009. A New approach to hindi text steganography by shifting matra. Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. International Conference on. pp. 199-202.
[6] Codr, J. 2009. Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide. Retrieved January **8**: 2010.
[7] Dhillon.J 2014. Symmetric and Asymmetric Cryptography Algorithm for Improving Data Security. International Journal of Scientific Engineering and Technology Volume No.**3** (Issue No.8): 1123-1125.
[8] Elgabar, E. E. A. and H. A. A. Alamin "Comparison of LSB Steganography in GIF and BMP Images." International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307.
[9] Goshwe, N. Y. (2013). "Data Encryption and Decryption Using RSA Algorithm in a Network Environment." IJCSNS **13(7)**: 10.
[10] Grantham, B. (2007). Bitmap Steganography: An Introduction, COT.
[11] Guo, L., B. Yan & Y. Shen 2010. Study on Secure System Architecture of IOT. Information Security and Communications Privacy **12**: 042.
[12] Inzunza-González, E., C. Cruz-Hernández, R. López-Gutiérrez, E. García-Guerrero, L. Cardoza-Avendaño & H. Serrano-Guerrero 2009. Software to Encrypt Messages Using Public-Key Cryptography. World Academy of Science, Engineering and Technology 54.
[13] Kothmayr, T., C. Schmitt, W. Hu, M. Brünig & G. Carle 2013. DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Networks **11(8)**: 2710-2723.
[14] Liu, W., Z. Liu & S. Liu 2013. Asymmetric cryptosystem using random binary phase modulation based on mixture retrieval type of Yang–Gu algorithm. Optics letters **38(10)**: 1651-1653.
[15] Marvel, L. M., C. T. Retter & C. G. Boncelet Jr 1998. Hiding information in images. Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on. **2** pp. 396-398.
[16] Mishra, S. February 2015. "A Survey on Crypto-Steganography." International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: **3** Issue: 2 081– 084
[17] Rainie, L., S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown & L. Dabbish 2013. Anonymity, privacy, and security online. Pew Research Center.
[18] Tirthani, N. & R. Ganesan 2014. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. IACR Cryptology ePrint Archive 2014:49

[19] Tyagi, M. V. (2012). "Data Hiding in Image using least significant bit with cryptography." International Journal of Advanced Research in Computer Science and Software Engineering **2**(4): 120-123.
[20] Zmudzinski, S., B. Munir & M. Steinebach 2012. Digital audio authentication by robust feature embedding. IS&T/SPIE Electronic Imaging. pp. 83030I-83030I-7.
[21] SARAIREH, S., AL-SARAIREH, J. A. A. F. E. R., AL-SBOU, Y. A. Z. E. E. D., & SARAIREH, M. (2018). A HYBRID TEXT-IMAGE SECURITY TECHNIQUE. Journal of Theoretical & Applied Information Technology, **96**(9).
[22] Sreekutty, M. S., & Baiju, P. S. (2017, April). Security enhancement in image steganography for medical integrity verification system. In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on (pp. 1-5). IEEE.
[23] AL-SARAIREH, J. A. (2017). HVM: A METHOD FOR IMPROVING THE PERFORMANCE OF EXECUTING SQL-QUERY OVER ENCRYPTED DATABASE. Journal of Theoretical & Applied Information Technology, **95**(14).
[24] Abood, M. H. (2017, March). An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms. In New Trends in Information & Communications Technology Applications (NTICT), 2017 Annual Conference on (pp. 86-90). IEEE.
[25] Saraireh S. S., Saraireh M. S., Saraireh S. S., and Saraireh M. S. (2017, Feb), "Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange," Int. J. Commun. Antenna Propag., vol. **7**, no. 1, p. 1.
[26] Rahim, R., Nurdiyanto, H., Hidayat, R., Ahmar, A. S., Siregar, D., Siahaan, A. P. U., . . . Zamsuri, A. (2018). Combination Base64 Algorithm and EOF Technique for Steganography. Paper presented at the Journal of Physics: Conference Series.
[27] Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A., & Bhat, G. M. (2018). Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. Multimedia Tools and Applications, **77**(1), 185-207.