Images Steganography Approach Supporting Chaotic Map Technique for the Security of Online Transfer

Yasser Mohammad Al-Sharo
Faculty of Information Technology
Ajloun National University, Jordan

***Abstract*—One of the most important issue in this domain is the security concern of the transfer data. The online transfer data may access illegally through attack the communication gate between the servers and the users. The main aim of this study is to enhance the security level of the online data transfer using two integrated methods; images steganography to hide the transfer data in image media, and chaotic map to remap the original format of the transfer data. The integration between these two methods is effective to secure the data in several format such as text, audio, and images. The proposed algorithm is the prototyped using JAVA programming, 20 images and text messages of usable sizes (plain data) were tested on the dataset using the developed programming. The simulation using local server is accomplished to analyze the security performance based on two factors; the plain data size and the data transfer distance. Many attacking attempts are performed on the simulation test using known attacking techniques such as observe the stego images quality. The experiment results show that about 85% of the attacking attempts fail to catch the stego images. 95% of the attacks fail in remap meaningful parts of the chaotic data. The results indicate the very good level of the propose security methods to secure the online transfer data. The contribution of this study is the effective integration between the steganography and chaotic map approaches to assure high security level of online data transfer.**

Keywords*—Security; steganography; chaotic map; encryption; network data

I. INTRODUCTION

The era of the globalization increase the importance of online data/information transfer as one of the most important success keys of the businesses competitive advantages [1]. Through the online gathering of the data, the businesses gain many advantages such as: (i) reduce the operational costs of gather the data between the organization branches, department, and users; (ii) improve the products quality based on real time services; (iii) assure the availability and accessibility of the services in anytime and from anywhere. However, several security threats such as viruses, warms, and hacking are concerns of the online data transfer [2,3,4].These threats could damage or stole the transfer data via the internet gate, which may lead to the fail of the technology of online data transfer. Thus it is important to assure the high security level of the online data transfer to allow the originations to gain the expected business benefits without high risks.

The security of online data transfer is not simple due to many factors like the volume of the transfer data, the format of the transfer data, and the transfer distance [5]. These factors effect on the selection of the security methods that could be applied to secure the online transfer data. For example, the symmetric or asymmetric encryption techniques are not suitable to encrypt large volume of data, especially the data of images, video, or audio format [6,7]. Hence, the selection of applicable security methods would be decided based on many factors that related to online data transfer.

The Steganography is effective approach that would be used to hide the online gathered data using the embedding images [8]. Steganography is effective due to many reasons such as ability to hide the data of various formats, ability to hide large volume of plain data, and the effectiveness of transfer hidden data over large transfer distance [8]. According to [9], The Steganography is more effective than the cryptography approaches due to difficulty of catch the plain data by the attacker and tries to decrypt it using many attacking techniques such as automatic decryption keys.

Kumar and Pooja [10] mentioned that although steganography is effective security approach, there plain data is hide as its original form, which make it simple for extract the plain data in case of catch the embedded data by the attacker. Therefore, it is more useful to support the steganography by other encryption or security techniques in order to hide encrypted data in the embedded image rather than hide the plain data as it is. For this purpose the chaotic map technique could be applied. In security systems, the chaotic scheme is used to create random swapping of plain information to increase the difficulty of stole the original information by attacker (Khan, & Shah, 2014). Technically, some elements positions of plain information are swapped using random sub situation key. The original values of swapped elements are updated to include the real value of the element plus the value of original element position [11]. This increases the difficulty of access the real value of plain information. The chaotic map is applicable to secure the various formats and volume of online transfer data.

Consequently, the steganography and chaotic map methods could be integrated effectively to secure the online transfer data. The plain data can be secured using chaotic map technique before hide the secured data in embedded file or image (steganography). Thus, it is complex to extract and remap the hidden and secured data due to necessity of accomplish two hacking stages on two effective security methods of online transfer data. The attackers need to know and catch the stego data, then remap the chaotic data, which expected to be so hard.

Keep in mind the above discussion, the main aim of this study is to enhance the security level of the online transfer data using two integrated methods (steganography and chaotic map). In this study, the algorithm of the proposed methods would be suggested, the prototype of the algorithm will explain, and the experiments tests would be conducted. The next section discusses the related works in order to construct the propose algorithm, the third section will explain the details of the research methods, section 4.0 discusses the findings, and lastly, Section V provides the study conclusion and the future works.

II. Related Works

Mollah et al. [6] explain the three junctions of the security of online data transfer; security of the users' devices, server security, and the security of communication paths. Most of data attacks are happen at the communication path [12], which represents the wire or wireless connection between the server and the users' devices.

The researchers propose several security methods to improve the security level of the transfer data via the online connections. The symmetric and asymmetric data encryption methods are effective to secure the textual plain data [6, 7, 13]. Although the data encryption is not expensive earthier in time or money, the symmetric and asymmetric is not effective for the large volume data such as images, audio or video.

Other researchers propose the load balancing method to assure that the transfer data is not holding in the connection paths due network traffic [14-17]. The load balancing technique aims to analyze the free connection paths and estimate the transfer paths of the whole data or blocks of data. This technique is helpful to reduce the opportunity of attack the hold data in the connection paths. The main drawback of load balancing is the possibility of rapid change in the network traffic, which require costly requirements of pre-paths booking. On other hand, the balancing technique is based on transfer the data as its plain form without encryption processes. Therefore, the risk of attack the data will be high.

Furthermore, the offloading transfer techniques is security methods that proposed by many researchers [12, 18- 21]. The offloading is based on reduce the online processes of data transfer as possible as can. The online connections are for the purpose of data transfer between the organization server and the online server. Hence, the data via offline mode can be gathered between the organization server and the users. Although, the offloading technique reduce the number of online connections, the organization need to have expansive network requirements such as offline servers and offline connections based on wire technology.

Additionally, the researchers suggested the devices signatures to improve the security level of online connections [22-24]. The signatures of users' devices can be defined in advance to access the services of online data transfer. The strange signature will be prevented from access the network services. Device signature is effective in case of small number of users or specific network services in the organizations. It is not possible to define the large number of signatures of users' devices, especially when the online services are global for all possible users such as yahoo email.

The steganography is proposed by many researches as effective security method to hide the plain data in embedding files such as images [25- 27]. Hence, it is difficult to detect the embedding files and extract the plain data from these files. Mahajan and Kaur [5] surveyed the main factors that could improve the steganography effectiveness. The main analyzed factors are the plain data characteristics (such as format and size), embedding files characteristics, and the data transfer distance. The selection of the embedding files is affected by the plain data characteristics and the transfer distance. The speed of data transfer is important to minimize the data attacking that may cause due to data holding/waiting in the transfer paths. Hence, it is not recommended to use large size of embedding files for steganography. Hence, the steganography effectiveness can be assured through use supporting techniques to strength the plain data security using suitable size of embedding files.

Sedighi et al. [26] discuss the steganography processes and calculations as Fig. 1 illustrates. The most useful embedding file that could use in the steganography is the image type. In order to assure effective stego processes, the candidate embedding image should be analyze (like variance estimation and detectably calculation) to deicide the most suitable part to hide the plain data. The main purpose here is the hide the plain data in embedding image that hard to be observed by the attackers. Thus, the plain data would code in a manner that not-effect on the quality of the embedding image.

Sedighi et al. [26] founded that it is effective to hide the plain data in a part of embedding image based on two main processes. Firstly, analyze the quality and variance of the embedding image based on the following equation:

$$R(\beta) = \sum H(\beta n)$$, Where R (β) is the lightness volume of the image parts. (1)

Based on the above equation it is useful to hide the plain data in the most lightness part. The second process is to decide what the pixels that can be replaced by the plain data with minimum effect on the selected part quality, and this can be obtained using the following equation:

$$D(x,y) = \sum \rho n[xn \; != yn],$$ (2)

Where $\rho n \geq 0$ is the cost of changing pixel xn tied to βn via: $\beta n = e \lambda \rho n / 1 + 2 e \lambda \rho n$, with $\lambda > 0$ determined from the payload constrain of the Equation #1

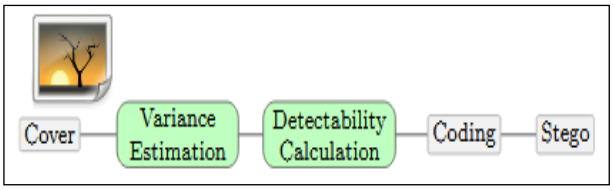

Fig. 1. Steganography Processes (Sedighi et al., 2016).

Another effective security technique is the chaotic scheme, which is used to create random swapping of plain dta to increase the difficulty of stole the original information by attacker [23]. The chaotic can be described in four main points which are: (1) permutation, where the values of the selected bits/pixels in the plain data are updated as the value of the pixel/bit plus the value of the position. Here it is necessary to work based on permutation to simplify the remapping of the updated data; (2) substitution, whereby the position of each updated bit/pixel is swapped with other bit/pixel. The De-substitution key is necessary to be known by the destination. The permutation and substitution rounds are depend on the data size; (3) De-substitution data using the key that owned by the destination; (4) De-permutation the data using the key that owned by the destination [11]. The main advantage of the chaotic map is the possibility to deal with plain data of various sizes and different format. However, the drawback of this technique is possibility to attack the data through trying to know the De-permutation and De-substitution keys.

Table I summarizes the advantages and disadvantages of the reviewed security methods and techniques. It can be concluded that the most useful integration could happen between the steganography method and the chaotic map technique.

III. Research Methods

As concluded from the above section the integration between the steganography and the chaotic map could conduct effective security level of the online transfer data. The scope of this study is the protection of online transfer data of text and image format due to wide using of these formats in the transferring processes. Fig. 2 illustrates the proposed integration processes. Firstly, the plain data will be protected using chaotic map technique through the permutation and substitution phases. The de-fusion key in each phase will be produced to simplify the remapping of the plain data. The suggested permutation rounds are 200 due to size of the plain data, which will explain in the dataset features in this section. The substitution rounds are 100 (half of permutation rounds). Each two permutation bits/pixels (two permutation rounds) will substitute in one round.

As illustrates in Fig. 2, after conduct the chaotic map processes, the produced data will processed by the steganography method. The format of embedding file is images due to effectiveness of hide the data in images with low affections on the images quality. Thus, the attacker will found difficulty in detecting the embedding images. The steganography processes are: (i) detect the most lightness parts in the embedding images using equation 1; and (2) replace the detected parts by the data that already processed by the chaotic map. In total, the chaotic technique will remap the plan data to increase the difficult of get meaningful data, and the steganography hide the chaotic data to increase the difficulty of catch the online transfer data. Hence, it is hard to attack the protected images using two effective and integrated security approaches (steganography and the chaotic map).

TABLE I. Summary of Security Methods and Techniques

Source	Security technique	Advantages	Disadvantages	Conclusion
[6, 7, 13]	Data encryption	-Not expansive -fast processes	- Used for textual plain data only. - challenges in handle the large data volume.	Can be used for online data transfer of texts. however, it is not recommended for the large data sizes.
[14, 15, 16, 17]	Load balancing	-Avoid the data holding in the online connections.	- The data not encrypted. - The unexpected traffic may happen when transfer the data.	Can be used as supportive technique beside other data security methods.
[12, 18, 19, 20, 21]	Offloading Transfer	-Reduce the online connections between the users and the online server.	- Require expansive requirements.	Can be used for local services of the organizations.
[22, 23, 24]	Device signature	- prevent the strange devices from accesses the network services.	- not possible for open access services of undefined users such as yahoo email.	Used for limit services of online data transfer.
[25, 26, 27]	Steganography	- Difficulty of detect the embedding files.	- The plain data is Hide as its original form.	Need to be supported by other technique.
[11, 23]	Chaotic Map	- Deal with data of various sizes and formats.	Ability to handle the De-permutation and De-substitution keys.	Can be use as supportive technique rather than main technique.

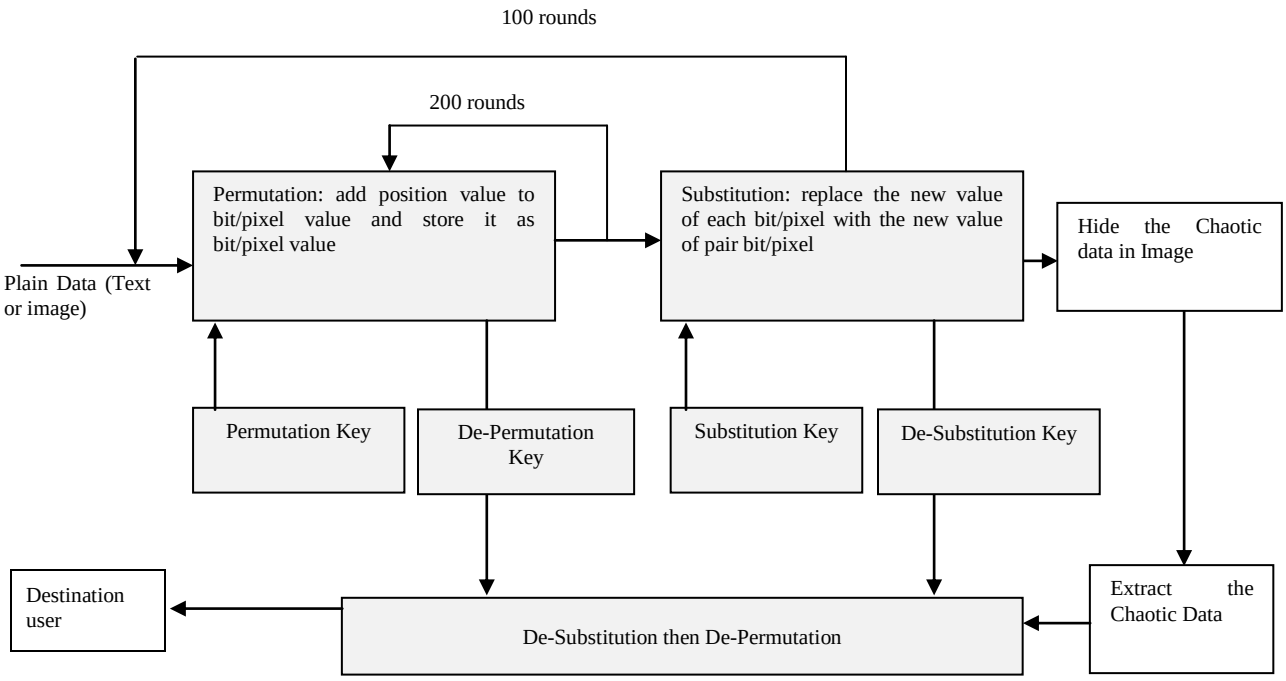

Fig. 2. Methods Design.

Based on the proposed methods in this study, a prototyping using Java programming language is developed to handle the following algorithm:

1. *Get plain data (text or image).*
2. Select 200 bits/pixels randomly.
3. The value of each selected bit/pixel= the value of the bit/pixel + the value of the current position.
4. Store the permutation key that used in previous step.
5. Randomly swap each bit/pixel in step 3 and with pair bit/pixel.
6. Store the permutation key that used in previous step.
7. Store the produced data
8. Detected the lightness of the embedding image: $R(\beta) = \sum H(\beta n)$
9. Hide the data in step 7 in the detected part in step 8: $D(x,y) = \sum \rho n[xn \; != yn]$.
10. Save the embedding image that contains the swapped plain data.

The dataset of this study is composed of the embedding image for the purpose of steganography, and this dataset is adopted by Mahajan & Kaur (2012) study for purpose such as steganography. The dataset is called Kodak which consists of 12 testing image of different features. The main features in dataset images are the quality (PSNR) and images dimensions. These features play important role in increase the steganography effectiveness. Table II summarizes the features of the steganography dataset.

In order to test the algorithm prototyping based on the experimental database, a network simulation is conducted using MATLAB distributed toolbox. Through this toolbox the online data transfer is simulated between two users over large transfer distance i.e. 5000 KM. The simulation includes many attacks techniques that produced at the connection paths of the simulation while transfer the data. The steps of the used attacking techniques are adopted from da Silva et al. [29] and Van Den et al. [30]. The adopted steps are programmed and simulated using MATLAB, and the main attacks techniques are as the following [31]: (1) Traffic analysis: this technique work on detect the embedding files of sizes over the usual or standard sizes i.e. image of size in MBs. This technique can be used to detect the embedding images of steganography. (2) Eavesdropping: this technique is usually used to capture the security keys between the sender and receiver (such as de-permutation key in chaotic map) before trying to resolve the plain data suing the captured keys.

TABLE II. FEATURES OF THE STEGANOGRAPHY DATASET

Image Name	Image Type	Image Size	Image Dimensions	Image Quality (PSNR)	Images Color Type
House	PNG	30.6 KB	256*256	25	Grayscale
House	PNG	28.3 KB	256*256	28	Grayscale
House	PNG	25.6 KB	256*256	33	Grayscale
House	PNG	26.4 KB	256*256	39	Grayscale
Lena	PNG	129 KB	512*512	25	Grayscale
Lena	PNG	250 KB	512*512	28	Grayscale
Lena	PNG	370 KB	512*512	33	Grayscale
Lena	PNG	400 KB	512*512	39	Grayscale
Kodak	PNG	511 KB	768*512	28	Color
Kodak	PNG	730 KB	768*512	30	Color
Kodak	PNG	802 KB	768*512	33	Color
Kodak	PNG	818 KB	768*512	43	Color

IV. DISCUSSION AND FINDINGS

As mentioned in the previous section, the proposed algorithm (in integration between steganography and chaotic map) was tested on dataset of 12 embedding images and simulated based on large distance of online data transfer.

The observation of the steganography processes indicates that the colored images of high PSNR (i.e. PSNR> 40) would be effective in hide the plain data of image type more than the gray-scale images of PSNR < 30; The size of plain images is up to 500 KB. Fig. 3 show embedding image quality before and after hide the plain data of image type. Thus, it is better to secure the plain data of images type using colored plain images.

On the other hand, it is effective to secure textual plain data of size up to 300 KB using gray-scale embedding image of PSNR> 30. Fig. 4 shows the quality affection of embedding image after hide text plain data up to 300KB size. Hence, the gray-scale embedding images of PSNR>=30 is used to hide the plain data of text type.

The effective embedding images are selected to hide the plain data of images and texts. These images are used to apply the proposed algorithm of this study based on the following experimental processes:

- The chaotic map is conducted on the plain data before complete the steganography processes.
- The network simulation is constructed using MATLAB distributed system.
- The embedding images that contain the plan data are transfer over large distances (i.e. 1000, 2000, and 5000 KM).
- The transfer data are attacked using two techniques; traffic analysis and eavesdropping.

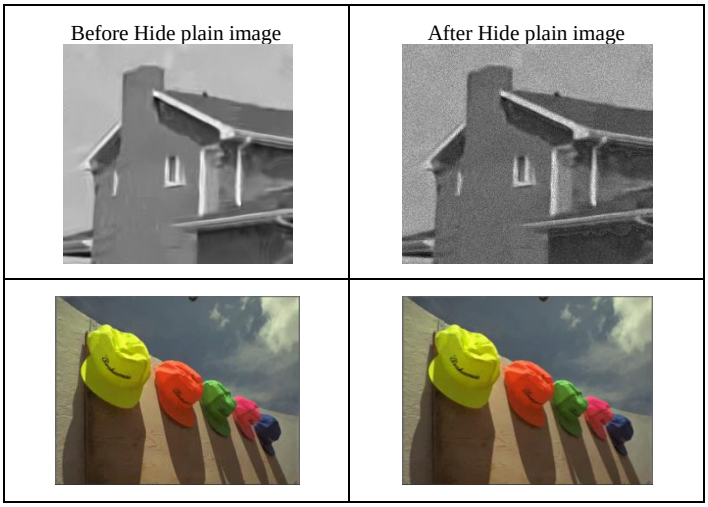

Fig. 3. Embedding Image Quality to Hide the Plain Images.

Fig. 4. Embedding Image Quality to Hide the Plain Texts.

The experimental processes conducted on 20 plain data; 10 image messages and 10 texts messages. The sizes of the images messages are between 400-500 KB, and the sizes of the text messages are between 100-300 KB. Fig. 5 shows the analysis of attacking techniques on the embedding files that contain the plain images. The traffic analysis technique fail in detect 8/10 embedding images. Consequently, the eavesdropping attacking technique fails in remap any plain data of the two detected embedding images.

On the other hand, Fig. 6 shows the analysis of attacking techniques on the embedding files that contain the plain texts. The traffic analysis technique fail in detect 9/10 embedding images. Consequently, the eavesdropping attacking technique success on remap meaningful parts of the plain text in the detected embedding image due to success of resolve the remapping keys.

Based on the experimental tests, it can be concluded that the proposed integration between the steganography and chaotic map techniques is effective. 17 out 20 embedding images (85% of all embedding images) are not detected by the attacks. On the other hand, 19 out 20 plain data (95% of the transfer data) are not resolved by the attacks. It is necessary to mentioned that the steganography represent the first defending stage in the proposed security algorithm, and the second defending stage is represented by the chaotic map.

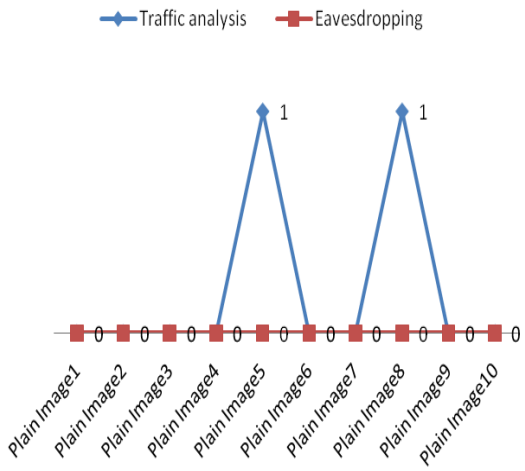

Fig. 5. Attacking on Plain Images.

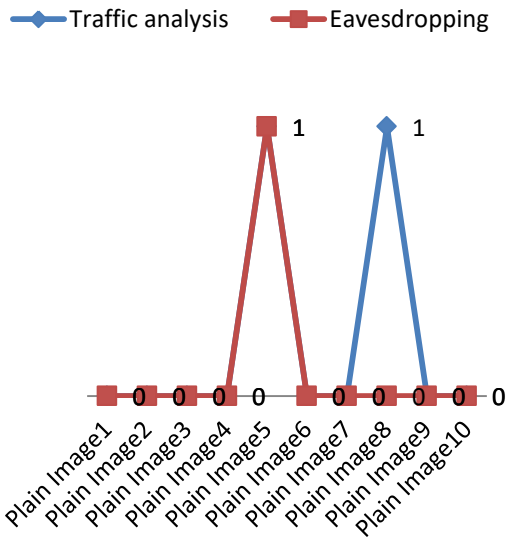

Fig. 6. Attacking on Plain Texts.

V. Conclusion and Future Works

The various businesses are gain benefit from the online transfer data. Hence, the security of the online transfer data is very important to assure the safety of businesses data. Several security approaches and techniques are reviewed in this study. The objective of this study is to perform the integration between the steganography and chaotic map techniques in order to secure the online data transfer. The proposed algorithm, prototyping, and simulation of the proposed techniques are conducted. The experimental results show the difficulty of attack and resolve the plain data due to difficulty of attack the two integrated security stage in this study. In the future, more experimental tests will be conducted based on different features of the embedding images, different selections of chaotic map, and different sizes of the plain data.

References

[1] Grabara, J., Kolcun, M., & Kot, S. (2014). The role of information systems in transport logistics. International Journal of Education and Research, 2(2), 1-8.

[2] Masala, G. L., Ruiu, P., & Grosso, E. (2018). Biometric authentication and data security in cloud computing. In Computer and Network Security Essentials (pp. 337-353). Springer, Cham.

[3] Haager, J., Sandwith, C., Terrano, J., & Saripalli, P. (2018). U.S. Patent No. 9,990,502. Washington, DC: U.S. Patent and Trademark Office.

[4] Kulkarni, M. P., Ghumare, S. A., & Kulkarni, A. (2016). Electronic Fund Transfer: A study of security control in selected banks of Pune Region. International Journal on Recent and Innovation Trends in Computing and Communication, 4(5), 486-489.

[5] Mahajan, M., & Kaur, N. (2012). Adaptive steganography: a survey of recent statistical aware steganography techniques. International Journal of Computer Network and Information Security, 4(10), 76.

[6] Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38-54.

[7] Liaqat, M., Chang, V., Gani, A., Ab Hamid, S. H., Toseef, M., Shoaib, U., & Ali, R. L. (2017). Federated cloud resource management: Review and discussion. Journal of Network and Computer Applications, 77, 87-105.

[8] Hamid, N., Yahya, A., Ahmad, R. B. & Al-Qershi, O. M. 2012. Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS) 6(3): 168.

[9] Nameer, N. & Eman, E. 2007. Hiding a Large Amount of Data with High Security using Steganography Algorithm. Journal of Computer sciences 223-232.

[10] Kumar, A. & Pooja, K. 2010. Steganography-a Data Hiding Technique. International Journal of Computer Applications IJCA 9(7): 24-28.

[11] Mishra, M., Singh, P. and Garg, C., 2014. A New algorithm of encryption and decryption of images using chaotic mapping. International Journal of Information & Computation Technology. ISSN, pp.0974-2239.

[12] Akherfi, K., Gerndt, M., & Harroud, H. (2016). Mobile cloud computing for computation offloading: Issues and challenges. Applied Computing and Informatics.

[13] Anwar, S., Inayat, Z., Zolkipli, M. F., Zain, J. M., Gani, A., Anuar, N. B., & Chang, V. (2017). Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey. Journal of Network and Computer Applications, 93, 259-279.

[14] Ghomi, E. J., Rahmani, A. M., & Qader, N. N. (2017). Load-balancing algorithms in cloud computing: A survey. Journal of Network and Computer Applications, 88, 50-71.

[15] Aslam, S., ul Islam, S., Khan, A., Ahmed, M., Akhundzada, A., & Khan, M. K. (2017). Information collection centric techniques for cloud resource management: Taxonomy, analysis and challenges. Journal of Network and Computer Applications.

[16] Madni, S. H. H., Latiff, M. S. A., & Coulibaly, Y. (2016). Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. Journal of Network and Computer Applications, 68, 173-200.

[17] Gani, A., Nayeem, G. M., Shiraz, M., Sookhak, M., Whaiduzzaman, M., & Khan, S. (2014). A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing. Journal of Network and Computer Applications, 43, 84-102.

[18] Bhattacharya, A., & De, P. (2017). A survey of adaptation techniques in computation offloading. Journal of Network and Computer Applications, 78, 97-115.

[19] Vaezpour, S. Y., Zhang, R., Wu, K., Wang, J., & Shoja, G. C. (2016). A new approach to mitigating security risks of phone clone co-location over mobile clouds. Journal of Network and Computer Applications, 62, 171-184.

[20] Shaukat, U., Ahmed, E., Anwar, Z., & Xia, F. (2016). Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges. Journal of Network and Computer Applications, 62, 18-40.

[21] Shuja, J., Gani, A., ur Rehman, M. H., Ahmed, E., Madani, S. A., Khan, M. K., & Ko, K. (2016). Towards native code offloading based MCC frameworks for multimedia applications: A survey. Journal of Network and Computer Applications, 75, 335-354.

[22] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[23] Khan, M. and Shah, T., 2014. A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. Neural Computing and Applications, 25(7-8), pp.1717-1722.

[24] Khan, S., Shiraz, M., Boroumand, L., Gani, A., & Khan, M. K. (2017). Towards port-knocking authentication methods for mobile cloud computing. Journal of Network and Computer Applications, 97, 66-78.

[25] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), 17333-17373.

[26] Sedighi, V., Cogranne, R., & Fridrich, J. (2016). Content-adaptive steganography by minimizing statistical detectability. IEEE Transactions on Information Forensics and Security, 11(2), 221-234.

[27] Rani, M., & Bedi, C. S. (2015). Review of Various Image Steganography Techniques and Different Type For Data Hiding Scheme. ZENITH International Journal of Multidisciplinary Research, 5(9), 19-23.

[28] Liu, J., Ahmed, E., Shiraz, M., Gani, A., Buyya, R., & Qureshi, A. (2015). Application partitioning algorithms in mobile cloud computing: Taxonomy, review and future directions. Journal of Network and Computer Applications, 48, 99-117.

[29] da Silva, E. G., Knob, L. A. D., Wickboldt, J. A., Gaspary, L. P., Granville, L. Z., & Schaeffer-Filho, A. (2015, May). Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study. In Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on (pp. 165-173). IEEE.

[30] Van Den Hooff, J., Lazar, D., Zaharia, M., & Zeldovich, N. (2015, October). Vuvuzela: Scalable private messaging resistant to traffic analysis. In Proceedings of the 25th Symposium on Operating Systems +Principles (pp. 137-152). ACM.

[31] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506.