Review of secure the online multimedia data using chaotic map and steganography techniques

Cite as: AIP Conference Proceedings **2404**, 030001 (2021); https://doi.org/10.1063/5.0068876
Published Online: 11 October 2021

Zainab Amin Al-Sulami and Hayder Salah Hashim

Review of Secure the Online Multimedia Data Using Chaotic Map and Steganography Techniques

Zainab Amin Al-Sulami [1, a)] and Hayder Salah Hashim [2, b)]

[1]*College of sciences, University of Basrah, Basrah, Iraq*
[2] *College of Administration and Economics, University of Basrah, Basrah, Iraq*

[a)] Corresponding author: zainab.abduljabba@uobasrah.edu.iq
[b)] Hayder_alasadi@uobasrah.edu.iq

Abstract. The security of data is considered as important issue in any organization. The highly level of security is required to prevent data attacked, damaged or stolen. The online data transfer is rapidly on demand to reduce the costs and time for the organization. This study aims to discuss security approaches that could be adopted in order to secure data transfer online. The literature in the security domain is discussed to determine the most suitable security techniques for the transfer data depends on the data nature, i.e. textual, video, images, or audio data. The discuss shows that techniques such as encrypted data are suitable to safe the textual transfer data. The chaotic map and steganography techniques are suitable to protect the images, video, and audio data. Steganography works to hiding the data in other plain media such as images. The chaotic map works on remapping the data pixel map in order to maximize the complexity of handling the original data by the attackers. It is recommended to offer integration between the security techniques to improve data transfer protection. For example, the data encryption would be supported by other techniques such as a chaotic map, and the steganography can be supported by techniques such as chaotic map. This paper offers important evidences about the security techniques that would be adopted which depends on the nature of data transfer as well as the integration between the techniques to enhance the protection of data transfer. The users or organizations can adopt security techniques according to their data in the environment of working. In the future, the privacy techniques of data transfer would be investigated to prevent the illegal accessing of the data.

INTRODUCTION

The online gates lead to the globalization revolution, whereby the data is transferred in real-time. The online data transfer makes it available and accessible at any time and from anywhere [1]. Thus, the online data transfer supports the competitiveness of the organization through reducing the time and costs of gathering business data. Security is one of the main concerns of online data transfer [2]. Security threats like viruses and worms could damage the data [3]. On the other hand, the attackers could steal the data that transfer via online gates. Hence, security concerns could limit the business applications of online data transfer. Consequently, the data must be highly protected in order to motivate the use of the applications of online data transfer. The data transfer security is falling in three directions; (1) the security of users' devices, (2) the security of data hosts (i.e. servers), and (3) the security of the online gates between the devices and the servers [4]. The data attacks mainly happen at the connecting gates fold, especially in the case of wireless connections [5]. Thus, this paper focuses on the effective security approaches that would be deployed to protect the data transfer at the connection layer.

There are several security techniques that can deploy to protect transfer data. However, the selected technique should be selected effectively depending on many factors such as data type, data size, and transfer distance [6], [7], [8]. The textual data would be secured using encryption techniques (i.e. symmetric), but the data encryption is not useful for data types such as audio or images [9]. Therefore, it is essential to observe the features of the available

2nd International Conference on Engineering & Science
AIP Conf. Proc. 2404, 030001-1–030001-8; https://doi.org/10.1063/5.0068876
Published by AIP Publishing. 978-0-7354-4136-1/$30.00

security approaches in order to protect the data transfer according to its nature. Hamid et al. [10] mentioned that the Steganography approach is effective to secure the large volume of data transfer of any type. However, this approach costs much processing and time. Steganography works by hiding the plain data in other media for instance audio, image, or video [11].

Moreover, a chaotic map is considered as an effective security technique that works on remapping the pixels map of the plain data in order to maximize the complexity of catching the original data forms by attackers. The chaotic map can deploy on data of any type and any size [12], [13], [14]. In total, this research mainly aim to discuss the various security techniques for adoption to save the transfer of data online according to the data type. Section 2 discusses the related works of the security of data transfer, section 3 provides the discussion of the related works, and section 4 presents some recommendations based on the discussion of the works, and section 5 presents the future works along with the conclusion of this discuss.

RELATED WORKS

This section discuss the most important security techniques for online data transfer such as data encryption, load balancing, offloading data, device signatures, chaotic map, and steganography.

Data Encryption

There are two types of methods that used to protect the data which are symmetric and asymmetric data encryption methods [9]. Both methods work on protecting data using a security key or code. Thus, the data should be decrypted using decryption key. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. Figure 1 illustrates symmetric data encryption [15]. But, Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys [16]. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security [17]. A public key is made freely available to anyone who might want to send you a message. Figure 2 illustrates Asymmetric data encryption [15]. The second private key is kept a secret so that you can only know. The main advantages of the symmetric and asymmetric data encryption are the simplicity and cost low for the processes. However, symmetric and asymmetric data encryption is not effectively secure data with a large size such as audios and videos. Exclusively, it is only working effectively to secure the textual data.

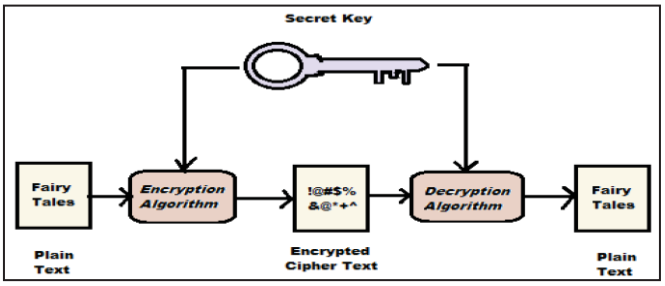

FIGURE 1. Symmetric data encryption [15]

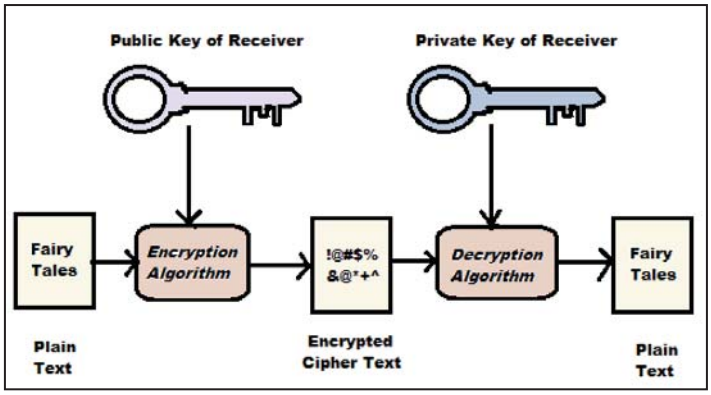

FIGURE 2. Asymmetric data encryption [15]

Load Balancing

The researchers mentioned that the data holding in the online connection paths lead to increase the opportunity to attack these data [18]. Thus, it's important to assure the speed of data transfers. The load balancing approach works on the segment the data into small parts or blocks and remerges the block at the destination device [18], [19].

The load balancing technique is helpful to estimate the data transfer according to free network paths [20]. However, the major disadvantage of this technique is the fast change in network traffic. Thus, the transfer data block may fail under the condition of the successful submission of all data blocks to the destination device. Any fail in submit the transfer blocks lead to rejecting the overall transfer process. Another drawback is that the data transfer is not protected by methods such as encryption techniques, whereby the attackers may handle some or all transfer data in an easy way.

Offloading Data

Many researchers suggested the offloading data technique as an effective method to secure the on online data transfer [5], [21].The offloading data transfer works on minimizing the processes of online data transfer into the most limited level. The organizations would apply the offline mode to transfer the data internally between the users' device and the organizational server [22]. The transfer online mode could only be used between the organizations servers and the online host in the necessary data. Thus, the attackers cannot attack the transfer data based on the offline mode.

The technique offloading security is effective to reduce the online processes of data transfer, whereby the attackers will be prevented from accessing the offline data transfer. However, this technique is not effective when the offline mode is applied. Another drawback is the need to have expansive network equipment to apply for the offline data transfer in the working environment.

Device Signature

The researchers suggested the device signatures technique as an effective approach to secure the online data transfer [23], [24].The signatures of users' devices should be recorded as friend devices to the network. Thus, the stranger signatures will not be allowed to access the network. Any trusted device or user needs to be defined in advance through discuss and register processes by the network administrator. The non-trusted devices will be defined as attackers and it will be allowed to use the network equipment.

The device signature is considered an effective method when handling a limited number of users in the organizations. However, the large numbers of user's devices are difficult to define, particularly, in the case of global online services for all users such as Gmail service.

Steganography

The steganography are effective security techniques suggested by several studies to provide secure online data transfer [25].Steganography works on embedded the plain data in other media such as video, audio, or images. The images are the most embedding media adopted in this approach [11].

Hence, the steganography maximizes the complexity of detecting the plain data by the attackers. However, there are many factors that affect the steganography effectiveness, such as the plain data size, embedding files quality, and the distance of the transfer [26].These factors require a useful selection of the embedding media in order to assure that the attackers will not notice the embedded data. The data attack that caused by (holding-waiting) of data in the paths of transfer can be minimized by the speed of the data transfer. Consequently, large size embedding file are not recommended for use in steganography. On the other hand, [27] explained that steganography should select effective embedding media size depends on the size of the plain data.

Furthermore, [28] clarified the steps of the steganography approach (Figure 3). The suitable embedding file would be selected depends on the size of the plain data and the distance of transfer. Choosing files to embed could be conducted based on attributes, such as file size, variance estimation, and color distribution. Thus, the plain data can be hidden in the most suitable parts in the embedding file. The steganography analyses' main goal is to conceal the plain data in embedded sections that the attackers will experience difficulties during the attempts to obtain it.Therefore, Can be plain data coded with low effect on the embedding file quality.

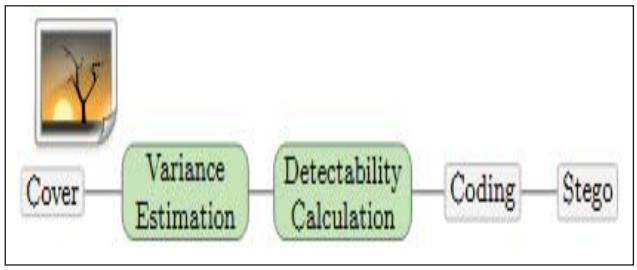

FIGURE 3. Steganography approach [28]

In [28] explained the required computation for effective steganography processes. Firstly, it is required to estimate the variance and quality of the embedding files equation (1):

$$R(\beta) = \sum H(\beta n) \quad \ldots (1)$$

Where R (β) is the amount of lightness of the image components, and n is number of pixels in the image.

It is essential to select the most lightness pixels as useful embedding parts of the plain data, based on the above equation (1).

The second computation stage is the replacement, whereby the plain data will substitute certain pixels with minimal impact on the quality of the embedding images. This move can be carried out according to equation (2):

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

Where n is the number of pixels in the image, $\rho n \geq 0$ 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).

Chaotic Map

Another effective security approach for the transferred data is the chaotic map. This approach works on rearranging the pixel map of the plain data through random pixels swapping. Thus, the attackers will find difficulty in catching the original map of the plain data. The destination users can use the map key to back the pixel map to the original form.

The chaotic map approach can be conducted using four main steps [29], which are as the following:

(1) Permutation: The randomly selected pixels in the plain data will be swapped with other pixels. The swapped pixels will be stored in the new positions as the original pixel value added to the original pixel position.

(2) Substitution: The number of substitutions is identified by the users. For example, if the user selects 50 substitutions, then 100 pixels will be swapped randomly. It is important to create the De-substitution key to remember the swapped pixel.

(3) De-substitution: The destination user can use the De-substitution key to re-swap the pixels as its original position. The position can be decoded based on the process #1.

(4) De-permutation: The original plain data can be decoded through extract the pixels values by the owned key of the destination.

The most beneficial feature of the chaotic map is the ability to conduct this approach on various plain data such as texts, images, videos, and audios. However, this approach can be attacked when the attackers try to resolve the De-permutation and De-substitution keys. Figure 4 illustrates the processes of the chaotic map.

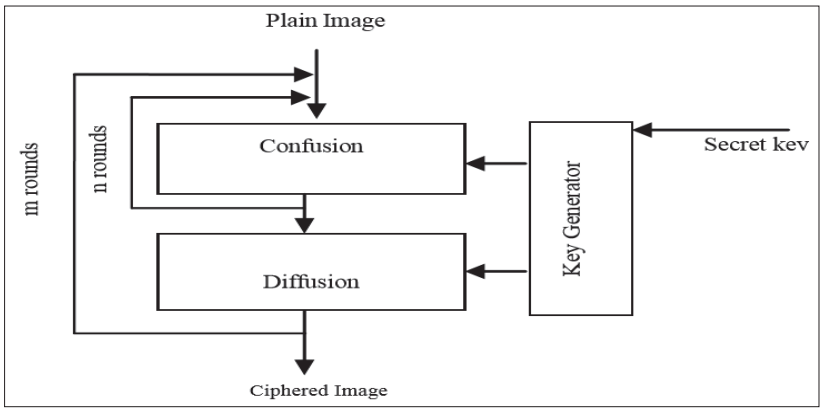

FIGURE 4. Structure of Chaotic Map [30]

DISCUSSION OF SECURITY TECHNIQUES FOR DATA TRANSFER

In the previous section, there are six security techniques were presented to secure the online data transfer; data encryption, balance loading, offloading transfer, device signature, Steganography, and chaotic map.

Each of the presented security techniques has advantages and disadvantages in the context of the security of data transfer online. The symmetric and asymmetric encryption methods use a security key to change the forms of plain data. The encryption cost is increases as the size of plain data is increases. Hence, the encryption methods (symmetric and asymmetric) is easy and not expensive to plain textual data, but, the encryption is expensive and complex to other data types such as images, videos, and audios due to large data size [6], [9].

The balance loading techniques are effective to reduce the volume of the binding data on the network, which minimizes the attacking opportunity in case of network traffic. However, this method is not effective when the attacker catches the transfer data because the data is transferred as it is the original form.

The offloading approach is effective to reduce the online processes of the data transfer, whereby the attackers' accessibility of the online data will be reduced. The main disadvantage of this approach is the need to own expansive network facilities in the organization in order to apply the offline mode of data transfer. Another disadvantage is that this approach is still needed the online mode of the data transfer.

The device's signature is a powerful approach to ban the unknown devices from the approach on the local network, whereby the paths of data transfer will be protected. However, this approach is not applicable in the case of a global network such as yahoo mail, Gmail, and online payment.

Steganography is strong security technique that applies for plain data of all types such as texts, audio, images, and videos. The main disadvantages of this approach are the processing cost as well as the expensive computation to

serve the security of data transfer. Another drawback is that the plain data is disguised as its original form, enabling attackers to extract the plain data and capture the embedded files in case of notification.

The chaotic map is effective to securely transfer data of various formats such as images, texts, and videos. The processes of the chaotic maps are simple and effective. However, the plain data can be resolved in case of handling the De-permutation and De-substitution keys by the attackers.

Consequently, the selection of the security technique depends on the nature of the data transfer. The encryption approach is suitable for textual data whatever the size of the transfer data. On the other hand, the chaotic map and steganography techniques are applicable for the data of various types such as texts, videos, audios, and images. Moreover, the device's signature would be deployed in the local networks for the data transfer of any size and format. Furthermore, the load balancing is a suitable technique that could support the security of large volume data through speed up the data transfer. Lastly, the offloading technique is suitable in organizations that have local network facilities for data transfer of any type and any size. A table 1 discusses the security methods and techniques along with its advantages and disadvantages.

In conclusion, the integration between the security techniques would offer effective protection for online data transfer. For example, data encryption can be integrated with other techniques such as offloading and load balancing. Also, the chaotic map can be integrated effectively with the steganography technique. The next section provides some recommendations based on the possible integration between the various security approaches.

TABLE 1. Summary of security techniques and methods for online transfer data

Source	**Security method or technique**	**Security Supporting**				**Advantages and Disadvantages**
		Data type	**Data Size**	**Cost**	**Processes Complexity**	
[9], [10]	Data encryption	Textual	Small	Not expensive	Simple	Simple processes. However, not applicable to multimedia
[18], [19], [20]	Load balancing	All types	Various sizes	Not expensive	Somehow Complex	Reduce the data binding on network. However, the data is not encrypted
[10], [21], [22]	Offloading data	All types	Various sizes	Not expensive	Simple	Reduce the online transfer processes. However, the data is not encrypted in online mode.
[23],[24]	Device signature	All types	Various sizes	Not expensive	Simple	Prevent the strange devices from accessing the network services. However, applicable for global network.
[25], [26], [27]	Steganography	All types	Various sizes	Not expensive	Simple	Difficulty of extract the plain data. However, the plain data is not encrypted.
[29],[30]	Chaotic Map	All types	Various sizes	Not expensive	Simple	Simple security processes. However, the attackers may know the De-permutation and De-substitution keys.

RECOMMENDATIONS

Based on the previous section, there are many recommendations that could be offered based on the integration between various security approaches that could be implementing to enhance the security effectiveness of online data transfer.

First of all, the encryption methods are an effective security approach to the textual data whatever, the volume of these data. The asymmetric encryption is the most useful technique for online data transfer due to the requirements of two different encryption and decryption keys. The decryption key is not transferred with the encrypted data, whereby it is difficult for the attackers to decrypt the transfer data.

Thus, the asymmetric encryption can be integrated effectively with other methods such as load balancing and chaotic maps to improve the security rank of transfer textual data. The transfer textual data based on the load balancing technique would be encrypted. On the other hand, the chaotic map can be applied to the textual plain data before encrypting this data.

Other integration can be conducted between the chaotic map and steganography techniques. This integration is recommended for the huge volume plain data of various types such as images, videos, audios, and texts. The chaotic map can be used to encode the plain data before hiding the chaotic data in embedding files. Thus, the attackers will find difficulty in detecting the embedded data and defuse the original map of the encoded data.

Furthermore, the chaotic map or steganography techniques can be integrated with the offloading data technique to secure the transfer data of any size and any type. The data would transfer without any security approach in case of offline mode. In case of online mode, the data transfer would be protected using security approaches such as a chaotic map or steganography. Additionally, the device's signature is applicable only to the local networks. Actually, this security approach does not need any integration with other security approaches. However, the encryption methods, chaotic map, or steganography can be conducted in the local transfer data in order to enhance the protection level of the transfer data.

The next section presents the conclusion and future works based on the presented evidences in this paper.

CONCLUSION AND FUTURE WORKS

This study discusses the security techniques that used to prevent the vulnerability of online data transfer. The security methods are compared according to specific indicators which are: data type, data size, cost , and processes complexity. Six security methods that are presented in this study; encrypted, load balancing, offloading data, device's signature, chaotic map, and steganography.

Based on the study discussions and comparisons, the following results are highlighted:

- The asymmetric encryption is effective in securing any size of text transfer data.
- The chaotic map and steganography approaches are applied to protect the transfer data of any size and any type.
- Devices signatures are an effective security approach to transfer data via local networks.
- The offloading and load balancing approaches are supported approaches to reduce the attacks on the transfer data via online gates.

This study presents many recommendations to improve the security level of the online data transfer according to data size and data type. The recommendations are based on the integration between the various security approaches to improve the security effectiveness of the online data transfer.

In the promising future, several studies would be conducted based on this study. The privacy approaches of the transfer data can be analyzed critically. On the other hand, the recommended integration between the security approaches can be elaborated and tested.

REFERENCES

1. J. Grabara, M. Man, and M. Kolcun, ILSHS **26**, 138 (2014).
2. W. Yaokumah and A.A. Dawson, 1 (2019).
3. G.L. Masala, P. Ruiu, and E. Grosso, 337 (2018).
4. S. Shakya, JAICN **01**, 45 (2019).
5. M. Arthur, in *International Conference on Computer, Information and Telecommunication Systems (CITS)* (IEEE, 2019), pp. 1–5.
6. H. Qiu, H. Noura, M. Qiu, Z. Ming, and G. Memmi, IEEE Trans. Cloud Comput. 1 (2019).

7. M. Liaqat, V. Chang, A. Gani, S.H.A. Hamid, M. Toseef, U. Shoaib, and R.L. Ali, Journal of Network and Computer Applications **77**, 87 (2017).
8. C.A. Lee, IEEE Cloud Comput. **3**, 42 (2016).
9. N. Alsaidi, M. Alshareef, A. Alsulami, M. Alsafri, and A. Aljahdali, IJCSIS **18**, (2020).
10. J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, J Supercomput **76**, 4041 (2020).
11. R. Meng, Z. Zhou, Q. Cui, X. Sun, and C. Yuan, **1**, 43 (2019).
12. M. Abdulwahed, S. Mustafa, and M. Rahim, in *9th International Conference on System Engineering and Technology (ICSET) (*IEEE, 2019), pp. 309–314.
13. Y. Luo, J. Yu, W. Lai, and L. Liu, Multimed Tools Appl **78**, 22023 (2019).
14. K. T and C. S, IJCNIS **10**, 60 (2018).
15. C. S, P. S, and S. G, in *International Conference on Electronics, Communication and Computational Engineering (ICECCE* (IEEE, 2014), pp. 83–93.
16. T. Azam, Cryptanalysis of the Encryption Scheme Based on Advanced Hill Cipher Algorithm, CAPITAL UNIVERSITY, n.d.
17. K.V. Pradeep, V. Vijayakumar, and V. Subramaniyaswamy, "Journal of Computer Networks and Communications ",**2019**, 1 (2019).
18. S. Aslam, S. ul Islam, A. Khan, M. Ahmed, A. Akhundzada, and M.K. Khan, "Journal of Network and Computer Applications" **100**, 80 (2017).
19. E. Jafarnejad Ghomi, A. Masoud Rahmani, and N. Nasih Qader, "Journal of Network and Computer Applications", **88**, 50 (2017).
20. A. Akbar Neghabi, N. Jafari Navimipour, M. Hosseinzadeh, and A. Rezaee, Int J Commun Syst **32**, e3875 (2019).
21. A. Bhattacharya and P. De, "Journal of Network and Computer Applications ",**78**, 97 (2017).
22. S.S. Keerthi, S.K. Shevade, C. Bhattacharyya, and K.R.K. Murthy, "Neural Computation", **13**, 637 (2001).
23. A. Singh and K. Chatterjee, "Journal of Network and Computer Applications", **79**, 88 (2017).
24. S. Khan, M. Shiraz, L. Boroumand, A. Gani, and M.K. Khan, "Journal of Network and Computer Applications ",**97**, 66 (2017).
25. M. Douglas, K. Bailey, M. Leeney, and K.. "Curran, Multimed Tools", Appl **77**, 17333 (2018).
26. M. Kaur, V. Kumar, and D. Singh, 65 (2020).
27. A. Sarkar, K. Solanki, and B.S. Manjunath, (2008)
28. V. Sedighi, R. Cogranne, and J. Fridrich, "IEEE Trans.Inform.Forensic Secur". **11**, 221 (2016).
29. C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "Multimed Tools Appl" **78**, 12027 (2019).
30. N. A. Al-Romema, A. S. Mashat, and I. AlBidewi, "COMPUTER **2"**, 77 (2012).