

Protect Text and Audio Files over the Internet

Mohanad J. Altalqani¹, Zahraa Jasim Jaber², Hawraa Ali Taher³

¹E-mail: mohanad.altalqani@uokufa.edu.iq, ²E-mail: zahraaj.altalakany@uokufa.edu.iq,

³E-mail: hawraa.alshimirty@uokufa.edu.iq

¹Department of Basic Science, College of Dentistry, Kufa University, Najaf, Iraq

²Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

³Department of Computer Science, Faculty of Education for Girls, University of Kufa, Najaf, Iraq

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: The science of information security has become a concern of many researchers, whose efforts are trying to come up with solutions and technologies that ensure the transfer of information in a more secure manner through the network, especially the Internet, without any penetration of that information. Due to the importance of digital data sent between the two parties through an insecure channel. As a result, there are many technologies and methods that are currently used in information security, including steganography and encryption. This paper proposes a safe method for text and audio files by encrypting them using the RC4 algorithm that relies on the chaos system. This system generates chaotic values that increase the randomness of the key and thus difficult to break. Then use the embedding technique in the color or grayscale images using the LSB sequential algorithm. I relied on hiding in the edges of the image, which were areas of strength where the change was not noticeable. The results showed a high ability to include data, as the PSNR scale reached more than 50, and the retrieved data was obtained without errors.

Keyword: Arabic Text, English Text, Audio steganography, LSB, Encryption Text, RC4, Edge Detection.

1. Introduction

Recently, due to advancements in technologies, most people choose to use the internet as the primary means of transferring data from one end to the other all over the world. Transferring data is easy, fast, and accurate using the net.

The "security threat" is one of the foremost problems related to the transmission of information over the net. Counseling must be secured so on transfer it, so information security has become very important and important factor to finish the transfer successfully without compromising it. Information security refers to protecting data from hackers or unauthorized users, and it provides high security to forestall data modification. There are various techniques used for this purpose like encryption and steganography (steganography and digital watermark) to spice up security measures in transmitting information over the net [1].

Information hiding techniques are classified into two sections: steganography and watermarking. Characteristics of the techniques comprise (a) imperceptibility, (b) survivability, (c) capacity, and (d) security. This paper focuses on Steganography, which could be a field within the domain of knowledge hiding that hides secret information in an undetectable way accepted the sender and intended recipients who have known it, making it the most candidate for hidden communication [2].

Steganography is a technique or method for hiding secret messages within a digital medium in order to suspend suspicions and suspicions that there is a secret communication to ensure that no one has knowledge of this communication other than the persons authorized to do so [3]. Image masking is one of the most advanced types in the science of concealment, because the environment provided by the nature of the image makes it more flexible in the process of hiding, as it has many and various characteristics that make the images an ideal medium for performing the processes of hiding. The image usually consists of a group of objects that increase the intensity of the color, which represents an edge that represents what represents the background. The regions that represent the edges have high color values, so their masking is not noticeable [4, 5].

2. Related Work

This section displays the works that have already been done on steganography utilizing distinctive systems. In 2020, Wang and et.al. Presented a hybrid method based on the replacement of the less significant bit (LSB) and HLAH. Since the sharp regions (edges of the image) in the images are not affected much by the changes, so it is preferred to hide them instead of the homogeneous areas. Therefore, he relied on including a large amount of confidential data in the edges of the image. As for the areas that do not have edges, a small part of the data was hidden. [6].

In 2020, Delmi and et.al. Presented steganography, the method is used Least Significant Bit Matching Revisited (LSBMR). Embedding region was on edge digital imagery to ensure the message was not detected in the image by visual. The method used to detect the edge region by using Canny Edge Detection [7].

In 2020, Prasad and Pal presented a simple method for embedding data within grayscale images. Rely on masking the edges of the image, which are strong areas of the image where changes are not noticed. Hide depends on a key (stego-key), and it determines which regions are embedding. [8].

In 2020, Ayub and Selwal presented an improved way to mask images as they were embedded in pixels that represent the edge of the image. These pixels have variable color density, thus ensuring security of confidential data. He used a set of spatial filters to reveal the edges of images, including Prewitt, Sobel, Laplacian and Canny. The masking method also adopted DCT, thus reducing the image size due to compression. [9].

3. Proposed Method

The proposed method includes three parts. The first part is to encode Arabic texts and English texts. The second part is to include the encrypted text within audio files without affecting the file. The third part consists in including the audio file in color or gray images in the least significant bits depending on a single sequence.

3.1 Encryption Texts

The encryption method based on the RC4 algorithm, which requires a key and clear text. To increase the power of the algorithm, the key generated using chaos systems. The chaos system characterized by high security. The security of chaos communication mainly comes from the complex dynamic behavior of the chaotic system, sensitivity to initial conditions, and the long-term unpredictability of dynamic behavior.

One type of messy system was used, which is Logistic Map. Logistic Map it is one of the simplest chaotic logistics maps used to generate chaotic signals. This map has been used in a number of applications including digital communications. Its properties have been studied extensively [10].

In order to approximate the logistic map one into a chaotic logistic map, the initial condition of x_0 in the interval must be $[-1, 1]$, and its equation is:

$$x_{n+1} = r * x_n * (1 - x_n) \quad (1)$$

Input: Texts Arabic or English

Output: Cipher Text

Begin:

1. Generate random numbers using logistic maps and with vector shape with a size of $1 * 256$.
2. Convert random values from the previous step whose value is between zero and positive one to integers between zero and 256 represent (Key).
3. Key generation based on integer values using the RC4 algorithm.
4. For i from 0 to 255

$S[i] = i$

End for

$j = 0$

for i from 0 to 255

$j = (j + S[i] + \text{key}[i \bmod \text{key length}]) \bmod 256$

swap values of $S[i]$ and $S[j]$

End for

$i := 0$

$j := 0$

while Generating Output:

$i = (i + 1) \bmod 256$

$j = (j + S[i]) \bmod 256$

swap values of $S[i]$ and $S[j]$

$K = S[(S[i] + S[j]) \bmod 256]$

output K

End while

5. Finally, Xor is done between the K output from the previous step and the plain text.

3.2 Embedding Text in Audio

This part includes the stego of the encryption text within an audio file in the LSB method. Only one bit is included so that there is no major change in the audio file.

Input: File Audio.
Output: Stego Audio.

Begin:

1. Record an audio file that contains the information to be sent.
 2. Converting the audio file into binary values.
 3. Converting the encrypted text into binary values.
 4. Embedding bits of the encryption text in the least significant bit of the binary values of the audio file.
 5. Converting the values after embedding into valid values and returning them as an audio file.
- End

3.3 Embedding stego Audio in image

This part includes embedding the audio file inside the image. This method relies on exposing the edges of the overlay image. The edges of the images are hidden due to the intensity of the contrast, as there is no significant change in them.

Input : Cover Image.
Output: Stego Image.

Begin

1. Read the cover image.
 2. Read stego audio file (message).
 3. Selection filter edge detection (Sobel, Prewitt, Kirch, and Canny).
 4. Edge edtection for three most significant bits of each pixel according to the specific filter type.
 5. Embedding bits of audio in pixels for the original image corresponds to the edge detection image.
- Step 6.** Apply the PSNR and MSE measure between the original image and the image after hiding to find the similarity between the two images:

$$MSE = \sum_{i=1}^M \sum_{j=1}^N (I(i, j) - C(i, j))^2 / M * N$$

$$PSNR = 10 \log_{10} (255^2 / MSE)$$

End

4. Result

This section deals with the results of the proposed method. This paper includes hiding Arabic texts and English texts and they have the same efficiency. Let it be encrypted "Hellow the World" or "كلمة من نم عاقل خبر من لنا".

1. The encoding of the English and Arabic text by the algorithm mentioned in the previous part is as follows:

Plain Text	Cipher Text
Hellow the World	ë-yÇÁbuõÑŠ Øž g
كلمة من نم عاقل خبر من لنا	«Fخ ُخ اذج قساو S ي ر ل و نة ك نة ق س ي ك ع ت»

We also note that the output of the encryption is very distinct due to the chaos system used. In the event that a hidden text is known, then the form of the text does not suggest any understandable sentence of the text, and this increases the work force.

2. The text is contained within audio file.

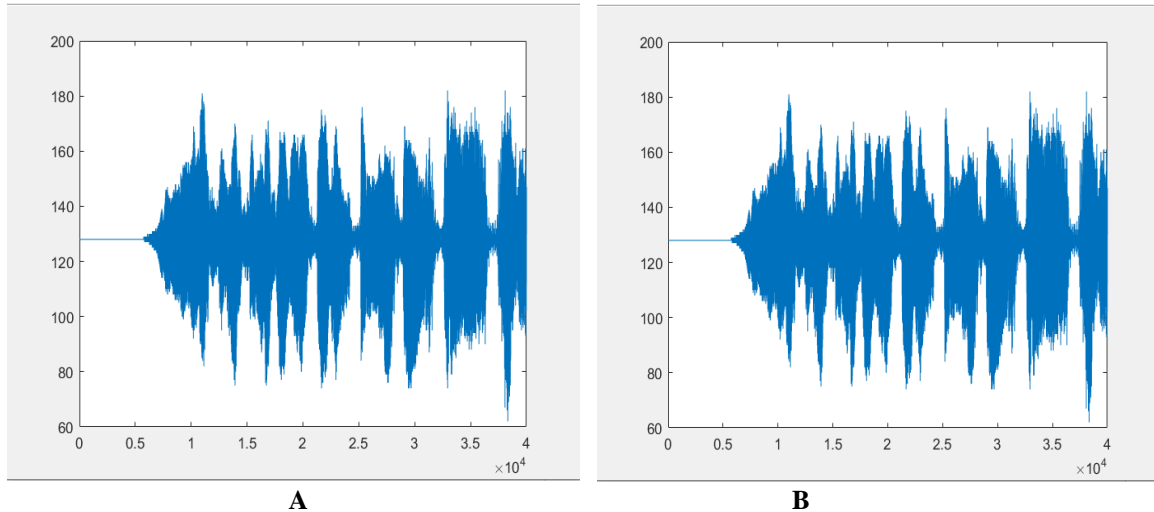


Fig. 1: (A) represented audio before stego (B) represented audio after stego.

We notice that although the encrypted text hidden in the audio file, there has been no very simple change. As this change was not noticed, the audio file itself was before and after hiding. This makes it easy to include text in an audio file and to send the audio file without unauthorized persons knowing the hidden text.

3. Hiding the audio file in the images, whether they are gray or color.









Cover Image	Filter Edge Detection	Edge Detection	PSNR
	Sobel		51.1670
	Canny		51.1670
	Prewitt		60.5620
	Krich		60.5620

Fig. 2: Explain the cover image, edge detection for three bit (most significant bit) and Psnr after stego.



Fig. 3: Stego image.

5. Conclusion

The proposed method is an effective way to maintain the security of the audio and text files sent over unsecured channels. Embedding the text in the least important bit of the audio file did not change the file, the audio information remained the same and this increases the efficiency of the work. The hiding of the audio file in the edges of the image makes it a very safe way to count changes in the image to the intensity of color values in those areas. The scale values were realistic and actual within the available range of previous works, but some of them exceeded despite the inclusion of two audio and text files. In addition, the hiding of color images is better than shooting images because they are more than a layer and more intense in color.

References

1. N. Koduri, "Information Security Through Image Steganography Using Least Significant Bit Algorithm," Master Thesis, Information Security And Computer Forensics University Of East London, 2011.
2. M Kavitha, Zaid Hamid Mahmoud, Kakarla Hari Kishore, Am Petrov, Aleksandr Lekomtsev, Pavel Iliushin, Angelina Olegovna Zekiy, Mohammad Salmani. Application Of Steinberg Model For Vibration Lifetime Evaluation Of Sn-Ag-Cu-Based Solder Joints In Power Semiconductors. Ieee Transactions On Components, Packaging And Manufacturing Technology. 2021; 11(3):444-450
3. Deepak Mathur, Dr. Prabhat Mathur "Edge Detection Techniques In Image Processing With Elaborative Approach Towards Canny" Computer Science Department, Lachoo Memorial College Of Science & Technology, 2016.
4. Dr. A. K. Saxena "Edge Detection Operators On Digital Image" , Srcem, Banmore(M.P.), India, 2013.
5. Abdulrahman Moffaq Alawad, Farah Diyana Abdul Rahman, Othman O. Khalifa, Norun Abdul Malek "Fuzzy Logic Based Edge Detection Method For Image Processing", Faculty Of Electrical And Computer Engineering, International Islamic University Malaysia, Malaysia, Department Of Electrical And Computer Engineering, International Islamic University Malaysia, Malaysia, 2018.
6. Wang, Y., Tang, M., & Wang, Z." High-Capacity Adaptive Steganography Based On Lsb And Hamming Code". Optik, 164685, 2020.
7. Delmi, A., Suryadi, S., & Satria, Y. "Digital Image Steganography By Using Edge Adaptive Based Chaos Cryptography". In Journal Of Physics: Conference Series (Vol. 1442, No. 1, P. 012041). Iop Publishing, January 2020.
8. Prasad, S., & Pal, A. K."Stego-Key-Based Image Steganography Scheme Using Edge Detector And Modulus Function". International Journal Of Computational Vision And Robotics, 10(3), 223-24, 2020.
9. Ayub, N, & Selwal, A."An Improved Image Steganography Technique Using Edge-Based Data Hiding In Dct Domain". Journal Of Interdisciplinary Mathematics, 23(2), 357-366, 2020.
10. Kehui Sun, "Chaotic Secure Communication: Principles And Technologies," Berlin Boston De Gruyter, 2016.