International Journal of Advances in Applied Sciences (IJAAS)
Vol. 11, No. 4, December 2022, pp. 312~323
ISSN: 2252-8814, DOI: 10.11591/ijaas.v11.i4.pp312-323

A new approach to hide texts into images and audio files using steganography and cryptography techniques

Miran Hikmat Mohammed
Department of Basic Science, University of Sulaimani, Sulaimaniyah, Iraq

Article Info

Article history:

Received Sep 6, 2022
Revised Oct 11, 2022
Accepted Nov 3, 2022

Keywords:

Audio processing
Cryptography
Image pixels
Steganography
Text encryption

ABSTRACT

These days there are many security issues facing users while they are using the internet for exchanging information among them. And, users use technology devices, such as mobiles and computers, and they connect them to the network and internet. Therefore, users always looking for a safe way to exchange information locally and globally, when they are connecting to a network. Also, these problems lead them to many further issues such as losing privacy, hacking, and detecting personal information. Although, many security techniques have been used to solve these issues by creating many different software utilities; some of them worked perfectly to some extent, while some others still did not comply with the security environment. This research paper finds a new methodology to secure text information while exchanging among permitted users over the internet. This method is a combination of cryptography and steganography with audio and imaging multimedia, which works on hiding and encrypting information before sending it over a network. As result, this technique will add additional security processes to the data exchange, and it will provide a more reliable environment for the user to connect to the network. In addition, the quality of the data will not be altered or noticed during the encryption and decryption process.

Corresponding Author:

Miran Hikmat Mohammed
Department of Basic Science, University of Sulaimani
Kurdistan, Sulaimaniyah, Iraq
Email: miran.mohammed@univsul.edu.iq

1. INTRODUCTION

Throughout the development of technologies, the security of electronic devices becomes an important aspect to provide a reliable environment for users to exchange data over a network either locally or globally [1]. For providing data protection, it is required to build a set of algorithms that refers to the method of shielding data from unwanted access. And, this can be done by using security techniques and algorithms such as data encryption, hashing, tokenization, and key management, which are data protection practices that secure secrecies across all devices and platforms [2], [3].

So, to secure sensitive data, companies and organizations all over the world invest extensively in information technology and cybersecurity capabilities. This is because they want to secure their sensitive information such as intellectual resources, consumer knowledge, and many other sensitive data, as they are saved in a database, and exchanged over the networks [4]. They also care about security on internet networking, and they use software such as antivirus, firewall, and much other utility software for providing guards to keep the data safe in their devices. Otherwise, the organizations' data are detectable and visible to all kinds of users, and those types of occurrence detection and response have three common elements: personnel, systems, and technologies [4], [5].

Also, the security of the network is not the only way to secure the data while they transmit among organizations or in the same organization. There is another important step which is the data itself that is needed to be encrypted and hidden by using steganography and cryptography techniques. This step will provide more reliability to data because they change its content and format into a shape that is understandable only by the permitted users who have the right access. Other users with no permission are unable to understand the content of the data, as they are encrypted and/or hidden in different media. So, there are two main terms in the world of security, which are steganography and cryptography [6], [7].

Steganography is the art and science of embedding hidden messages in a cover letter such that no one but the sender and intended recipient respondents to the message's presence [7]. Today's most frequent type of steganography is hiding files within other files such as image files on a computer. One of the main mechanisms that follow this structure is the least significant bits of the data, which encodes the color of each pixel of the image that is used to encode the hidden file. Changing the least significant bits alters the image's appearance only slightly, and the difference is undetectable to the naked sight, and this is a good point for providing a secure message before sending [8]. Whereas, if the changes are noticeable, the colors will appear slightly wrong, as if the image was captured with a low-resolution camera in low light. So, it is very essential to tune the algorithms correctly, because the human eyes and ears can distinguish various and comparable frequencies and colors [9]. Figure 1 shows the main idea of the steganography of image pixels.

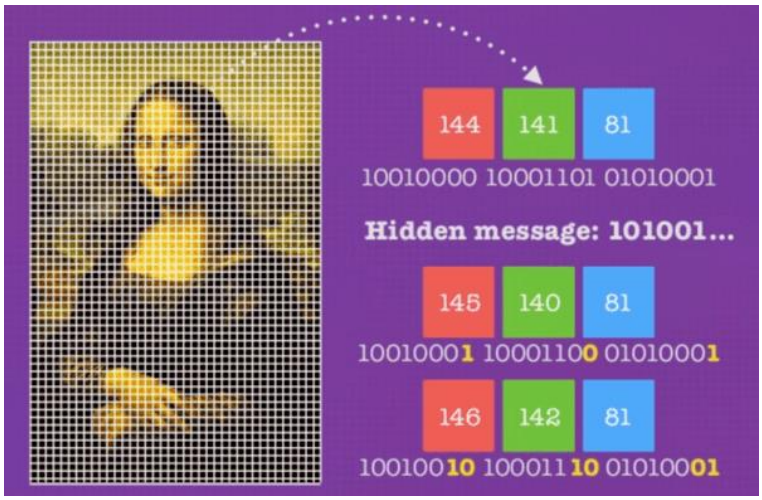


Figure 1. Steganography technique hiding text in image pixels [10]

On the other hand, cryptography is known as the science of securing texts from outside observers, and it is an encryption technique that takes the original statement (plaintext) and turns it into ciphertext, which is incomprehensible. For getting back the original text, the allowed users have the required key to decrypt the message and ensure that it can be read. Also, in cryptography, the strength of an encryption's unpredictability is investigated, making it more difficult for anyone outside the organization or the system to determine the algorithm's key or input [11].

Secret key cryptography, also known as symmetric cryptography, encrypts data with a single key. Symmetric cryptography uses the same key for both encryption and decryption, making it the simplest type of cryptography [12]. The cryptographic algorithm encrypts the data using the key in a cipher, and when the data has to be accessed again, only someone with the secret key may decrypt it. Secret key cryptography can be used on both in-transit and at-rest data, but it is more usually used on the latter because disclosing the secret to the message's recipient can lead to compromise [13]. Whereas, asymmetric cryptography, often known as public key cryptography, encrypts data using two keys. One key is used to encrypt the message, while the other decrypts it. In contrast to symmetric cryptography, if one key is used to encrypt, the message cannot be decrypted with the same key; instead, the other key must be utilized. One key is kept private and is referred to as the "private key", while the other is shared openly and can be used by anybody, thus the term "public key". The private key cannot be deduced from the public key due to the mathematical relationship between the keys, while the public key can be derived from the private one. The private key should not be shared and should only be kept by the owner [13], [14]. Figures 2 and 3 illustrate the process of encrypting text with a given secure key with symmetric and asymmetric encryption.

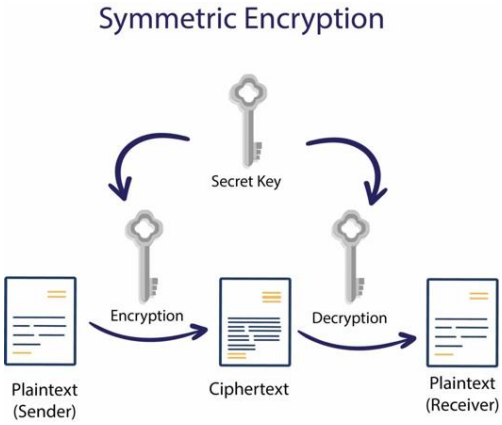


Figure 2. Encryption process using cryptography-symmetric encryption [14]

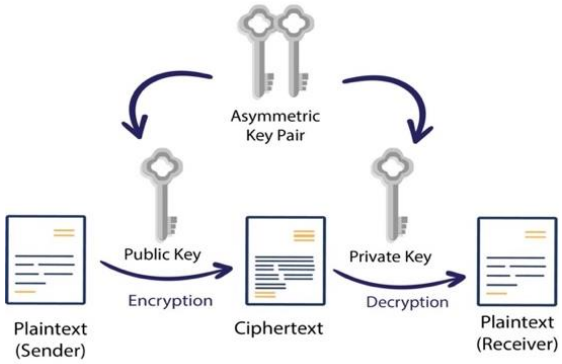


Figure 3. Encryption process using cryptography-asymmetric encryption [14]

While, cryptography converts data into cipher text, which is incomprehensible without a decryption key, steganography does not modify the data format; instead, it masks the message's presence. However, in cryptography, anyone who intercepted this encrypted letter would immediately notice that encryption had been used. On the other hand, when sending private documents, steganography is more discrete than cryptography, and it works on merging two different or same documents to the values of the pixel, frequency, and text value [15]. Also, steganography deals with binary numbers when trying to embed two different documents together, and it makes it harder for readers to reveal the original data [15], [16].

Moreover, data encryption and steganography techniques are considered two primary components used to secure data manipulation, each has its set of algorithms, ranging from different security levels, such as in-text encryption, triple data encryption standard (DES), rhythmic slow activity (RSA), and blowfish. Also, in steganography, there are many uses of multimedia for hiding data in images, sounds, and videos [17].

Also, data protection ensures digital data security when stored on operating system servers and distributed over the internet and other computer networks. Also, some new security algorithms replaced old versions, and these changes were essential for network and communications security. These algorithms maintain anonymity at the core of key security measures such as verification, integrity, and non-repudiation. Authentication guarantees that a message's origin is checked, while integrity ensures that its contents have not changed since it was sent. Non-repudiation often means that the author of a message cannot refuse to send it [17], [18].

This study aims to propose a new method of securing text messages before sending them over a network. The method is merging both techniques of cryptography and steganography by adding a secure algorithm for encrypting the text. The media used for this proposed security technique are images and audio. The other part of this research is designed as follows: section 2 is relative work, which presents the most recent work that has been in related idea and describes the method that follows. In section 3 the proposed

method in this research is discussed with the steps and the technique that are used. In section 4 the discussion of the result is demonstrated with all the steps and algorithms that are used in this research. Finally, in section 5 conclusion form the final idea and the result behind this research.

2. RELATED WORK

Many researchers have conducted research in this area with different methodologies, and some of them concentrate on one specific part which is either steganography or cryptography. On the other hand, some other researchers used both techniques, but they just used one level of cryptography or steganography, and this sort of security level is not enough, as it can be found easily by people. The authors of the paper [19], try to Combine cryptography and steganography, which has resulted in the creation of a new mechanism. The 2-dimensional haar discrete wavelet transform (2-D HDWT) was used on the cover image to extract its coefficient characteristics, and the advanced encryption standard (AES) method was applied to the secret images to encode them before hiding them in the cover image. Following the use of the 2-D HIDWT on the output of alpha blending, the alpha blending function was used to combine the cover image, the secret image, and the stegoimage. Because steganography and cryptography were combined, the proposed system provided more imperceptibility and dependability. Figures 4 and 5 demonstrate the main idea of the proposed method.

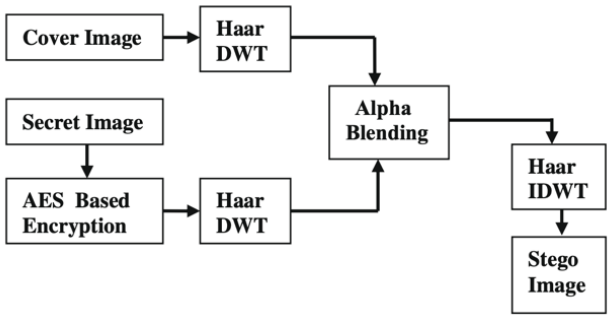


Figure 4. Hiding process for the proposed steganography techniques [19]

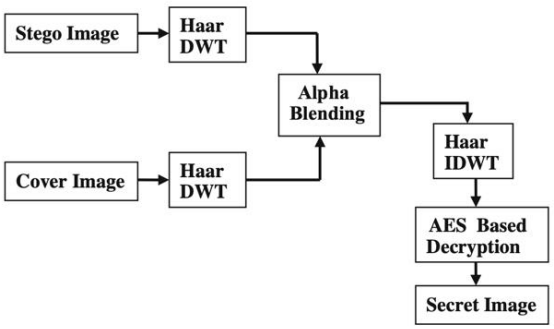


Figure 5. Revealing the process for the proposed method [19]

The proposed work paper [20] uses a technique to enhance the AES algorithm, which is used to encrypt plaintext, and it used the elliptical curve cryptography (ECC) algorithm, which is then used to encrypt the AES key. So, this will result in which can end in an overall increase in device protection through applying software-based countermeasures to avoid potential timing side-channel attack vulnerabilities. Also, a higher order of AES is used, with a key size of 192 bits and 12 rounds of iterations, as opposed to the basic AES model, which has 128 bits and ten rounds of iterations, to increase the reliability of data encryption, as it is shown in Figures 6 and 7. Although the researchers use a high level of encryption and encrypt the key as well, it would be better to hide the result encrypted message into a level of steganography, such as among image pixels, this will give a high level of security.

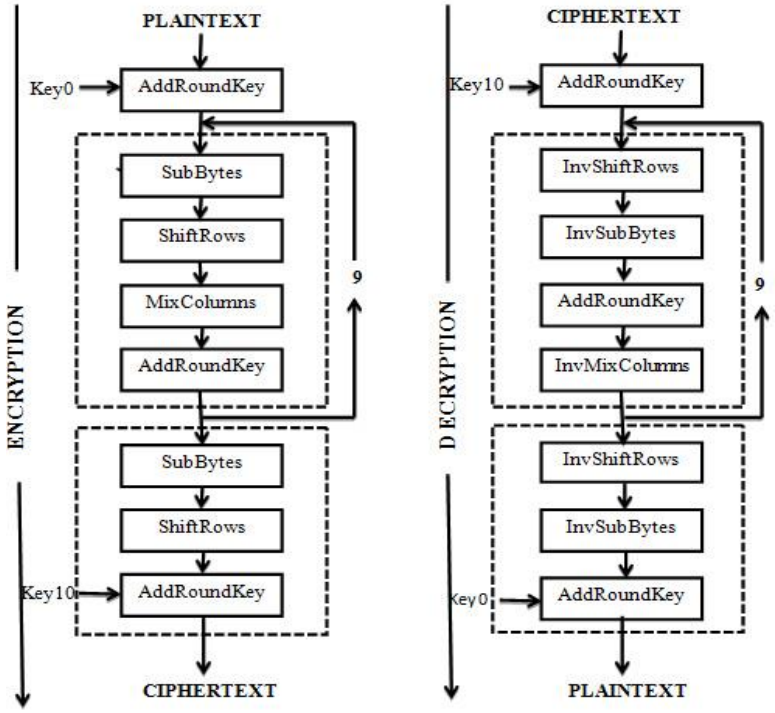


Figure 6. AES encryption and decryption process [20]

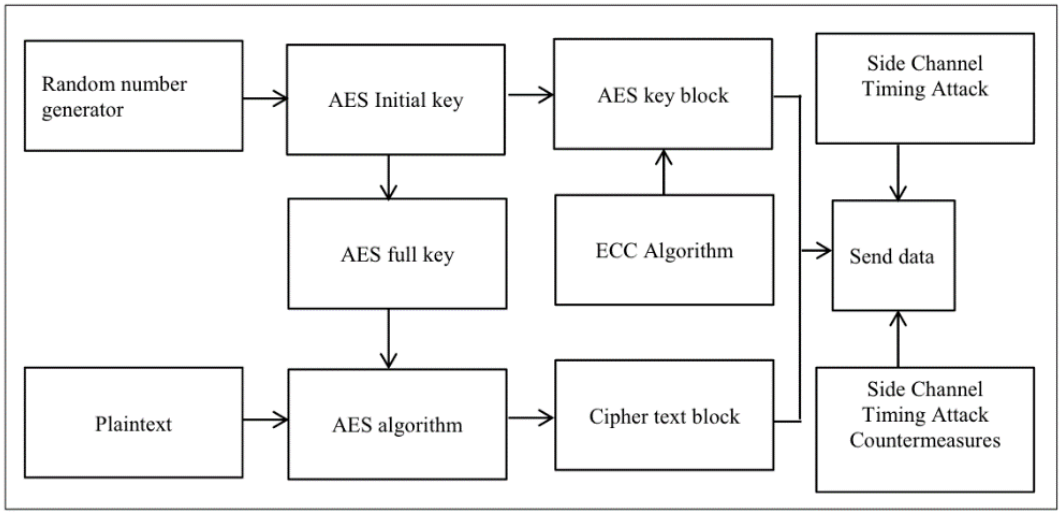


Figure 7. Hybrid algorithms of AES and ECC [20]

Saleh *et al*. [21] discuss the issues behind using cryptography and steganography that could be used to provide data security. Also, it discusses that each of these two techniques has got problems. For example, in cryptography, the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. On the other hand, though, in steganography, the problem is that once-hidden information is revealed or even suspected, the message has become known.

Thus, the author has merged the two techniques for data security which helps to improve the security of the information. In cryptography they used the AES algorithm has been modified and used to encrypt the secret message. Also, the encrypted message has been hidden using the method inside. Therefore, two levels of security have been provided using the proposed hybrid technique, and Figure 8 shows the

process of the proposed system. However, the author of this research depends only on one step of steganography, which is one image only, and it would be much more secure if there is another step of steganography either using another image or and hide the resulting image in the audio file.

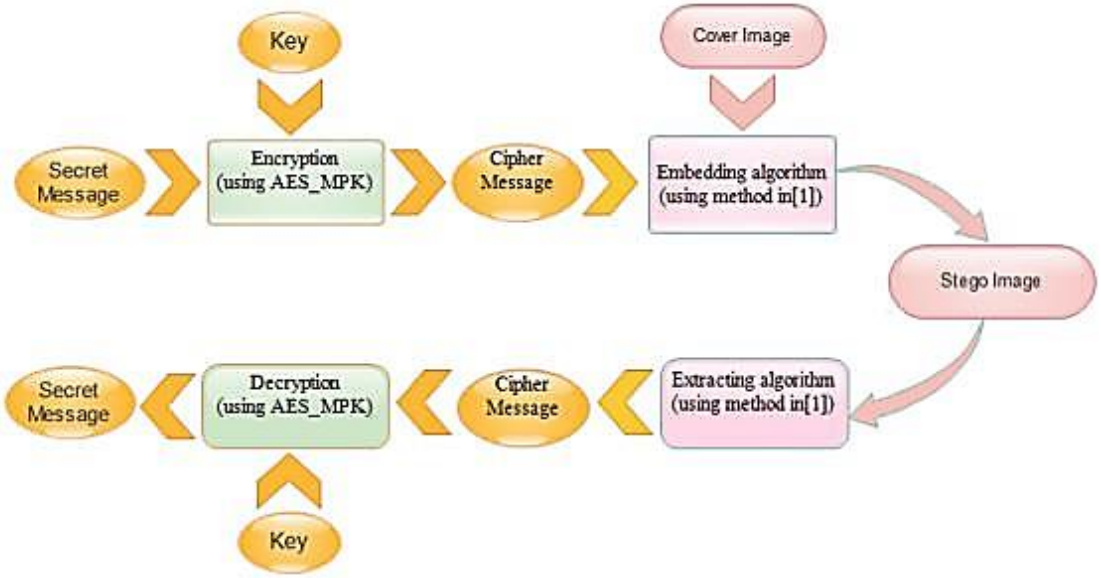


Figure 8. Block diagram of proposed system [21]

In the implemented work in the paper [22], AES and least significant bits (LSB) were combined in a novel way to guarantee a safe transfer of the data between the transmitter and the receiver. After performing a discrete cosine transform (DCT) on the image's pixels, the AES is used to encrypt the secret information in the carrier image's spatial domain, and the LSB is used to embed the secret information in the transform domain of the same image. By XORing the secret information's encoded bits with the carrier image's pixels, an additional security layer has been introduced to this work. The suggested system achieved a high peak signal to noise ratio (PSNR) of 62.72; as a result, it offered three information security levels and error-free decryption.

3. PROPOSED RESEARCH METHOD

The proposed work in this research paper is about the combination of the two terms of security techniques: cryptography and steganography. Cryptography is for encrypting the inserted text, while steganography hides the encrypted text in other media. Also, a new methodology is proposed to secure the text in both techniques, which is different from previous related works. Also, for this study, Python programming language is used which is one of the dominant software used today for many areas.

As the first step, which is the encryption process, a text will be inserted with any length of character numbers. Then these characters will be converted to other text variables, which is done by reversing the whole text. This technique has been done by using Python programming languages, which are used in all the steps of security techniques in cryptography and steganography.

After the text is reversed, another new methodology will come into account: converting each character to American standard code for information interchange (ASCII) code, then converting each code to a binary format. By considering the LSB algorithm technique, an additional step has been added: converting each first bit of the binary from 0 to 1 and vice-versa. This operation is done by mathematical calculation with adding and subtracting operations. Finally, in the same process, the binary output will be reserved again. So that, in this step, the inserted text has been encrypted, Figure 9 shows the process of cryptography.

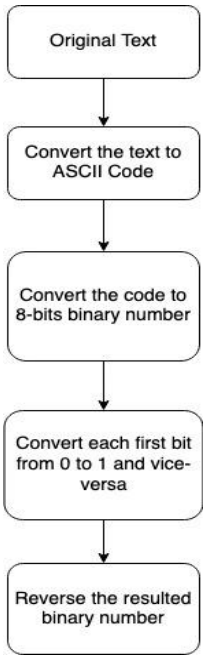


Figure 9. Cryptography process for securing the text

As the second step, another process of security level starts, which is hiding the binary output from the previous among red, green blue (RGB) image pixels. The image file has been generated using Python programming, and it has three-channel color features RGB. It is saved into the computer devices in the same path as the Python file. In this process, each color channel has 8 bits, which equals 24 bits in total. So that each bit of the binary text will be hidden in a pixel value at the first digit of each binary number of RGB, which means we need to convert the pixel values of images into binary as well. As the number of image pixels has many pixel values, and our image size is 150×150, it equals 22500, and that number is enough to store small message text as binary values. Although the image pixel values have been changed, however, the quality of the image is remaining the same in resolution and size. As the image is generated randomly and is not a famous image or known photo, Figure 10 shows the process of hiding the text value binary in the generated image.

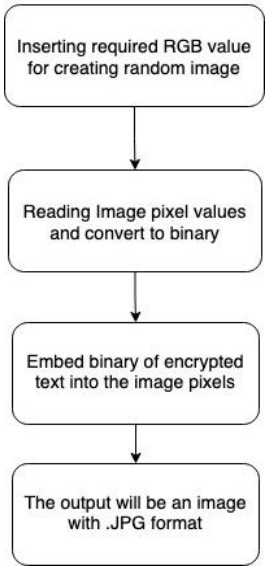


Figure 10. Embedding the encrypted text into an image

After that, a more complex step will start to provide a more secure environment for hidings techniques, and this is by hiding the newly generated image from the previous step that holds the encrypted message text into the audio file with the ".wav" file format. This file audio is generated with a random recorded voice text or any sound audio such as a beep. The primary process of hiding images inside the audio file is processed by reading the values of audio file data within the sample rate range, which keeps the audio high quality. Then, convert the data sound values, which are in numbers into binary format.

Later, the values of image pixels should also be converted to binary numbering format to hide the pixel values inside the audio file. This hiding technique has been done by calculating each 8-bits of each color channel together and inserting them into a single audio data 8-bits. This operation will loop until the complete image pixel is hidden in the audio file. There is an enormous range of some values in the audio file so that there will be enough space to store the image pixel values into the audio values. Later, as the final step, the audio file will be generated with text hidden inside the image and the image itself hidden inside the newly generated audio file, without changing the quality of the sound, Figure 11 shows the process of hiding image data in the sound file.

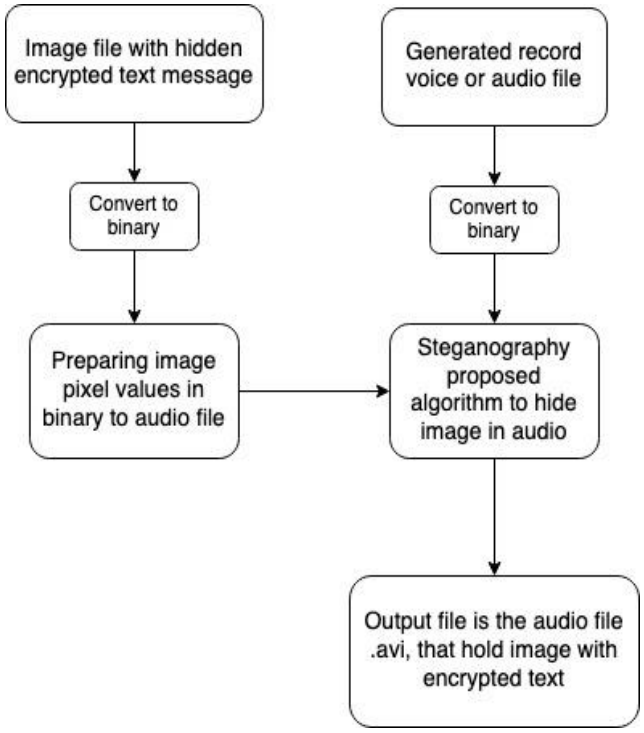


Figure 11. Embed generated image into the audio file

To get the encrypted text inside the image and audio file at the front end of the permitted user with a decoding algorithm, the decryption process starts. In this stage the process starts with getting back the image outside the audio file; this can be done by getting back the pixel values from those binary numbers in audio bits, especially in the range that the binary pixel values are saved. Then, separate the binary numbers for each channel RGB, and regenerate the image again. At the end of the looping process, we will get the image file.

The extraction of the text from the image is the last stage of the steganography process. The process starts by taking out the first bit of each pixel value in the image, accumulating all the extracted bits together, and then separating every 8-bits. After that, convert every 8-bits to a number, and from the resulting number, the original character is extracted according to the ASCII. Lastly, the combination of characters is set to the reverse order, in the final stage, the original text is shown. Figure 12 illustrates the stages of decryption and extracting the original text.

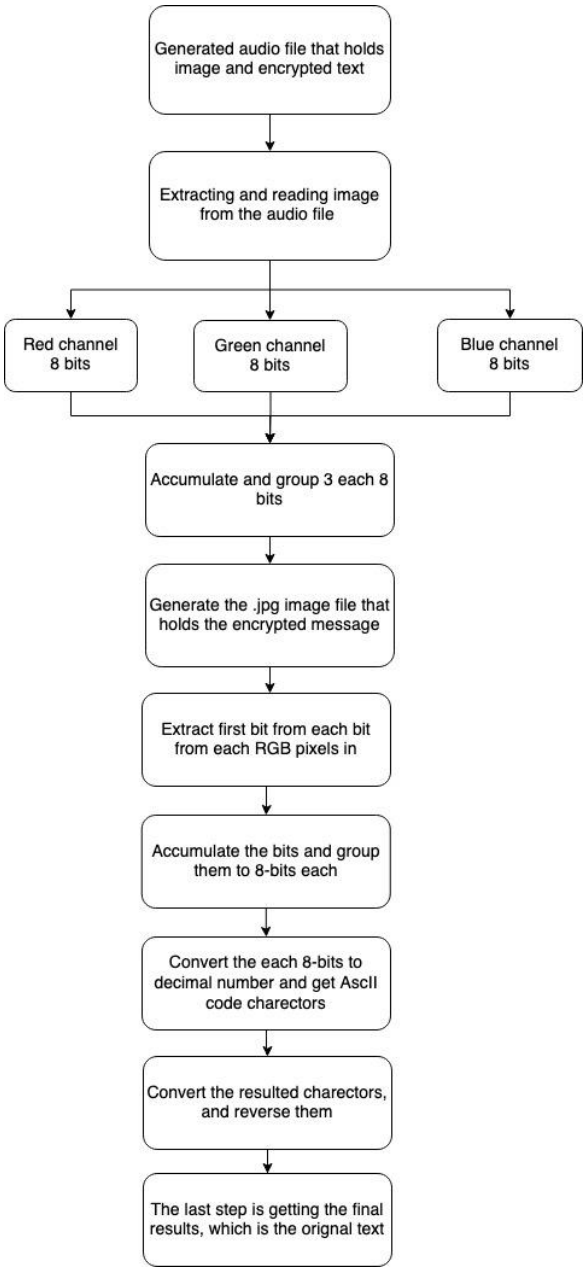


Figure 12. Description process for getting original text

4. RESULTS AND DISCUSSION

The results of this research show that, while encrypting the inserted texts into the proposed algorithm, provides a high level of security. The reason is that the texts are converted to binary after they are reversed in order. So, it is clear that text in the case of reversion is hard to read, even though the text is also converted to binary numbers. As a result, we have encrypted the text in high-security demands.

Also, it can be noticed that the image that wants to be used as a medium for the steganography process is generated randomly with three color channels which are RGB, and mixed colors from these RGB, as it is shown in Figure 13. Hence, the generated image is not understood or illustrious to anyone, it is just random colors of rectangles. So, it is good to use such random images as a medium to hold text, because unpermitted users will not be able to detect any kind of imagination that there is text hidden inside such images like this kind. As the image consists of three channels of color there are enough spaces to get a high opportunity to hide long texts.

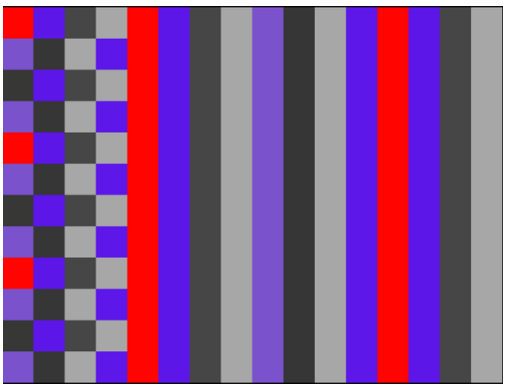
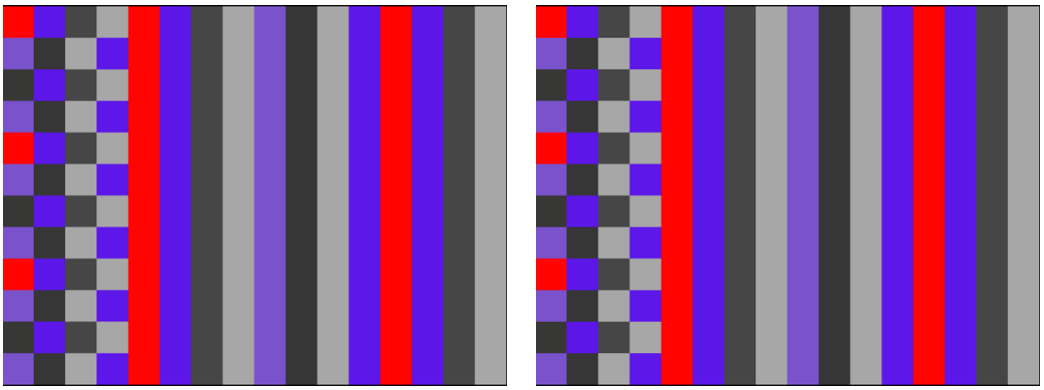


Figure 13. The generated random RGB image

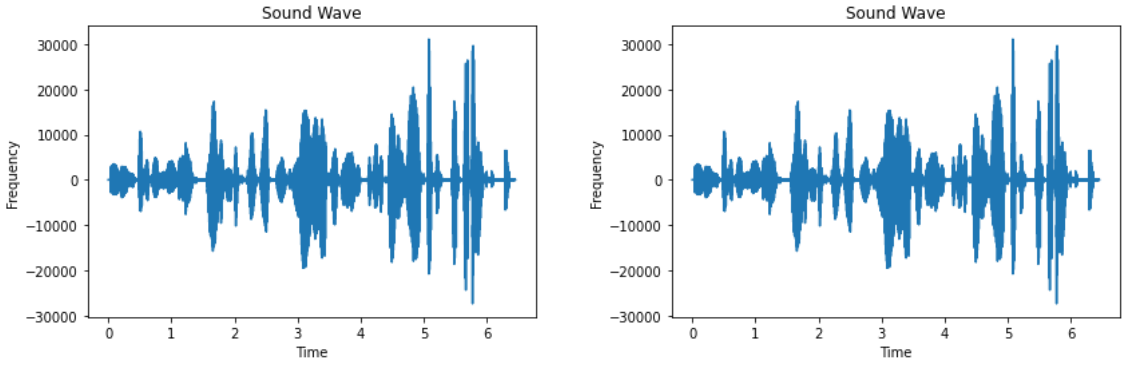
After the text is hidden inside the image among the pixel with three RGB channels, no changes are happening to the image. That means that the image quality remains the same without distortion or an increase in size with big changes. So, it gives a benefit for the proposed algorithm, which can hide text in the image with any changes that happen to the image quality, and ordinary people will not detect any changes and will not get the text. Figure 14 shows the comparison between the original and manipulated images, Figure 14(a) is showing the generated RGB image with text hidden inside the quality it does not change compared to the original image and Figure 14(b) is showing the original image.



(a) (b)

Figure 14. The comparison between the original and manipulated images, (a) the generated RGB image with text hidden inside the quality does not change compared to the original image and (b) the original image

After that, the image with the text inside goes to the next step which is inserting the image into the sound data with the respect to the frequency rate value. Also, the quality of the generated sound remains the same, there is not any kind of added noise or echo in the newly generated sound. The technique in this step is to find the spaces among the sound frequencies, then hide the data inside, which are bits of image pixel plus the text messages. As a result, the algorithm shows that the sound quality did not change or the size does not increase that much to be noticed, as it is shown in Figure 15. The generated sound with the image and text hidden inside the quality does not change compared to the original image shown in Figure 15(a) and Figure 15(b) shows the original sound.



(a) (b)

Figure 15. The sound quality: (a) the generated sound with image and text hidden inside the quality does not change compared to the original image and (b) is the original sound

However, the algorithm needs a key to decrypt the original text from the sound and the image data. So, the recipient needs to have key decryption for the whole process. And, the process is not easy because it goes into many steps of the decryption process and only the permitted users can get access to the text. So, by comparing the proposed algorithm to other previous works, it can be noticed that the proposed algorithm used more than two steps of security with a combination of steganography and cryptography techniques, and this is including the encryption of the text with a new approach. This is by converting text to a binary that makes the text unpredictable because the text in the generated binary has been reversed. Also, two levels of steganography medium have been used, which image and audio are processing. On the other hand, most of the works that had been done previously used only one step of the steganography or cryptography algorithm, and they are more about the traditional process.

5. CONCLUSION

It has been noticed that, with the increasing steps of security, the security of data exchange will increase. It is mainly because two categories of security techniques are used, cryptography and steganography. The cryptography steps helped to provide a secure text by reversing and converting the text into a more secure structure that is unreadable and undetectable y normal users. On the other hand, the steganography process is divided into two levels: hiding text in the image, then hiding the image with text inside an audio file. As the quality of both media does not change, so it is an excellent way to get a high-security level while trying to send text and data over the network, and it is one of the main requirements for nowadays users when they want to get contact and exchange text messages among each other with a high standard of security.

For future work, author plan to propose a new method for hiding text in short movie videos, by splitting the text into two parts. The first will be hidden among the video frames, while the other part will be hidden in the video sound. Also, author will add another technique to keep the quality of the video images and the sounds at the same level of excellence without changes. So, this will provide a high quality of securing messages over the network.

REFERENCES

[1] S. Zaman *et al.*, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *{IEEE} Access*, vol. 9, pp. 94668–94690, 2021, doi: 10.1109/access.2021.3089681.

[2] D. N. Akhtar, D. B. Kerim, D. Y. Perwej, D. A. Tiwari, and D. S. Praveen, "A Comprehensive Overview of Privacy and Data Security for Cloud Storage," *International Journal of Scientific Research in Science, Engineering and Technology*, pp. 113–152, Sep. 2021, doi: 10.32628/ijsrset21852.

[3] I. Torre, F. Koceva, O. R. Sanchez, and G. Adorni, "A framework for personal data protection in the {IoT}," in *2016 11th International Conference for Internet Technology and Secured Transactions ({ICITST})*, 2016, pp. 384–391, doi: 10.1109/icitst.2016.7856735.

[4] J. S. Rauthan and K. S. Vaisla, "Privacy and Security of User's Sensitive Data: A Viable Analysis," in *Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering*, 2017, pp. 61–71, doi: 10.15439/2017r45.

[5] R. Dastres and M. Soori, "A Review in Recent Development of Network Threats and Security Measures," *International Journal of Computer and Information Sciences*, vol. 115, no. 1, pp. 75–81, 2021.

[6] N. Jirwan, A. Singh, and S. Vijay, "Review and analysis of cryptography techniques," *International Journal of Scientific Research in Computer Science*, vol. 4, no. 3, pp. 1–6, 2013.
[7] S. Sandeep and A. Singh, "A Review on the Various Recent Steganography Techniques," *International Journal of Computer Science and Network*, vol. 2, no. 6, 2013.
[8] V. Sharma, "A New Approach to Hide Text in Images Using Steganography," *International Journal of Advanced Research in A New Approach to Hide Text in Images Using Steganography*, vol. 3, no. May 2013, pp. 701–708, 2017.
[9] R. Shanthakumari, S. Varadhaganapathy, S. Vinothkumar, and B. Bharaneeshwar, "Data hiding in Image steganography using Range Technique for secure communication," in *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies ({ICAECT})*, 2021, doi: 10.1109/icaect49130.2021.9392480.
[10] G. Kipper, *What is Steganography?* 2007, ISBN: 9781597491389, doi: 10.1016/B978-159749138-9/50016-8.
[11] J. Saturwar and D. N. Chaudhari, "Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking," in *2017 Second International Conference on Electrical, Computer and Communication Technologies ({ICECCT})*, 2017, doi: 10.1109/icecct.2017.8117849.
[12] E. R. Arboleda, C. E. R. Fenomeno, and J. Z. Jimenez, "{KED}-{AES} algorithm: combined key encryption decryption and advance encryption standard algorithm," *International Journal of Advances in Applied Sciences*, vol. 8, no. 1, p. 44, Mar. 2019, doi: 10.11591/ijaas.v8.i1.pp44-53.
[13] S. Sharma and Y. Gupta, "Study on Cryptography and Techniques," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT*, vol. 2, no. 1, pp. 249–252, 2017.
[14] Encryption Basics, "What is Cryptography in security? What are the different types of Cryptography?," *Encryptionconsulting.Com*, 2022.
[15] A. A. AL-Shaaby and T. Al Kharobi, "Cryptography and Steganography: New Approach," *Transactions on Networks and Communications*, vol. 5, no. 6, Dec. 2017, doi: 10.14738/tnc.56.3914.
[16] N. Francis, "Information Security using Cryptography and Steganography," *International Journal of Engineering Research and*, vol. 3, no. 28, pp. 1–5, 2015, doi: 10.17577/IJERTCONV3IS28029.
[17] J. G. Song and Y. Z. Chao, "Research about Authentication and Data Security Based on Media System," in *2010 International Conference on Multimedia Communications*, 2010, doi: 10.1109/mediacom.2010.34.
[18] M. Trnka, T. Cerny, and N. Stickney, "Survey of Authentication and Authorization for the Internet of Things," *Security and Communication Networks*, vol. 2018, pp. 1–17, Jun. 2018, doi: 10.1155/2018/4351603.
[19] V. K. Sharma and D. K. Srivastava, "Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard," in *Lecture Notes in Networks and Systems*, Springer Singapore, 2017, pp. 353–360, doi: 10.1007/978-981-10-3935-5_36.
[20] N. Mathur and R. Bansode, "{AES} Based Text Encryption Using 12 Rounds with Dynamic Key Selection," *Procedia Computer Science*, vol. 79, pp. 1036–1043, 2016, doi: 10.1016/j.procs.2016.03.131.
[21] E. Marwa, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, 2016, doi: 10.14569/ijacsa.2016.070651.
[22] A. Tauhid, M. Tasnim, S. A. Noor, N. Faruqui, and M. A. Yousuf, "A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform," *Journal of Information Security*, vol. 10, no. 03, pp. 117–129, 2019, doi: 10.4236/jis.2019.103007.

BIOGRAPHIES OF AUTHORS

Miran Hikmat Mohammed I am a Lecturer at the college of Dentistry at the University of SulaimIani in Iraq Kurdistan Region. And I am a well-educated and knowledgeable IT and Teaching professional with over eight years of experience within the educational and IT Industry working at the University of Sulaimaniyah and an MSc and BSc in Computer Science. Extensive experience gained in IT management, coordination, lecturing, and website maintenance and development. He can be contacted at email: miran.mohammed@univsul.edu.iq.