An Approach for Securing Voice Communication via Image Watermarking Technique

Miran Baban *miran.mohammed@univsul.edu.iq*
Basic Science Department
University of Sulaimani
Sulaimani, Iraq

Mahdi Younis *mahdi.younis@univsul.edu.iq*
Information Technology
University of Sulaimani
Sulaimani, Iraq

Abstract

Nowadays, Internet users use many social websites for communication with each other, and some of the users may live in another part of the world. Thus, communication becomes much easier and faster. However, with internet growing and their users, it becomes more likely to be attacked by hackers and intruders to access people personal data. Also, some professional hackers can detect the entire communication component for instance; text, image, video and voice messages.

In this paper, it is focused on one component, which is voice communication; and the main idea of this work is to hide the voice message that generated from one side and convert to a wave data, then to the binary code consequently on the receiver side. Later, the generated code will hide inside an image before reaching the destination. The final step is to reverse the whole security process that has been done in the source side. Therefore it can provide a safe environment for voice communication among the internet client.

Keywords: Watermarking, Binary, Voice, Hide, Image, Security, Communication, Stenography.

1. INTRODUCTION

These days the use of Internet technology has grown rapidly compared to its' early years, due to the purpose of exchanging data and information quickly by Internet users. Thus, to provide this opportunity, it requires a secure environment to hide sensitive data from one side and release the secret key on the receiver side [1] [2].

For instance, digital communication technology, such as internet technology faces different kinds of data security and privacy issues. The main reason for this issue is that illegal access to information without permission, and it requires security techniques to protect sensitive data. Cryptography, steganography and digital watermarking are examples of Security techniques that are used in internet security purposes [3] [4].

For securing data, there are various techniques in the form of digital contents, such as; text, image, audio, and video. Thus, digital watermarking is a method for embedding some secret information in the cover image which can later be decrypted for some different purposes like owner identification, authentication, content protection and copyright protection [5].

The impact of digital watermarking techniques is entirely based on the robustness of the inserted watermark against various types of attacks. Also, it is a method used to improve the ownership

over the image by replacing the low-level signal directly into the picture. Also, it is used for the tamper proofing and authentication [6].

The digital watermarking is commonly used for the security of the digital content and to protect the data from unpermitted users and provides the ownership right for the digital data. Another important characteristic of digital watermarking is imperceptibility and robustness against various types of attacks or standard image manipulation like filtering, scaling, rotation, cropping and compression [7].

The steganography is Greek words consist of two noun parts steganos (hidden) and graphos (writing). Also, it means a technique for protecting information in a cover media to avoid detecting sensitive information by intruders. Moreover, it is the main technique in the most securing data research area that most researchers discuss its importance and techniques for hiding sensitive information in cover media.

Media, such as text, image audio, and video steganography can be applied one on each other. So that; it can be done by using steganography techniques [8] [9]:

- Pure steganography can be implemented where there is not stego key. It depends on the guess of the party, who is not allowed to access the communication.
- Secret key steganography, this technique is the most vulnerable to be obtained by the third party, which is the person that is unauthorized to access the communication. The reason is that the secure key is provided in this technique.
- Public key steganography, this technique depends on providing a secure key that is used to secure the communication, the keys are public and private keys.

Moreover, steganography means to conceal a data of a particular multimedia file into another hypermedia, this is including hiding sound data into images. And, this will help the network to get a security environment along with communication and exchanging data among the network users. For example, security may require to send voice messages over LAN or WAN network [10] [11].

The voice is another digital media that is used in the most daily activities, and it does not require to have any tool to produced and listen to it. The source of voice comes from living beings as it is come from throat after pushing from a lung to the throat and then the vocals vibrate. Later the sound comes out and transfers through the air as a transmission medium. This transmission is done in a signal which is called the “spectrum of a generic speech signal” [12] [13].

So that, the voice is considered to be an example of signal processing, which is a new development among technologies that provide two types of waves, analogs, and digitals. Moreover, in all the digital technologies they have capabilities to do important conversion between two different medium and stages. From analog to digital, and it happens when the sound enter into the computer (from the source), while on the destination side the process will reverse, Digital to Analog [14] [15].

This study discusses securing audio into a cover image file using digital watermarking. Also, it is organized into seven main sections, Section 1 Introduction and background research, Section 2 Related work, Section 3 Research Methodologies, Section 4 Proposed Algorithm, Section 5 Implementation and Design, Section 6 Result and discussion and Section 7 research conclusion.

2. RELATED WORK

Yahya et al. (2015) stated their works with proposing a new algorithm for embedding two images to hide specific information in the cover image with watermarking technique. Moreover, this idea has been done with implementing the indication of the probabilistic neural network. In the following, the planning for their work is indicated step by step.

First, they are started with reading two image files, the first file as the cover image, and the second one as the watermarked image. After that, the first image is decomposed into wavelet coefficient blocks and the watermarked image converted to the binary blocks. The next step, they embedded the binary blocks into the wavelet coefficient blocks. After that, they got new values from embedding, after that step they used the result in PNN training step. Finally, they came out with extracting and testing the quality of the watermarked image [16].

Rinza et al. (2015) implemented an idea of cryptography which about securing a text message inside voice signals. Although; the authors indicated their idea in the abstract with hiding a piece of information from sound data into a cover image, the main work stated that to cover up a text message into voice signals with using LSB algorithm. The following is the step by step planning for their work.

They created a GUI by Matlab software to implement the security idea of hiding text data inside voice signal, and this by reading a voice file which is recorded or selected from any drive. Then a button name “hide text” is enabling and a text box is used for writing any text to hide in the voice file. When this button is pressed, the text will be hiding inside the voice file. Also in GUI form, there is another button which functions for ensuring that the process of embedding text in the voice has been embedded.

In addition, some researchers concentrate on the technique of securing text with different encryption mechanisms, such as RSA, AES ciphertext and other encryption and decryption methodologies. According to Zahraa (2016), show the technique of encrypting texts with using AES-2 Keys procedure, and show the steps of the process, which can provide a process of hiding the actual data from being noticed.

On the other hand, there are some studies showed that there are possibilities to hide text directly into the images, by putting the binary data from text into the pixels randomly or in some specific area on the images. For example, hiding text according to the pixel position such edges of the images and using the RGB mechanism, which can use to hide the text as a method of steganography [19] [20].

3. PROPOSED ALGORITHM

The main question that this paper may ask is “**How to encrypt and decrypt the sound data in a cover image?**” to Solve this question some steps and process has been taken while conducting research:

3.1 Encryption Steps

- The first step started with recording a particular sound with the wave file type (.wav).
- Then, read the recorded sound file and converted to wave data to get the binary code.
- Next step is to read any type of image files.
- After the process of getting the binary code and read a cover image by doing a particular technique, then and another step starts which is hiding the binary code into an image file
- Later, a new watermarked cover image will generate with hidden binary sound code inside.

3.2 Decryption Steps

- First of all, it is started with reading the watermarking image file.
- In the next step, it asks for taking out the binary code part from the cover image.
- Then, convert the binary data to the wave data.
- Finally, write the sound file

In this work, it is concentrated on hiding bits from one source into other sources, with using some mathematical operation. For example, to hide a sound data into a particular cover image with the different file type, it requires converting sound to wave data then to binary code. Therefore; the generated binary code embedded with cover image pixels. The following are the main mathematical calculation that performs the hiding action:

a. Sound Embedded Algorithm

Test image pixels value if less than 255 (<255) then:
Pixels value= pixels value + bits of sound file
Whereas, image pixels value is equal to 255 (==255) then:
Pixels value= pixels value - bits of the sound file

b. Sound Extraction Algorithm

Test watermarked a cover image with the original cover image to extract the binary code:
If watermarked cover image pixels value is equal to original cover image pixels value then:
The bit=0
If they are is not equal then:
The bit=1

After getting the binary code the next step is converting the binary code to wave data then convert it to sound file.

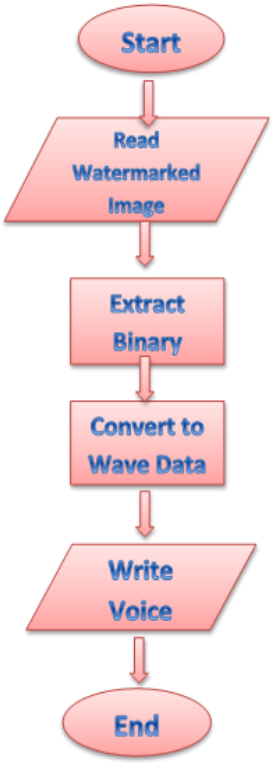


FIGURE 2: Decrypting Sound File.

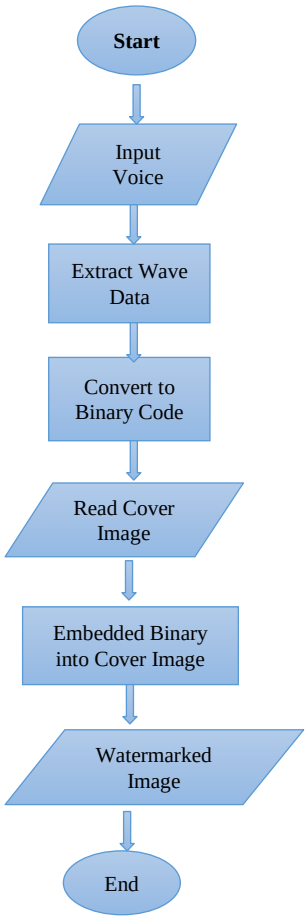


FIGURE 1: Encrypting Sound File.

4. IMPLEMENTATION AND DESIGN

This paper implemented its algorithms on Matlab software which is used for mathematical purposes. Thus, images data has organized in a 2D array, so it is proper to use this software to manipulate image pixels. Also, the same purpose is used for deploying sound data to work on its binary values.

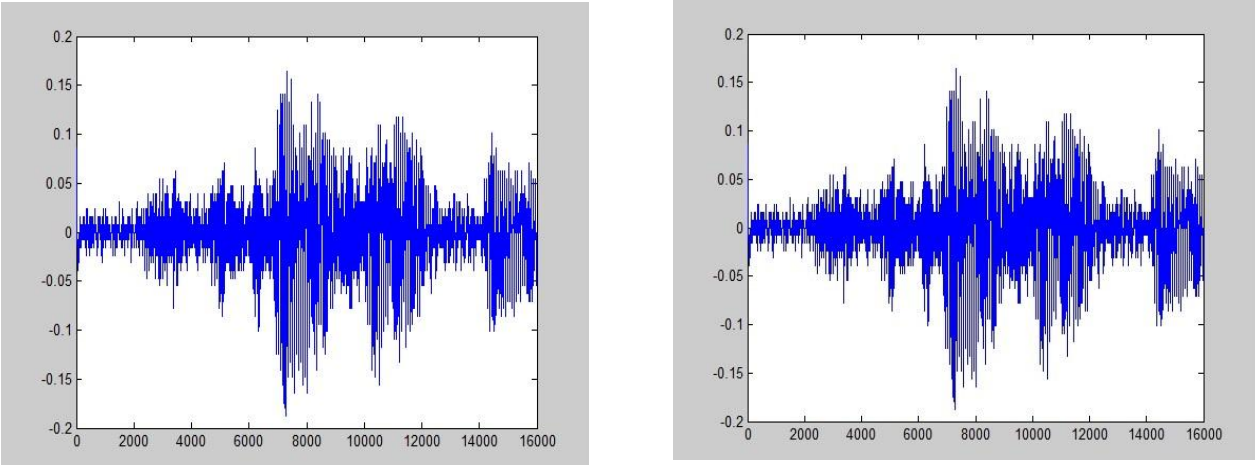
The main algorithm that is used in this paper is to hide sound information among image pixels and produced a watermarked image, then for the newly created image, another algorithm is proposed to extract the original sound data inside it.

5. RESULT AND DISCUSSION

The result of this paper is to get the same sound data as the original sound file. So that, it has been noticed that both sounds before and after implementing the two most important algorithms which are encryption and decryption with using the digital watermarking technique are unique.

In figure (1a) shows the plot of original sound data arranged on the X and Y axis which represent the sound values and the plot of this image are before implementing an encryption algorithm. While figure (1b) shows the same data of the sound that produced after applying decryption method from the image that digitally watermarked.

The final result from these two practicality foundations that is in both cases the sound data are the same in values and quality.



(a) Original Sound. (b) Sound that Produced.

FIGURE 3: (a) and (b) Shows Original and Produced Sound.

Moreover, the original image has been read first to be used for hiding sound data in their pixels values with using an encryption algorithm. Therefore; the original image becomes digitally watermarked. In figure (2a) shows the original image before the watermarking process, while figure (2b), shows the watermarked image with sound data. As a result of the two figures shows that there are not any noticeable changes in human visions.

Also, this proposed method can help to produce a better security environment, which works on securing both parts of digital data, which are sound and text at the same time. This is due to the mechanism of the method, which first converts the analog sound to digital (when entering to the computer), then the sound will convert to text, and the text will be encrypted and hide in the image specified image.

Moreover, it has been shown that this method response to the algorithm quickly, and can give the result as description quickly after that has been encrypted. Also, it is noticed from the figures the changes will not affect the quality of sound data and image pixel. So that, it can be said that this method has its advantages to be used as security for sending voice data over the networking.

However, there are different techniques have been found and used by researchers that show the ideas in the same field of study. Yet, they just concentrate on the encrypting the text with different security techniques, for example, cipher encryption, Modified AES-2 Keys and other hiding text techniques.

On the other hand, some other researcher used the technique of hiding text inside image pixels, for instance hiding the text on the edge of the images or among the pixels with RGB rate, but there is not such a technique that can be used to hide the sound data into image pixels, after converting the digital sound data to text and then putting them among the photo pixels.

(a) Original Image. (b) Image that Produced.

FIGURE 4: (a) and (b) Shows Original and Produced Image.

6. CONCLUSION

To sum up, this paper has proved that there are many ways to encrypt sensitive data over the network via a digital watermarking algorithm to provide a secure environment for communications. Thus, the main work in this paper is to provide a new proposed method to hide sound file into a specific cover image. The outcome of this process has shown that there are possible opportunities to arrange for getting security purposes and it has found that, there are not any signs of hiding data in the cover image. Besides the cover image, the quality and the data of the original sound file are the same as newly produced sound data that has been got from the cover image. As well as this similarity, while plotting the sound data by Matlab software shows the same plots.

7. FUTURE WORK

This research can be extended to included different kind of steganography methodologies techniques, for example hiding the required sound data in the edges of images by using Mathematics Matrix techniques without losing image data quality.

Also, from this research, it can be seen that the amount of sound data are encrypted into the specific image pixels. So that, the next research can be done by using different techniques, such as hiding the data into two separate image files as an encryption technique and fetching them from these two images as a decryption procedure.

8. REFERENCES

[1] Future of Internet technologies. Daniel Pavlić, Mile Pavlić, Vladan Jovanović. s.l. : IEEE, 2012.

[2] Internet technologies in depth. the technique of spam recognition based on header investigating. Adamov, Abzetdin. Azerbaijan, Baku: IEEE, 2011.

[3] Provided security measures of enabling technologies in Internet of Things (IoT): A survey. Minela Grabovica, Srđan Popić, Dražen Pezer, Vladimir Knežević. Serbia : Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016.

[4] The visions, technologies, applications and security issues of Internet of Things. Shen Guicheng, Liu Bingwu. s.l. : Institute of Electrical and Electronics Engineers (IEEE), 2011.

[5] Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Yahya AL-Nabhani, Hamid A. Jalab *, Ainuddin Wahid, Rafidah Md Noor. s.l. : Journal of King Saud University Computer and Information Sciences, 2015, Vol. 27.

[6] A Survey: Digital Image Watermarking Techniques. Preeti Parashar, Rajeev Kumar Singh. 6, s.l. : International Journal of Signal Processing, Image Processing, and Pattern Recognition, 2014, Vol. 7.

[7] A Survey of Digital Watermarking Techniques and its Applications. Lalit Kumar Saini, Vishal Shrivastava. 3, s.l. : International Journal of Computer Science Trends and Technology (IJCST), 2014, Vol. 2.

[8] A Study of Various Steganographic Techniques Used for Information Hiding. C.P.Sumathi, T.Santanam, G.Umamaheswari. 6, s.l. : International Journal of Computer Science & Engineering Survey (IJCSES), 2013, Vol. 4.

[9] Steganography Techniques-A Review Paper. Jaslen Kour, Deepankar Verma. 5, s.l. : International Journal of Emerging Research in Management and Technology, 2014, Vol. 3.

[10] Meng, P., Hang, L., Yang, W., Chen, Z. and Zheng, H. (2009). Linguistic Steganography Detection Algorithm Using Statistical Language Model. 2009 International Conference on Information Technology and Computer Science.

[11] Zhi-Hui Wang, The Duc Kieu, Chin-Chen Chang and Ming-Chu Li (2009). Emoticon-based text steganography in chat. 2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA).

[12] Increasing the hiding capacity of low-bit encoding audio steganography using a novel embedding technique. Olanrewaju R.F., Khalifa O., Rahman H.A. s.l. : World Applied Sciences Journal 21, 2013.

[13] Hanai, S. and Suzuki, M. (2013). SOUND PROCESSING APPARATUS, SOUND PROCESSING METHOD, AND SOUND PROCESSING PROGRAM. The Journal of the Acoustical Society of America, 134(5), p.3962.

[14] HIGH-SPEED DIGITAL SIGNAL PROCESSING ELECTRONICS FOR THE TLS LONGITUDINAL FEEDBACK SYSTEM. M. S. Yeh, K. T. Hsu, C. H. Kuo, W. K. Lau, J. F. Lee, H. J. Tsai, SRRC, Hsinchu. New York: IEEE, 1999.

[15] Boontawan, R., Tooprakai, S., Dejhan, K. and Yimman, S. (2016). Algorithmic Scheme-Integrated Bandwidth Compensatory Reconstruction Filter of Digital Signal Processing System. Journal of Signal Processing, 20(3), pp.91-103.

[16] Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. AL-Nabhani, Yahya, et al., et al. 4, Saudia Arabia: Journal of King Saud University, 2015, Vol. 27.

[17] Security System for Sending Information Containing Hidden Voice Data by Steganography (SIOVE) Using Matlab. Rinza, Bárbara Emma Sánchez, Salgado*, María del Rocío Guadalupe Morales and Olguín, Cristian Omar Cortez. 1, Bárbara Emma Sánchez Rinza, María del Rocío Guadalupe Morales Salgado*, Cristian Omar Cortez Olguín Faculty of Computer Science, Benemérita Universidad Autónoma de Puebla, Universidad Popular Autónoma del Estado de Puebla Puebla, Puebla : International Journal of Engineering and Innovative Technology (IJEIT), 2015, Vol. 5.

[18] K., Z. (2016). Text Encryption using Modified AES-2 Keys. International Journal of Computer Applications, 149(4), pp.27-31.

[19] Rawat, D. and Bhandari, V. (2013). Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method. International Journal of Computer Applications, 67(1), pp.22-25.

[20] Hussein. Rustom, N. (2017). A Review in Using Steganography Applications in Hiding Text Inside Digital Image (BMP). International Journal of Advanced Research in Computer Science and Software Engineering, 7(1), pp.36-41.