Research Article

Combining RSA and audio steganography on personal computers for enhancing security

Nouf Al-Juaid[1] · Adnan Gutub[2]

Abstract

This paper proposed an enhanced system for securing sensitive text data on personal computer benefitting from the combination of both techniques: cryptography and steganography. The system security is generated by involving RSA cryptography followed by audio-based steganography as two sequential layers to ensure the best possible security gaining the advantages from both. The study modeled the system and implemented it to be tested to explore the relation between security, capacity, and data dependency. The experimentations covered securing data within 15 differently sized audios showing interesting results. The results gave enhancement in capacity versus security trade-off, allowing the user and application to be the decision maker in the choice. The work showed the possibility of accepting security of 1-LSB, 2-LSB, and 3-LSB methods and their reasonable effect on the cover. The study also shows that using 3-LSB is giving acceptable security benefitting extra capacity more than 1-LSB and 2-LSB found in the literature.

Keywords Audio steganography · Hiding text on PC · RSA cryptography · Security for personal computer

1 Introduction

Usually, we need to secure sensitive data that we store on personal computers such as e-mail messages, credit card information, and corporate data. Concealing sensitive secret data within individual computers have the benefit of using the available files on the computer to perform as the cover media [1]. In order to provide confidence and safety to the user to protect his information on a PC, we can combine cryptography and steganography techniques for hiding sensitive data. The security obtained using steganography to conceal sensitive data inside a cover media depends on the belief that no one can suspect that there are any data hidden. However, if anyone notices that there is a change in the cover media, the sensitive data can be discovered. Therefore, it is better to use another technique such as cryptography to encrypt the sensitive data before hiding it in the cover media. That will ensure that even if the embedded text is discovered, no one can know its content because it is encrypted. Therefore, for higher security, we can take advantage of combining the two techniques to ensure that even for the very difficult security breakthrough the secret data remain unharmed or not used in a bad manner. We in this paper proposed a resilient security system utilizing audio-based steganography depending on the use of obtainable files from PC, in addition RSA cryptography as assurance layer. The system hiding techniques involve cryptography and steganography as two layers to insure full protection of the sensitive information on a PC. Steganography [2], in general, is the science of concealing information through a certain process in another medium type, i.e., text, image, audio, and audios. After combining the secret within the cover object, the result file is known as stego-file.

Cryptography, as the second layer on this security system, is different completely than steganography. Cryptography is known as encoding the secret clear text into ciphertext. Cryptography requires a secret key for the

✉ Adnan Gutub, aagutub@uqu.edu.sa | [1]Computer Science Department, Taif University, Taif, Saudi Arabia. [2]Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia.

SN Applied Sciences (2019) 1:830 | https://doi.org/10.1007/s42452-019-0875-8

Received: 21 March 2019 / Accepted: 2 July 2019 / Published online: 4 July 2019

encoding/decoding process to secure the secret data. In our system, the secret text data going through the crypto layer involving a security key, is followed by the steganography layer to produce the file containing the secret encrypted data that i known as the stego-audio file. Figure 1 shows an overview of the two-layer security system.

In this paper, we suggested and performed the flexible system using two techniques in two layers, i.e., cryptography and steganography, to gain the advantage from them and provide the best security for PC applications. The first layer, cryptography is using RSA crypto method, and the second layer, steganography depends on the audio-based steganography concealing the encrypted data in the least significant bit (LSB). In a way to improve the capacity, we suggested increasing the LSBs [3]. The key improvement in this study compared to other similar work is the ability to utilize some of the available audio PC files, assumed undetectable media, to conceal secret data for personal usages [4]. This work is innovatively benefitting from the human hearing sense in security applications, which is usually unutilized. We prove that it can be acceptable similar to the other security applications or may be better, which is completely different the normal visual security studies. Furthermore, our work technical computation recommended further utilizing 3-LSB in hiding data in order to increase capacity preserving the quality of the audio file after the embedding [5]. To be more specific, we studied the previous literature using AES symmetric key crypto algorithm to encrypt data [6] fully adjusting the work to utilize RSA public key crypto algorithm highlighting its benefits that will be elaborated later.

The paper is organized as follows. The next section, Sect. 2, covers literature review introducing the related research that has used the crypto-stego system utilizing audio steganography with cryptography for securing data on PC. Section 3 presents the details of the proposed method for securing data in PCs, followed by implementation of the proposed method in Sect. 4. Section 5 discusses in more detail the relationship between the system security priority and data dependency depending on the benefit of this flexible security system on 15 different audios that produced interesting comparison results. Section 6 concludes the paper with summary of the work and shows some ideas for possible future research work.

2 Literature review

This section is concerned with research papers that propose methods for securing secret text using cryptography and audio steganography. Deshmukh et al. [5] proposed an efficient system for hiding data in an audio file with two layers of security. In the first layer, the data are encrypted with a cryptographic algorithm. In the second layer, a modified LSB algorithm is used to hide the secret text inside an audio file. The advantage of the proposed system is that sound variations in the audio file cannot be detected because the data are hidden in LSBs and hence the sound quality is retained. In addition, the size of the file is fixed, even after hiding. In contrast, Asad et al. [6] suggested an enhanced version of the conventional LSB modification technique in audio files. This improvement requires two steps. Firstly, to embed a secret message, the bit number of the cover message should be random. Secondly, the sample number that contains the next secret message bit is chosen at random. Asad et al. [6] used 256-bit AES to encrypt the text before concealing it inside the audio file in case the message is revealed. Shaikh et al. [7] proposed a method to secure data. Firstly, the secret data are encrypted using an RSA algorithm, and then multiple LSBs are used to embed the data in audio samples. In this method, the most significant bits (MSBs) of the sample are used to determine which LSBs are used to conceal the secret text. The advantages of this work are that it provides more capacity and is more secure for hiding text than standard LSB while creating no noticeable sound distortion. The properties of the audio file do not change after concealing

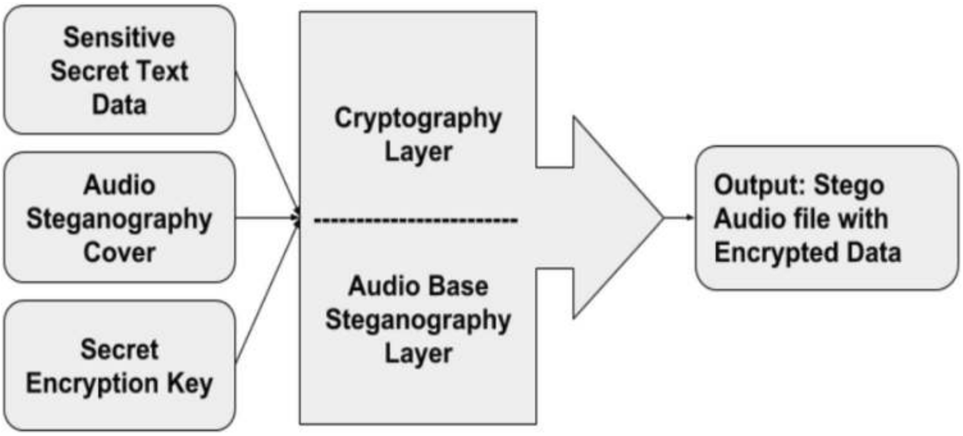

Sensitive Secret Text Data
Audio Steganography Cover
Secret Encryption Key
Cryptography Layer
Audio Base Steganography Layer
Output: Stego Audio file with Encrypted Data

Fig. 1 Overview of the 2-layer security system

the secret message. A new approach that protects data utilizing cryptography and audio steganography is presented by Saurabh et al. [8]. They suggested keeping secret message bits as showing randomness unrecognized insertion into the audio data that guarantees safely reaching data from the unwanted desired side. This method works by using two layers. In the security layer, R-Prime RSA is used to encrypt the message in order to enhance the RSA encryption algorithm. The next layer uses a genetic algorithm (GA), which inserts the message into the audio based on the LSB algorithm with random layers. Saurabh et al. [8] used random layers to increase robustness in order to ensure that an attacker cannot discover the hidden information; even if the attacker knew about the secret message, it would be difficult to extract. Thus, a higher capacity and robustness are achieved without distortion of the audio file. Similarly, Padmashree et al. [9] presented a system that uses steganography and cryptography for audio. This system uses an RSA algorithm to encrypt the public key of the text file that is embedded in an audio file. In the steganography process, the LSB is used to insert the cipher text into the fourth and fifth LSBs. The results show that the hidden data do not change the quality or size of the audio file. An efficient approach for hiding data is presented by Ravali et al. [10]. They proposed a system based on audio steganography and cryptography to conceal a data file in two stages. The first stage involves the use of a Blowfish algorithm to encrypt the data file before it is hidden in the audio file. The second stage involves applying a spread spectrum steganography technique to conceal the data file inside the audio file. The advantage of this method is that the size of the file does not change for any audio format even after the message is embedded. It also provides greater protection of data from attackers and is suitable for any size of data files. Abikoye et al. [11] produced a system utilizing cryptography and steganography techniques to provide an efficient method of protecting data from an intruder. This system uses the LSB to encode the message inside the audio file. In addition to enhancing the security of the data, Abikoye et al. [11] used the data encryption standard (DES) algorithm to encrypt the data before concealing them. The advantage of this work is that it keeps the size of the audio file same even after the data are embedded. Furthermore, this method is suitable for all audio formats. In this work, we studied the proposal to combine the two techniques of cryptography and steganography. We are using RSA algorithm in the first layer and audio-based steganography in the second one. We suggested concealing the data in the 3 lower bits (3 LSBs) in the audio file to increase the capacity of hidden data preserving the security robustness against the attacker. The research proved keeping the audio file acceptable such that no distortion can be recognized nor heard via users; this assures promising research direction to be open for innovations.

3 Flexible system modeling and security priority

To ensure high security convenient for individual computers applications, advancing from the different techniques presented in the second section above, our suggested system using both cryptography and steganography as two separate layers to give the best security.

The flexible system can be shown as a group of operations flow graph (Fig. 2) clarifying the two processes of hiding and retrieving the secret text data. The crypto layer is using RSA crypto algorithm and is a public cryptographic system that depends on two keys: one for encryption and the other for decryption. The reason for choosing this cryptography algorithm among other crypto schemes is that it is still considered safe and secure using required mathematics to prove its effectiveness [12]. RSA is still attractive and hard to crack involving the problem of factorization of prime numbers [13].

The RSA algorithm solves the problem of key management and key distribution by using two keys, i.e., public and private keys [14]. Assume that there are two people who want to participate in a private conversation without it being read by a third party. The first one who sends the message creates a key based on two large prime numbers p and q as follows. First, let p and q be two different large random primes. The product of these large primes is denoted as n, i.e., $n = pq$. Because of the primality of p and q, the Euler function of n can be computed as the product of the Euler functions of p and q:

$$\varphi(n) \ = \varphi(p)\,\varphi(q) = (P-1)(q-1) \tag{1}$$

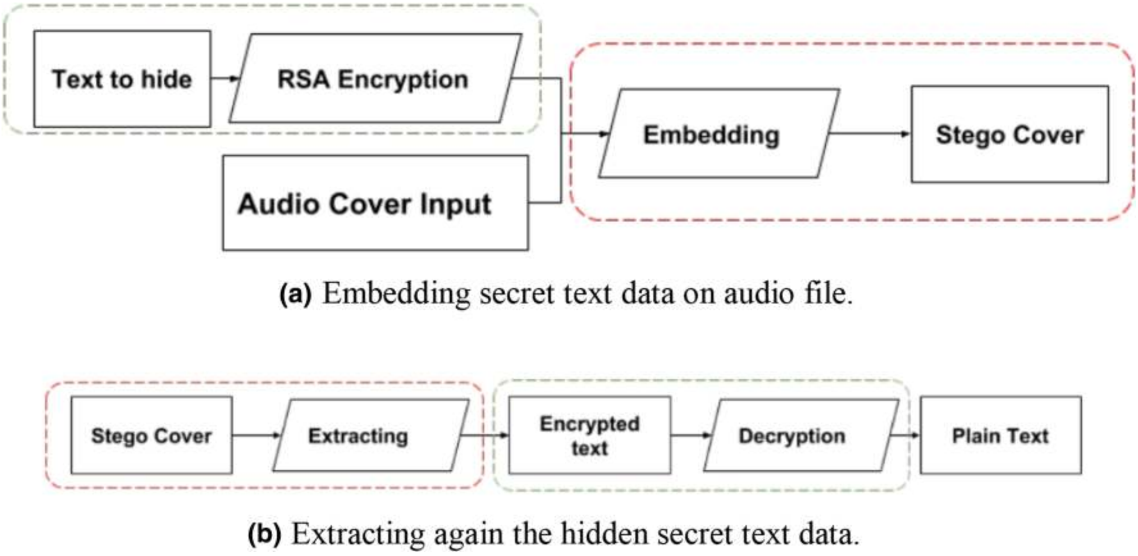
The parameter n is called the modulus of the system. For example, when Alice wants to generate her key pairs (k_e, a and k_d, a), she chooses a large random number $1 < e < \varphi(n)$ that is a relative prime to $\varphi\ (n)$, i.e., gcd $(e, \varphi(n)) = 1$. She then computes the number d as the multiplicative inverse of e modulo $\varphi(n)$, i.e., d satisfies the congruence

$$ed \equiv 1 \bmod \varphi(n) \tag{2}$$

The public key of Alice $\left(k_eA\right)$ is the pair (en), and thus, e is referred to as the encryption exponent. Her private key is $\left(k_d, A\right) = d$, where d is referred to as the decryption exponent. If Bob wants to send an encrypted message to Alice using RSA encryption, he uses her public key $\left(k_eA\right) = (en)$. To encrypt, he raises the plain text m to the power e and reduces modulo n:

$$c = m^e \bmod n \tag{3}$$

Alice decrypts the text with her private key $\left(k_dA\right) = d$ by raising the cipher text c to the power d and reducing modulo $n\ :\ m = c^d$mod$n$. RSA can be understood in more



(a) Embedding secret text data on audio file.

(b) Extracting again the hidden secret text data.

Fig. 2 Process flow graph of the proposed flexible security system

depth in many resources such as [12]. The flowchart of the RSA encryption and decryption is shown in Fig. 4.

In our system, the steganography layer is depending on the audio-based steganography as in concealing the encrypted data resulting from the cryptography layer. In fact, we have increased the hidden bits in the audio using several least significant bits (LSBs) instead of one bit to improve the system capacity, as will be shown in the next section, which is a different improvement to the 3-layer work presented in [15].

In audio files (WAV), after selecting the cover and converting it to binary, each sample in the audio file contains 16 bits, as shown in Fig. 3.

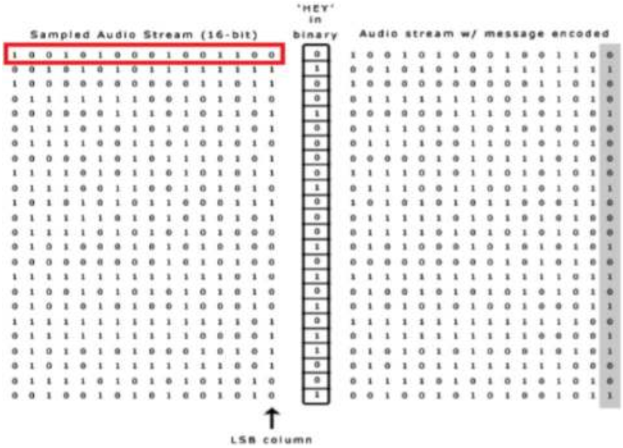

Sampled Audio Stream (16-bit)
'HEY' in binary
Audio stream w/ message encoded
LSB column

Fig. 3 The binary form of each sample in audio file with 16 bits

4 The security system implementation

A system that guarantees high security for sensitive data has been designed and implemented using MATLAB platform. The two-layer security system for hiding sensitive text data on PCs is implemented using the MATLAB programming language because it offers very good performance for numerical computation, analysis of the data, capabilities of visualization, and the tools for developing the applications. This system is benefitting from the idea presented in the literature related to Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding [16]. In addition to that, MATLAB is providing ease of use to the functions where its interface leads the user through the two-process encryption and decryption of messages, i.e., into or from the cover, respectively. MATLAB has a large user community with lots of free code and knowledge sharing. Another interesting feature found in MATLAB software platform is its clearly written documentation with many examples to benefit from. The aim of this implementation is to study the idea of combining the two techniques as a 2-layer security system and to test different experiments to enhance this research field. An objective of implementation is to help crypto security designers and programmers to improve our system idea and make it practically usable. This research is found having common applications with several other visual models [17] but providing audio (unseen) research study (Fig. 4).

Running the system begins with entering the secret sensitive text data message and the secret key, which is

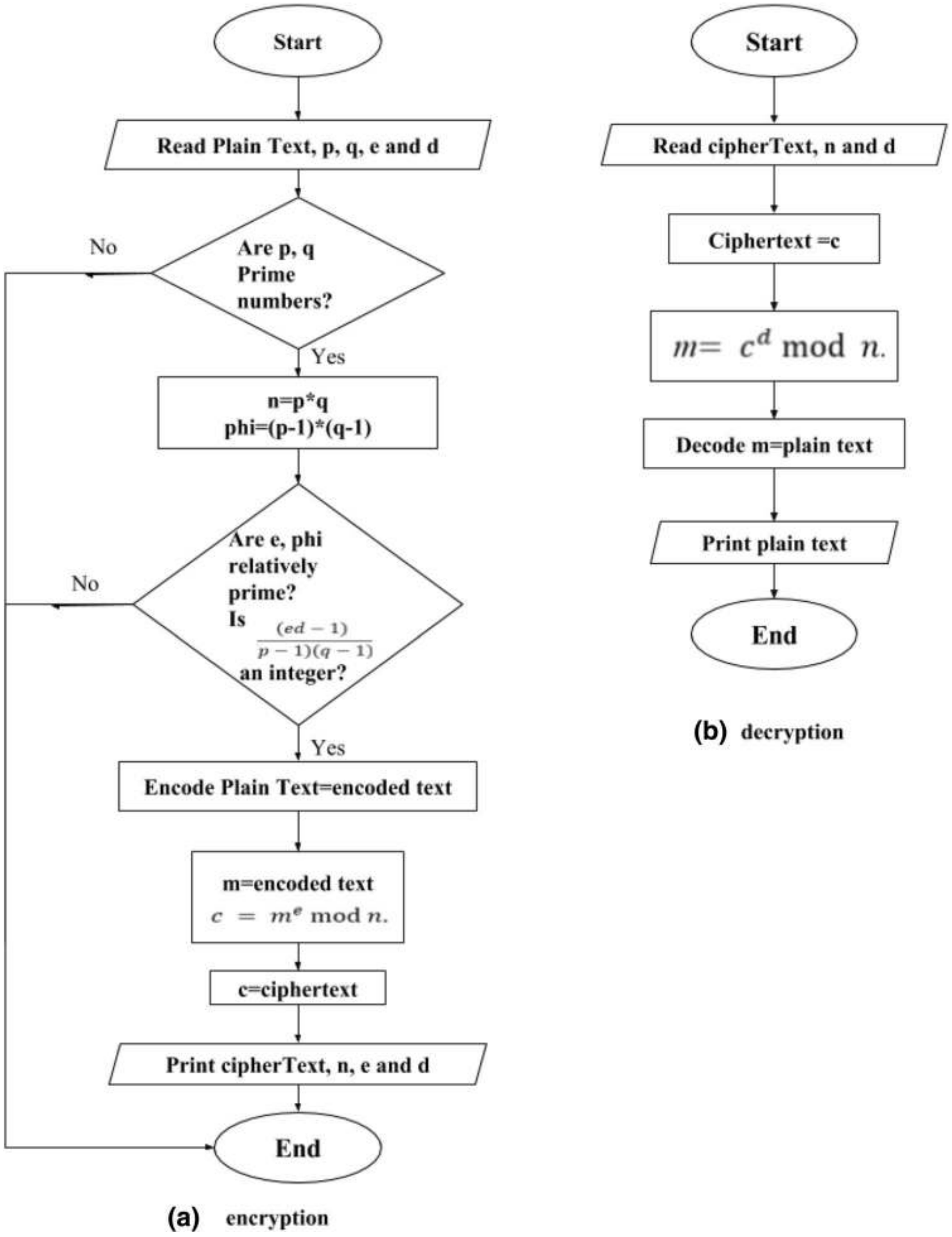
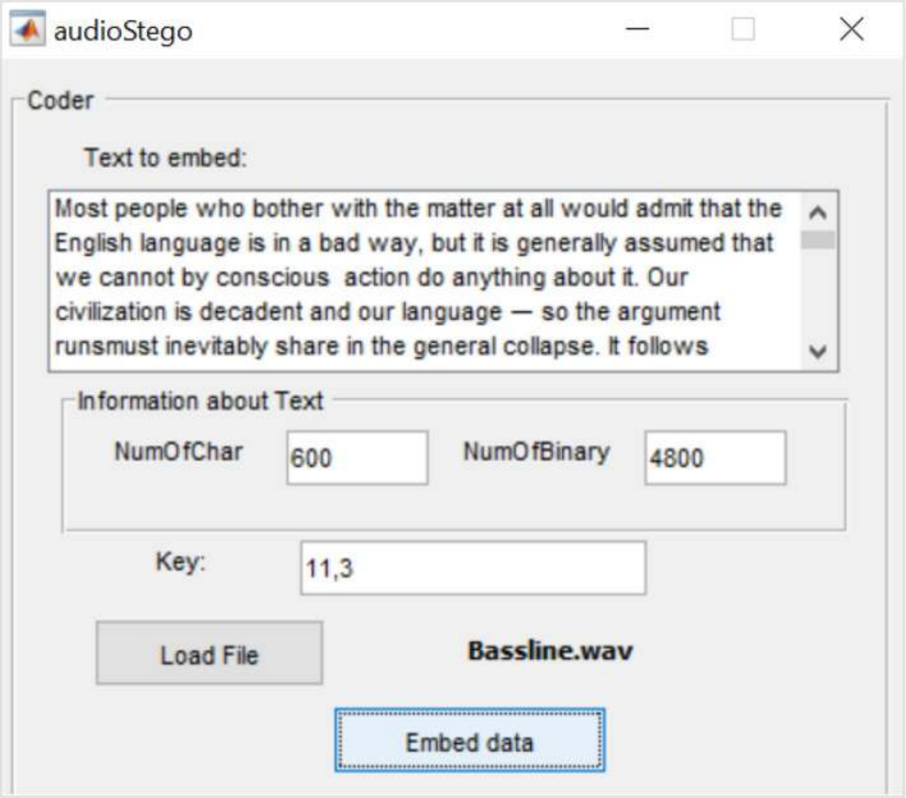


Fig. 4 Block diagram of RSA algorithm

representing the first layer cryptography layer. During this layer process, the program converts each char of the secret data into an array of binary bytes to be encrypted using RSA. On the other hand, the steganography layer also asks for audio as a cover file that will be converted into binary form. This second layer can start its process at the same time while the first layer is running, i.e., preparing the audio as binary bits, but will not start concealing text until the ciphertext is produced.

The implementation of the proposed method that was discussed previously can be observed as a process flow graph in Fig. 5, as a testing example. The system used cover audio file “Bassline” with 16 bits per sample, with size 3.45 MB. The implementation example uses the sensitive secret text data message *Text* with 600 characters as follows: “Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot by conscious action do anything about it. Our civilization is decadent and our language, so the argument runs must inevitably share in the general collapse. It follows that any struggle against the abuse of language is a sentimental archaism, like preferring candles to electric light or hansom cabs to aero planes. Underneath this lies the half-conscious belief that language is a natural growth and not an instrument which we shape for our own purposes.”The algorithm first encrypts the sensitive text data



Most people who bother with the matter at all would admit that the English language is in a bad way, but it is generally assumed that we cannot by conscious action do anything about it. Our civilization is decadent and our language — so the argument runsmust inevitably share in the general collapse. It follows

NumOfChar: 600

NumOfBinary: 4800

Key: 11,3

Bassline.wav

Fig. 5 The system interface showing bits statistics and the process of concealing secret text starting by RSA encryption followed by the audio-based steganography

(*Text*) with the secret key "11,3." The button "Embed Data" will not be active except if the audio is capable of holding all the bits of ciphertext. Concealing the secret data within the two-layer system then results proper security hiding in the stego audio file.

Figure 6 shows the interface that can be used as an example of retrieving back sensitive data that were concealing into a file using the two-layer system. By pressing the button "Decrypt Text," the program will be extracting the secret text data. It starts by sensing the LSBs within the stego audio collecting the bits together to produce the ciphertext. Then, the reverse cryptography layer decrypts the ciphertext using a secret key as inputs to generate the secret plain text message.

5 Results

The secret sensitive text message "*Text*" is encrypted and then hidden within 15 different audios, as introduced before, in order to be analyzed and compared. To clarify this elaboration, we selected 15 differently sized PC cover audios and noted the results. Table 1 lists the results of this experiment for 15 differently selected PC audios. The security testing study hided sensitive secret data, concealed in audio stego-cover, is resulting in bits changed based on the LSB choice used as listed in Table 1. These results made up the percentage computation of security and capacity per audio using the security of each audio as calculated using PSNR (peak signal-to-noise ratio) based on the formula [18]:

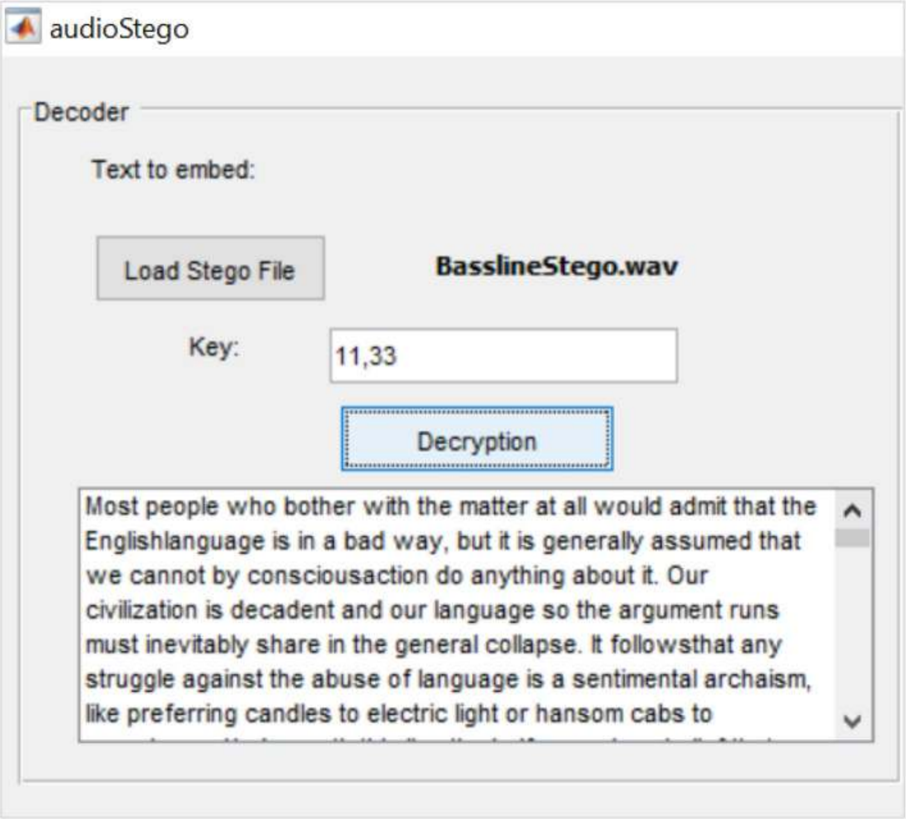
$$\mathrm{PSNR} = 20\log_{10}\frac{\mathrm{MAX}}{\sqrt[2]{\mathrm{MSE}}} \tag{4}$$

where MAX refers to the maximum intensity of the given resolution of each pixel and the MAX value in the image is 255. On the other hand, MSE is defined as the square of the error between the cover without any hidden data and the stego cover after hiding the message [19]. The difference between the two covers can be measured using MSE. The formula below represents this:

$$\mathrm{MSE} = \sum_{i=0}^{\text{allpixels}}\ \sum_{j=0}^{\text{all pixels}} \frac{(\mathrm{cov}(i,j) - \mathrm{steg}(i,j))^2}{m \times n} \tag{5}$$

Also the capacity of per audio is the amount of data that can be hidden in the audio file without significantly changing it. It is measured according to the cover that is used. The following formula illustrates the metric:

$$\text{Capacity} = \frac{(\text{number of characters }) \times 8}{\text{number of bits}} \times 100 \tag{6}$$



Key: 11,33

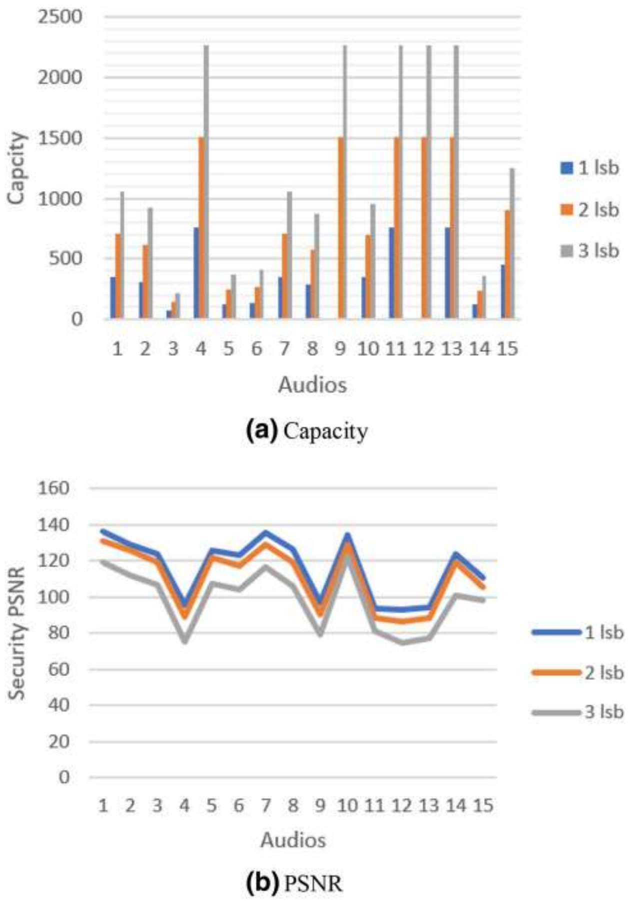
Most people who bother with the matter at all would admit that the Englishlanguage is in a bad way, but it is generally assumed that we cannot by consciousaction do anything about it. Our civilization is decadent and our language so the argument runs must inevitably share in the general collapse. It followsthat any struggle against the abuse of language is a sentimental archaism, like preferring candles to electric light or hansom cabs to

Fig. 6 Extracting back the secret message

Table 1 Testing results of stego-embedding the encrypted fixed sensitive data "text" in 15 different audios

Audio test-file number	High security and low capacity (1 LSB)		Medium security and capacity (2 LSB)		Low security and high capacity (3 LSB)	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
1	352.9	136.2	705.9	130.8	1058.8	119.0
2	306.1	129.2	612.2	125.3	918.4	111.7
3	73.1	123.5	146.2	119.2	219.3	106.6
4	756.0	95.4	1512.0	88.8	2268.0	75.4
5	123.5	125.4	247.0	121.6	370.5	107.4
6	135.8	122.9	271.7	117.4	407.6	104.2
7	352.9	135.5	705.9	129.2	1058.8	116.5
8	289.1	126.2	578.2	119.3	867.4	105.7
9	756.0	96.5	1512.0	90.5	2268.0	79.3
10	350.8	134.1	700.0	128.8	950.7	122.5
11	756.0	93.4	1512.0	87.99	2268.0	81.3
12	756.0	93.1	1512.0	86.08	2268.0	74.5
13	756.0	94.3	1512.0	88.37	2268.0	76.8
14	120.2	123.5	240.4	119.2	360.5	100.6
15	450.3	110.3	900.6	105.5	1250.0	98.2

In this work, we study the effect of the secret text on security and capacity in per audio using different LSBs. The selected LSBs are 1-LSB, 2-LSB, and 3-LSB to conceal the secret text into in each audio as shown in Table 1. The results of the security and capacity of audios after hiding the secret text in different LSBs are presented in Fig. 7. It is to be noted from Fig. 7 that depending on the LSB used and audio files available on the PC the security and capacity are changed, which means that cannot be predicted. Every cover audio is showing percentage of security result based on the specific LSB used. As shown in Fig. 7 when increasing the number of LSBs to conceal the secret text, the security will be decreased. On the other hand, capacity of the amount of the data that can be hidden in audio cover file will be increased when increasing the LSBs. In addition, the size of the cover audio has a different effect on security and capacity when concealing one text. From Fig. 7, it is observed that audio "1" with 1-LSB is giving the highest security percentage to hide secret text.



(a) Capacity

(b) PSNR

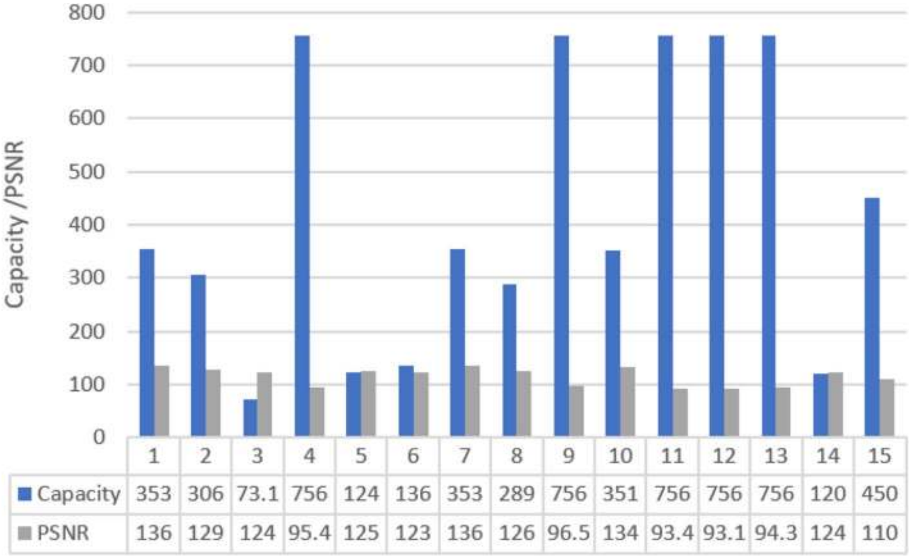
Fig. 7 **a** Capacity and **b** PSNR values when hiding one text using different audios of different sizes

From Fig. 8, it is observed that audios 4, 9, 11, 12, and 13, with 1-LSB stego-system, is giving the highest capacity with appropriate security, while audios 1 and 7 are providing the highest security with appropriate low capacity than the previous files.

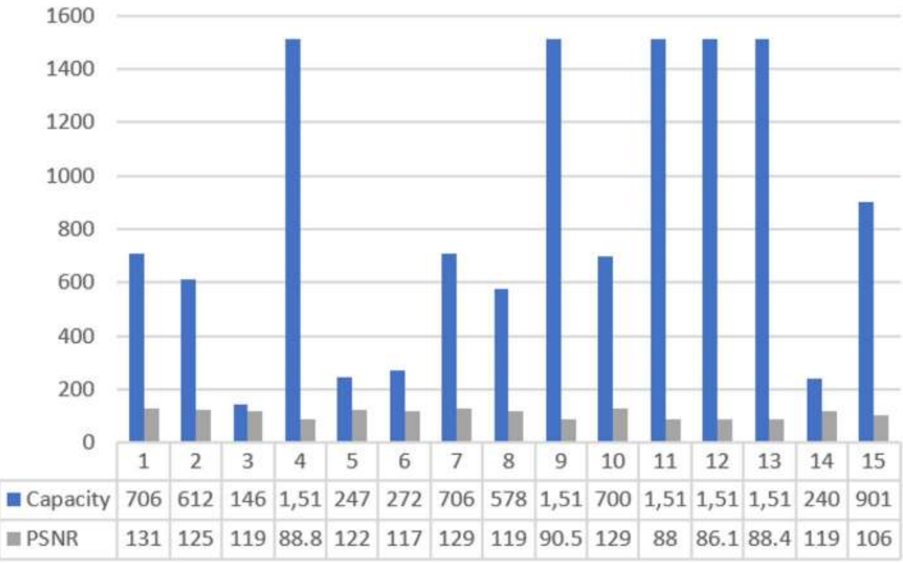
Utilizing 2-LSB increased the capacity of hiding information with acceptable security less than that for 1 LSB. It is to be noted from Fig. 7 that audio "12" is giving the lowest security percentage to hide secret. The audio "1" is the best choice to conceal the text according to the values of PSNR. Notice that the audio "1" is also the best choice for the user when he is using 3-LSB method.

From Fig. 8, it is noticed that audios 8 and 14 provide the same percentage of security with noticeable different values of capacity. This shows that not only the size of files affected the percentage of security, but also the binary content of the files affected the percentage of security verifying the data dependency importance as can be observed from the detailed analysis figures, i.e., Figs. 9, 10, and 11. Note that our work used 3-LSB in the stego layer to increase the capacity of the hidden sensitive text as an improvement to the known usage of 2-LSB. In fact, this study clarified that 3-LSB and 2-LSB can provide the same security level giving acceptable performance as well as the fact of confidentiality that no one can notice the hidden data in the audio cover.

Fig. 8 Capacity and PSNR values when hiding one text utilizing 1 LSB and different audios of different sizes

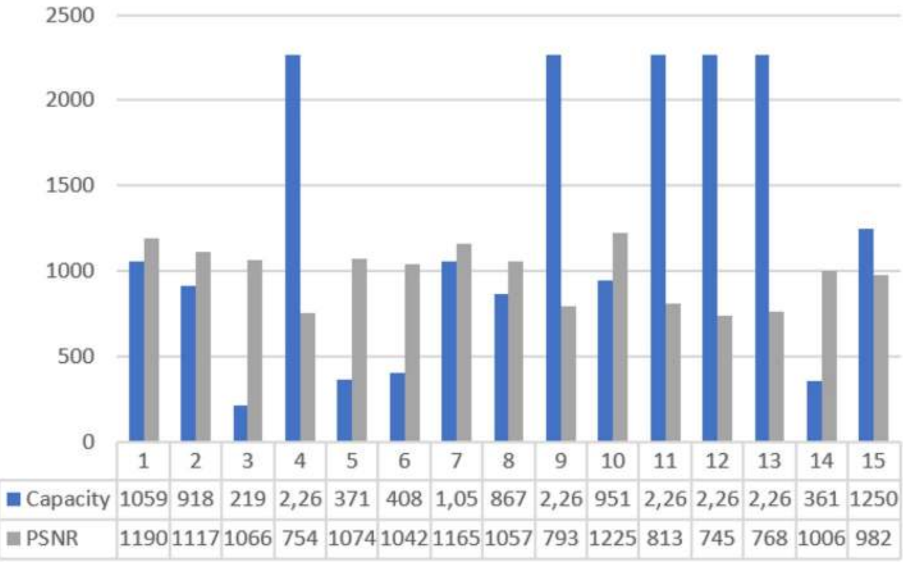


	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
■ Capacity	353	306	73.1	756	124	136	353	289	756	351	756	756	756	120	450
■ PSNR	136	129	124	95.4	125	123	136	126	96.5	134	93.4	93.1	94.3	124	110



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
■ Capacity	706	612	146	1,51	247	272	706	578	1,51	700	1,51	1,51	1,51	240	901
■ PSNR	131	125	119	88.8	122	117	129	119	90.5	129	88	86.1	88.4	119	106

Fig. 9 Capacity and PSNR values when hiding one text utilizing 2 LSB and different audios of different sizes



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
■ Capacity	1059	918	219	2,26	371	408	1,05	867	2,26	951	2,26	2,26	2,26	361	1250
■ PSNR	1190	1117	1066	754	1074	1042	1165	1057	793	1225	813	745	768	1006	982

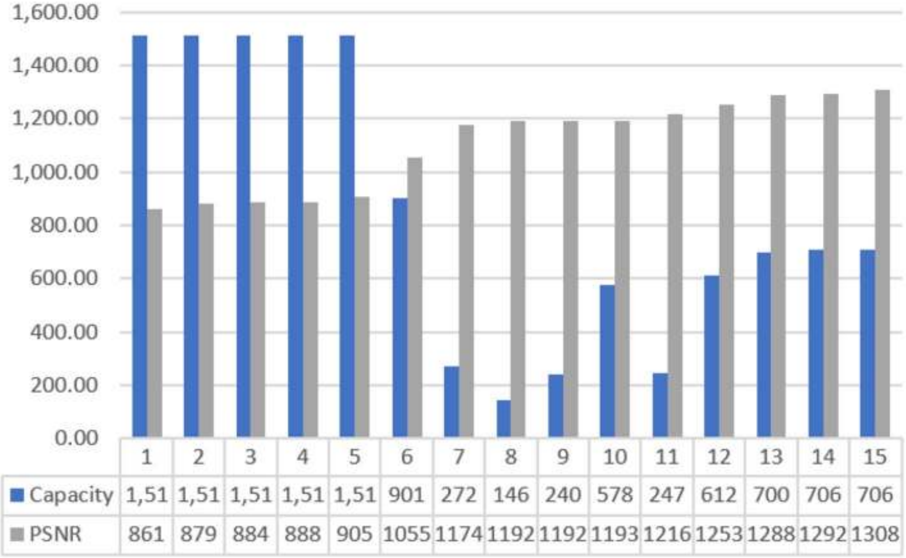
Fig. 10 Capacity and PSNR values when hiding one text utilizing 3 LSB and different audios of different sizes

The main difference between this work and the previous similar studies is our ability to utilize some of the available audio files to conceal secret data within a PC. Furthermore, our work suggested using 3-LSB in hiding the data to increase the capacity with consideration of the quality of the audio file after the security embedding. To clarify more, in comparing our work with Asad et al. [6], we found that in [6] they used AES secret key crypto algorithm to encrypt data while we improved it using RSA public key crypto algorithm according to the advantages that have been discussed above. In addition, we found in their work [6] that they are using 6-LSB and 7-LSB which increase capacity, but risk altering the audio files adding noise to it. Therefore, we suggested our work using 3 LSB offering an acceptable trade-off between acceptable capacity and security. Also considering comparison of our presentation with the previous work in [11], the authors suggested concealing the data in 1 LSB which results in the loss of the capacity, while it was proven that using 3 LSB increases the capacity preserving acceptable security.

6 Conclusion

In this work, we presented a security system within two separate layers for concealing secret data on personal computers. We used two methods: cryptography and steganography. The system was performed on the MATLAB platform showing motivating outcomes. The system concealed data in the audio in steganography layer using

Fig. 11 Capacity and PSNR values utilizing 3 LSB reordered based on increasing PSNR results



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
■ Capacity	1,51	1,51	1,51	1,51	1,51	901	272	146	240	578	247	612	700	706	706
■ PSNR	861	879	884	888	905	1055	1174	1192	1192	1193	1216	1253	1288	1292	1308

several LSBs to increase the capacity without deterioration of the security, which was performed to accept the security of 1-LSB, 2-LSB, and 3-LSB methods. The system examined the relationship between the secret data to be hidden in the normal audio files of the PC, and its effecting analysis on security by experimenting the proposal on 15 differently sized audios presenting interesting outcomes.

For future work, we suggested two improvements: first one, adapting the crypto layer to test different symmetric algorithms and the second improvement that modifies the method to make it support other languages like Arabic.

Acknowledgements Authors thank Taif University and Umm Al-Qura University for motivating this cooperative research.

Compliance with ethical standards

Conflict of interest We declare that this article is original and has no conflict.

References

1. Al-Otaibi N, Gutub A (2014) 2-Leyer security system for hiding sensitive text data on personal computers. Lect Notes Inf Theory Eng Technol Publ 2(2):151–157
2. Al-Otaibi N, Gutub A (2014) Flexible stego system for hiding text in images of personal computers based on user security priority. In: Proceedings of 2014 international conference on advanced engineering technologies (AET-2014), Dec 2014, pp 250–256
3. Gutub A (2010) Pixel indicator technique for RGB image steganography. J Emerg Technol Web Intell 2(1):56–64
4. Al-Otaibi N, Gutub A, Khan E (2015) Stego system for hiding text in images of personal computers. In: The 12th learning and technology conference: wearable tech/wearable learning. Effat University
5. Deshmukh R, Deshmukh P (2011) 4 Layer enhanced security for audio signals using steganography by modified LSB algorithm and strong encryption key. Int J Adv Res Comput Sci 2(2):492–495
6. Asad M, Gilani J, Khalid A (2011) An enhanced least significant bit modification technique for audio steganography. In: 2011 international conference on computer networks and information technology (ICCNIT), pp 143–147
7. Shaikh A, Solanki K, Uttekar V, Vishwakarma N (2014) Audio steganography and security using cryptography. Int J Emerg Technol Adv Eng 4(2):317–318
8. Saurabh J, Ambhaikar A (2012) Audio steganography using RPrime RSA and GA based LSB algorithm to enhance security. Int J Sci Res 1(2):62–65
9. Padmashree G, Venugopala PS (2012) Audio steganography and cryptography: using LSB algorithm at 4th and 5th LSB layers. Int J Eng Innov Technol 2(4):177–181
10. Ravali SVK, Neelima P, Sruthi P, Sai Dileep P, Manasa B (2014) "Implementation of blowfish algorithm for efficient data hiding in audio. Int J Comput Sci Inf Technol 5(1):748–750
11. Abikoye Oluwakemi C, Adewole Kayode S, Oladipupo Ayotunde J (2012) Efficient data hiding system using cryptography and steganography. Int J Appl Inf Syst 4(11):6–12
12. Goshwe N (2013) Data encryption and decryption using RSA algorithm in a network environment. Int J Comput Sci Netw Secur 13(7):9
13. Zhou X, Tang X (2011) Research and implementation of RSA algorithm for encryption and decryption. In: 6th international forum on strategic technology (IFOST), 2011
14. Gutub A, Khan E (2011) Using subthreshold SRAM to design low-power crypto hardware. Int J New Comput Archit Appl 1(2):474–483
15. Alanizy N, Alanizy A, Baghoza N, AlGhamdi M, Gutub A (2018) 3-Layer PC text security via combining compression, AES cryptography 2LSB image steganography. J Res Eng Appl Sci 3(4):118–124
16. Alsaidi A, Al-lehaibi K, Alzahrani H, AlGhamdi M, Gutub A (2018) Compression multi-level crypto stego security of texts utilizing colored email forwarding. J Comput Sci Comput Math 8(3):33–42. https://doi.org/10.20967/jcscm.2018.03.002
17. Al-Nofaie S, Fattani M, Gutub A (2016) Merging two steganography techniques adjusted to improve arabic text data security. J

Comput Sci Comput Math 6(3):59–65. https://doi.org/10.20967/jcscm.2016.03.004

18. Harshitha K, Vijaya P (2012) Secure data hiding algorithm using encrypted secret message. IJSRP 2(6):1–4
19. Jain V, Kumar L, Sharma M, Sadiq M, Rastogi K (2012) Public-key steganography based on modified LSB method. J Glob Res Comput Sci 3(4):26–29

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.