Hiding Encrypted Speech Using Steganography

ATEF J. AL-NAJJAR, ALEEM K. ALVI,
SYED U. IDREES, ABDUL-RAHMAN M. AL-MANEA
Computer Engineering department
King Fahd University of Petroleum and Minerals
KFUPM Box 1727, Dhahran 31261, Saudi Arabia

Abstract: — In this paper, we have proposed a cryptosystem using state of the art technology. We used the minimum possible compressed speech file for encryption. Additionally we applied data compression to speech files and added further compression. Then we applied data encryption techniques to minimize security threats. We applied the symmetric and asymmetric encryption algorithms to the compressed speech files. This was followed by hiding these files into cover images using steganography. This camouflages the secret data and reduces chances of eavesdropping. By using compression, the capacity has been increased. However, after applying encryption, the size of the encrypted data becomes much greater than the input file size, therefore hiding it in a cover demands more capacity. We have analyzed the size of the cipher texts of the compressed speech data for further enhancement of the capacity.

Keywords — Speech compression, Symmetric and asymmetric encryption, Steganography

1 INTRODUCTION

This paper deals with the proposed cryptosystem including compression, encryption and steganography. The proposed system incorporates these technologies in steps. The objective of the system is to send the secret speech data with security, transparency and robustness. Figure 1 shows the relation between capacity, transparency and robustness. If we increase the capacity of any cover to store data with more than certain threshold value, then its transparency will be affected. With high capacity, the steganography is not strong enough to keep transparent from the eavesdroppers. Similarly it is vise versa for robustness. It is a tradeoff between the capacity, robustness and transparency. It is required to select all parameters in such a way that steganography can be achieved on the best level.

Steganography is used to hide the secret message data using any other innocent cover object (may be text, image, audio or video etc.) in such a way that another person could not know about the existence of the original message. However it is different with cryptography in the sense that cryptography encrypts the data to be secured, which is generally understood and visible. Any one can try brute force or any other algorithm to break it.

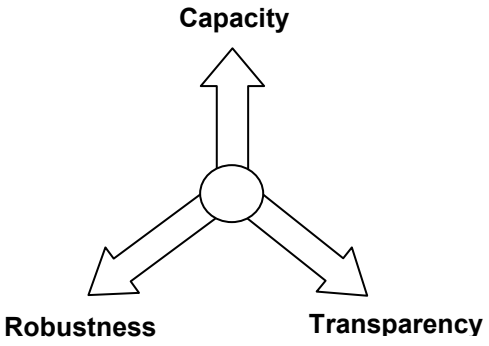


Figure 1: Tradeoff between capacity, transparency and robustness [1]

Steganography does not use algorithms to encrypt information. On the contrary, it is a process to hide data within another object so that it is hard to detect its presence. A secret message can be hidden in a *wav* file, graphic file, *exe* file or *html* using tags etc.

In this paper we hide the compressed speech data after applying selected cryptographic algorithms. Nowadays, *secure communication* means the object data send by encryption either it is half duplex or full duplex, real time or non real time, the security is one of the major parameters. This is the war between eavesdroppers and cryptography experts who develop the algorithms for secure communications. Always the need of better secure communications in comparison of the existing ones is creating the motivations to develop more and more secure systems. However, by applying encryption techniques, we can have encrypted data of our speech ready for transmission, but is it still secure? The answer depends on the type of encryption techniques, the time required to break it. However, in addition to this, by using steganography techniques we reduce the chances of suspicion on secret data from eavesdropper who caught the message object (cover).

In symmetric key algorithms, when DES was broken by using special computing power [2], 3DES algorithm was suggested for increasing the key size three times that of DES without changing the DES algorithm [3]. RSA as asymmetric algorithm use longer keys for more security [4]. However, this cannot eliminate the struggle against eavesdropping entirely. Hidden messages can be concealed from eavesdroppers using steganography. It means he/she is unlikely to attempt an attack on the captured data.

2 COMPRESSION

Preparation for the encryption step includes the use of the smallest size secret speech data using the appropriate file format without loosing the quality of the secret speech. We have taken one speech sample that includes three 'Hello' word voice. We store this sample using 7 uncompressed, 6 lossy compressed and 1 lossless compressed formats. For further compression we apply the LZ77 algorithm [5, 6] using *zip* utility to compress. We have found little improvement in size with certain audio formats. Figure 2 shows the comparison among these audio codec algorithms.

We have observed that there is no change in size for the uncompressed formats and also for some compression formats. In lossy-compression, we have observed that there is much compression. However, after the LZ77 algorithm was applied, some of them showed improvement and some did not. In lossless compression, there is improvement in decreasing size, but no improvement using the LZ77 algorithm.

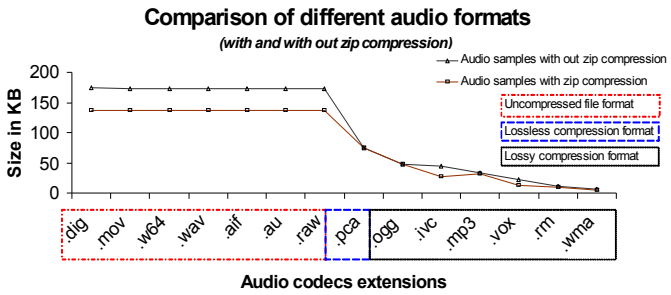


Figure 2: A comparison of audio samples

We found that the Windows Media Audio (WMA) format is the best candidate among others for encryption and then steganography. Because WMA file format gives the smallest file size (with using specific settings for encoding). We found a further reduction of 1KB in size from the original (WMA file of sample) after applying the LZ77 algorithm.

3 ENCRYPTION

Encryption is the process of transforming information; e.g. plaintext, into encrypted text called ciphertext. That ciphertext can only be decrypted by having specific information.

Decryption refers to the reverse process. Encryption/decryption has been used from ancient times to modern age for secret communication. Nowadays, use of security is for communication either real time or not, in internet, e-commerce, mobile telephones, banks, automatic teller machines, and in digital rights management, etc.

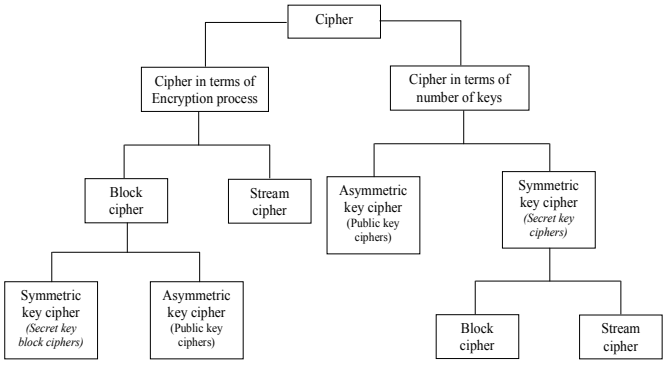


Figure 3: A taxonomy of cryptosystems based on [7]

Figure 3 shows the taxonomy of the cryptosystems in term of the number of keys and encryption process. We have used the secret key cipher and public key cipher i.e. 3DES (cipher block chaining), Asymmetric Encryption Standard (AES), and RSA, respectively.

Encryption creates the secret encrypted message for protecting the confidentiality. However for integrity, authorization and authenticity we need further techniques; for example, a message authentication code (MAC) or digital signatures. Cryptosystems are based on cryptographic software and hardware to perform encryption and decryption. However, successfully using cryptosystems to ensure security is not hundred percent sure. Any weakness or flaw in the system design or execution can allow successful attacks from the eavesdroppers.

4 STEGANOGRAPHY

Today, many algorithms show their stability for secure communications, e.g. RSA with large key size, say 1024, as public key cipher or AES as private key cipher. However it provides more security if eavesdroppers can not detect the presence of the secret message either encrypted or not. If encrypted secret message is detected then eavesdropper starts to work out the message by applying the technique to decrypt. At this stage cipher algorithms must be sophisticated that the time for breaking it, is must be beyond the present context. An encrypted hidden message into a cover object makes eavesdropping more difficult.

The word "Steganography" is of Greek origin and means "covered or hidden writing". Hiding media may be text, image, audio, video, binary or html file etc. This apparent media object looks as a message called cover. For instance, in old ages, a message may be hidden by using invisible ink between the visible lines of innocuous documents. Modern steganographic techniques differ with the historical ones. There implementation require algorithmic procedures and are complex in nature. However, it provides more security. Figure 4 shows the classification of the information hiding presented in [8, 9, and 10]. Based on this taxonomy we use modern steganography with images for hiding the encrypted data.

Steganography has the advantage to cryptography that secret messages do not attract attention to an eavesdropper. If the message is encrypted but not hidden; it will arouse suspicion and may be in itself be the victim of the attacker, whether he or she breaks it or not, but attempts are done. This also makes incriminating on sender when encryption is illegal in their countries [11].

In some application scenarios, multimedia steganography techniques have to satisfy two basic requirements in order to make the cover object and stego object perceptually indiscernible. The first requirement is perceptual transparency and the second one is high data rate of hidden data. With few changes, every application requires a high bit

rate of an embedded data [12].

A cover object (image, audio or video etc) with a large size (means comprising of a large number of bits) can be used to hide the secret message with more ease. Because it has good capacity to store the data without revealing any change in the original cover object. For this reason, a digital cover object containing large amounts of data is used to hide messages on the internet and on other communication media.

A cover can be created in any way, e.g. 2 least significant bits of each byte of an image can be replaced with the bits of the secret message. This LSB replacement does not greatly affect the cover object (image) to reveal the change.

The other practice of the information-hiding is "A digital watermark"; that can be inserted on the digital images so that illegal copies of the images can be detected with some more sophisticated method. This practice is also carried out while printing currency notes at the monetary agencies.

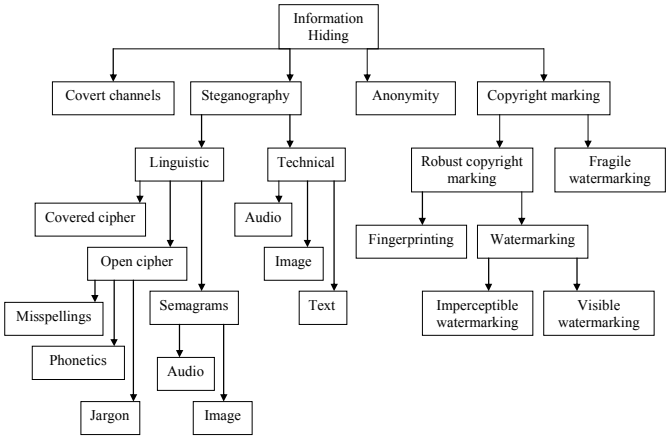


Figure 4: A classification of information hiding techniques based on [8, 9, 10]

and steganography in our system, for enhancing security. We have selected the speech file as the secret message stored into a smallest file format (e.g. wma). For further compression we apply the LZW compression algorithm and store it into zip file format. This finally compressed file is encoded into integer numbers using MATLAB.

We use the selected RSA from asymmetric category and 3DES and AES (Rijndael) from symmetric encryption algorithms to encrypt the integer numbers. The selection is made because of there diverse algorithmic procedure. However; the 3DES is the ancestor of AES. This encrypted data is hidden in a cover object (we use the image) using a simple steganography technique (2 bit LSB insertion with minimal affect on the perception of the cover object.). Then, the given cover has been modified to store the encrypted compressed speech data. The resulting cover object is a stego object without showing significant change. The whole sending-end process of the cryptosystem is shown in Figure 5.

Now only the recipient knows the technique to recover the message and then decrypt it using the receiving-end part of the cryptosystem, discussed later

5.1 Sending End

We have been selecting speech file format with least size by experimenting with available codec's. The best we have found is the WMA format, which is smaller in size and preserving the quality of the speech. The smaller size leads to faster computation during the encryption/decryption process, and reduces the power consumption (if battery is used) of the overall system in case of handheld devices.

The purpose of hiding encrypted compressed speech files into cover object (using steganography), is to mislead the eavesdropper. This will minimize the threat of eavesdropping. Encrypted compressed speech file inside image as cover object is a unique combination of hiding the message to achieve more secure communication. For increasing the capacity, audio or video files can be used for the cover object. However, using an image as the cover object, capacity has been increased by selecting a least size gray image or three dimensional

images etc.

Table 1: Comparative analysis of data compression for speech

Types	Comparative Analysis of Data Compression for Audio / Speech				
	Samples	Size in Kilo Bytes			
		file formats		wma only	
		wav	wma	zip	rar
General	Hello *(3 times)*	173	6	5	5
Quranic Verses in Arabic and their translations in English and Urdu languages	Bismillah *(Arabic)*	940	8	6	6
	Bismillah *(English Translation)*	747	6	5	5
	Bismillah *(Urdu Translation)*	809	7	5	5
	Surah-e-Ikhlas *(Arabic)*	2463	16	13	13
	Surah-e-Ikhlas *(English Translation)*	2465	17	14	14
	Surah-e-Ikhlas *(Urdu Translation)*	3048	19	16	16

Selecting the least file size using WMA codec and then applying a compression algorithm to reduce the data size yields good results (in terms of decreasing the size). Table 1 shows the comparative results of data compression. The samples text is mention in appendix A.

Table 1 describes the significant change in size from *wav* to using WMA (codec) with maintaining the quality of speech. Additionally, by applying the LZW compression algorithm, further reduction in size is obtained. However there is no difference between zip and rar compression.

We have done additional experiments to understand the effect of the size of the secret message in terms of the different linguistics. We have selected three languages: Arabic, English and Urdu for this purpose. We have taken the same secret message in all three languages recorded in *wav* and WNA formats. It is observed that different file sizes were obtained for the same message in different languages, and Urdu has taken more file size in comparison of Arabic and English. We left it for future research to repeat the same experiment with as many languages as possible, and find the language in which the secret message is always stored (statistically) in a lower size. Then we can manage the language translation for from one end of the crypto system to another.

5.2 Receiving End

The receiving-end of the cryptosystem performs the reverse of all steps which have been done before. The detailed diagram of the receiving-end cryptosystem is shown in Figure 6

. It receives the stego object and retrieves the hidden encrypted data. This encrypted data is converted from binary to integer numbers and then decrypted using the decryption algorithm. This decrypted data is decoded into the zip file and decompressed using the LZW compression algorithm (using zip utility). The result is the secret speech file.

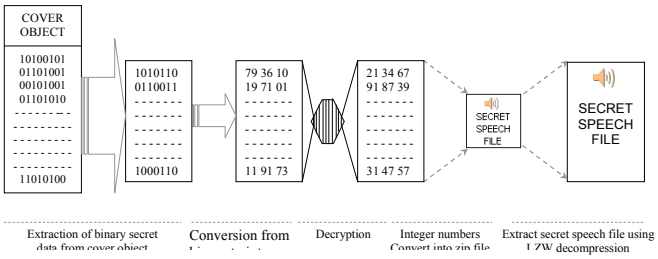


Figure 6: Receiving-End of the proposed cryptosystem

We used a number of samples of speech, in different languages (i.e. English, Arabic, Urdu), to get a mix of frequencies. This was done to enhance the accuracy of the results. Therefore a reverse procedure has the following steps, i.e. (1) the removal of the bits from the stego, (2) conversion into integers, (3) decrypting the temporary result with the decryption key and (4) finally decompressing; that gives the original secret speech. This whole process is shown in Figure 6.

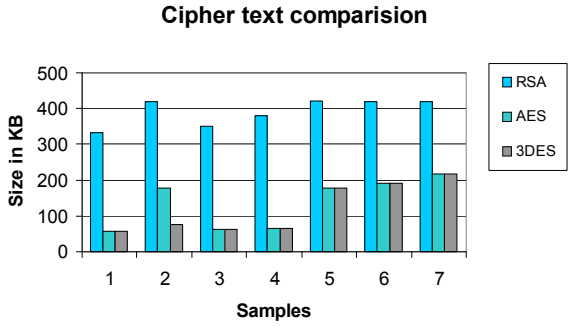


Figure 7: A comparison of cipher text

Figure 7 show that the comparison of the cipher text after encryption and that gives the requirement of the capacity of the cover object. This shows that the RSA (asymmetric algorithm) has more cipher text in size as compared to the 3DES and AES (symmetric algorithms). In this case, the less capacity symmetric algorithm is best to encrypt the data. On the other hand, if the capacity is available, (e.g. cover object as video) then RSA will be preferable because it solves the key management problem.

In [13], Lisa M. Marvel elaborates on the capacity of a cover by developing a capacity metric that can be used as a performance criterion for the class of steganographic methods that add the secret speech data. It is used for all types of cover data including imagery and audio. It is used to calculate precise estimate of the maximum amount of payload that can be embedded and successfully extracted from the cover data.

In [14] Kaushal M. Solanki have introduced a general framework for a data hiding system, based on the following steps i.e. (1)encoding of message & host image with secret key, (2) generation of a composite image, (3) avoiding intentional/unintentional processing attacks, (4) decoding with the secret key to get original message.

6 CONCLUSION

We have discussed vital issues of a cover object that contains essential speech data by saving compressed speech files in different languages using ss and lossy audio formats. We have shown the s for the overall operations. As a complete system, data encryption techniques applied on essed speech minimizes security threats. nography was further used to hide the pted data for improved security. It minimizes eat of eavesdropping.

cipher texts of the compressed speech data that the asymmetric algorithm produces large text file in comparison of the symmetric algorithm. Figure 7 shows that in case of utilization of asymmetric algorithm always we need approximately 5.7 times more capacity in cover object as compared to symmetric algorithms.

REFERENCES

[1] J. Fridrich, Applications of data hiding in digital images, Tutorial for the ISSPA 1999 conference in Brisbane, Australia, 1999.

[2] Fred Moore, "Preparing for encryption:

In the name of God, Most Gracious, Most Merciful
[112:1] Proclaim, "He is the One and only GOD.
[112:2] "The Absolute GOD.
[112:3] "Never did He beget. Nor was He begotten.
[112:4] "None equals Him."

new threats, legal requirements boost need for encrypted data", Computer Technology Review, August-Sept, 2005

[3] NIST, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher" , Special Publication 800-67.

[4] R. L. Rivest and R. D. Silverman, `Are "strong" primes needed for RSA?', Preprint , 1999, 1--23. http://citeseer.ist.psu.edu/rivest99are.html

[5] Jacob Ziv and Abraham Lempel; A Universal Algorithm for Sequential Data Compression, IEEE Transactions on Information Theory, Vol.23, No.3, pp.337-343, May 1977.

[6] Vito Dai and Avideh Zakhor, Lossless Compression Techniques for Maskless, Video and Image Processing Lab, Department of Electrical Engineering and Computer, Univ. of California/Berkeley, http://www-video.eecs.berkeley.edu/papers/vdai/spie4688-67.pdf

[7] Ian Barnes, Ramesh S., Lecture on Public Key Cryptosystem, Department of Computer Science, Faculty of Engineering and Information Technology (FEIT) Fall semester 2006, The Australian National University , Accessed on June 29, 2007, http://cs.anu.edu.au/Student/comp3410/lectures.html

[8] F. L. Bauer, Decrypted Secrets-Methods and Maxims of Cryptology, Berlin, Heidelberg, Germany: Springer-Verlag, 1997.

[9] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, Information Hiding - A Survey, Proceedings of the IEEE, special issue on protection of multimedia content, Vol.87,No.7, pp.1062-1078, July 1999.

[10] D. Vitaliev, Digital Security and Privacy for Human Rights Defenders, The International Foundation for Human Right Defenders, pp.77-81, Feb. 2007.Lisa M. Marvel, Image Steganography for Hidden Communication, Ph.D. Dissertation, Spring 1999, University of Delaware, US.

[11] Caloyannides, M.A., Encryption wars: shifting tactics, Spectrum, IEEE, Vol. 37, No. 5, pp.46 – 51, May 2000

[12] R.J. Anderson, F. A. P. Petitcolas, On the Limits of the Steganography, IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, 1998, pp. 474-481.

[13] Lisa M. Marvel, Image Steganography for Hidden Communication, Ph.D. Dissertation, Spring 1999, University of Delaware, US.Kaushal

[14] M. Solanki, Multimedia Data Hiding: From Fundamental Issues to Practical Techniques, Ph.D. Dissertation, December 2005, University of California, Santa Barbara, US.

7 APPENDIX A

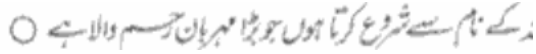
In this appendix A we have given he scripts of the all the speeches which we have used in the Table 1.

Bismillah:
Arabic

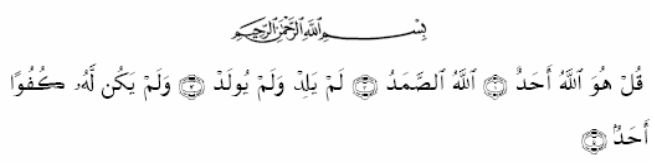
English translation:

In the name of Allah, Most gracious, most merciful

Urdu translation:

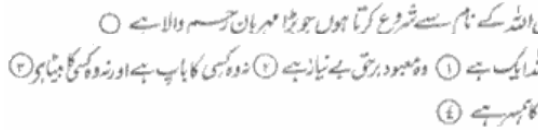


Surah-e-Ikhlas:
Arabic



English translation[1]:

Urdu translation[2]:



[1] Islamic portal, http://www.quran-islam.org/110.html
[2] Comprehensive portal of Urdu http://www.loveurdu.com/quranurdu/home.asp?Pid=547