Development of New Covert Audio Cryptographic Model

Ziyad Tariq Mustafa Al-Ta'i

Department Computer Science,College of Science-University of Diyala

Receiving Date: 01-02-2011 - **Accept Date:** 14-06-2011

Abstract

New covert cryptography is a different trend in cryptography field, because it has the features: (secrecy, covert, and simplicity). In this paper, a proposed new covert audio cryptographic model is presented by software simulation. The proposed model has the ability to cryptographically hide secret audio messages in image cover.

The proposed model was implemented using: (dual secret sharing method in order to obtain secrecy feature, masking technique in order to obtain covert feature, and psychoacoustics effects in order to obtain simplicity feature).

The performance of the proposed model has been successfully tested by computer simulation and the results presented both quantitavely and qualitatively. Finally, the proposed model has been implemented between two nodes through the Internet network.

Introduction

Broadband communication networks and multimedia data available in a digital format (images, audio, video) opened many challenges and opportunities for innovation[1]. Speech is probably the most fundamental form of communication available to us and our society has become highly dependent on our fast and accurate means of transmitting spoken messages. Usually the aim of communicants is merely to transmit a message as quickly, accurately and cheaply as possible. There are, however, a number of situations where the information is confidential and where an interceptor might be able to benefit immensely from the knowledge gained by monitoring the information circuit. In such situations the communicants must take steps to conceal and protect the content of their spoken message. Of course, the amount of protection will vary. On occasions it is sufficient to prevent a casual listener from understanding the message but there are other times when it is crucial that even a determined interceptor must not be able to deduce it [2].

.New covert cryptography is a different trend in cryptography field, because it has the features: (secrecy, covert, and simplicity). This new trend has appeared for two main reasons: first: cryptography has solved the problem of protecting privacy of information content, but it has not protected the anonymity of its sender and receiver. Second: to have a trusted system, one has to build it on his/her own, or the system must be simple enough so that one is able to check its correctness in implementation [3].

It is often thought that communications may be secure by encrypting the traffic, but this has rarely been adequate in practice. Classical researchers concentrated on methods for hiding messages rather than for enciphering them. So the study of communications security includes not just encryption but also traffic, whose essence lies in hiding information [3].

In the increasingly connected modern world, one may wish to be able to protect not only secrecy of the communication but also privacy of the communicators. Anonymous communication allows one to communicate without revealing who is communicating. Anonymous communication, the onset of computer technology and the Internet has given new life to information hiding and the creative methods with which it is employed [4].

Information hiding, in general, is covering sensitive information within normal information. This creates a hidden communication channel between the sender and receiver such that the existence of the channel is unnoticeable. Hidden channels have advantages over the encrypted channels that the anonymity of communication is protected [5].

Audio hiding, in particular, is a method for embedding information into an audio signal. It seeks to do so in a robust fashion, while not perceivably degrading the host signal (audio cover). To protect audio files against hacking , the researchers have ensured that the algorithm embeds bits of hidden information in deeper layers of the audio file and alters other bits to decrease the error [6].

In 1995, Naor and Shamir [7] opened the door to new covert cryptography in which cryptographic computation can be done without the use of a computer. Their research has mainly focused on guaranteeing privacy, and the (decryption) requires only primitive technology.

Desmedt et al. [8] pointed out that traditional hiding and steganography methods have the disadvantage that once their method is known, any one can find embedded message. Therefore, they have been combined the concepts of new covert cryptography and information hiding to create new covert cryptographic models which are perfectly secure and whose (decryption\extracting) process involves primitive technologies only [9][10].

New Covert Cryptography

Since the speech or real pictures are much better means of communications between a human user and a cryptographic device, it is convenient to develop simple cryptosystems whose plaintexts are barely binary digits, but higher level languages such as audio or images. These cryptosystems are preferable to have the following properties:

1. Secrecy: the information sent is protected from unwanted eyes.
2. Covert: the existence of the secret channel is invisible to others.
3. Simple: the decryption involves simple device only.

Therefore, these systems are called New Covert Cryptographic models [5]. One might question why one needs simple models. It is known that an encryption device can securely leaks its private keys to the network without creating any trace. Thus a complex black-box system may not be trusted. To have a trusted system, one has to build it on his/her own, or the system must be simple enough so that one is able to check its implementation correctness [5].

New covert cryptographic models are previously described in different ideas by different authors such as:

- Visual cryptography [7].
- Cerebral cryptography [11].
- Binary audio cryptography [8].
- Optical Cryptography [8].
- Non Binary audio cryptography [9].
- Moire' Cryptography [10].

The Proposed Model

Primitive Model

The primitive model is shown in figure (1). This model depends on weak points of Human Visual System (HVS) such as: Masking effect and Phase effect. The idea of decrypting/extracting secret audio message is taken from [9], but with development.

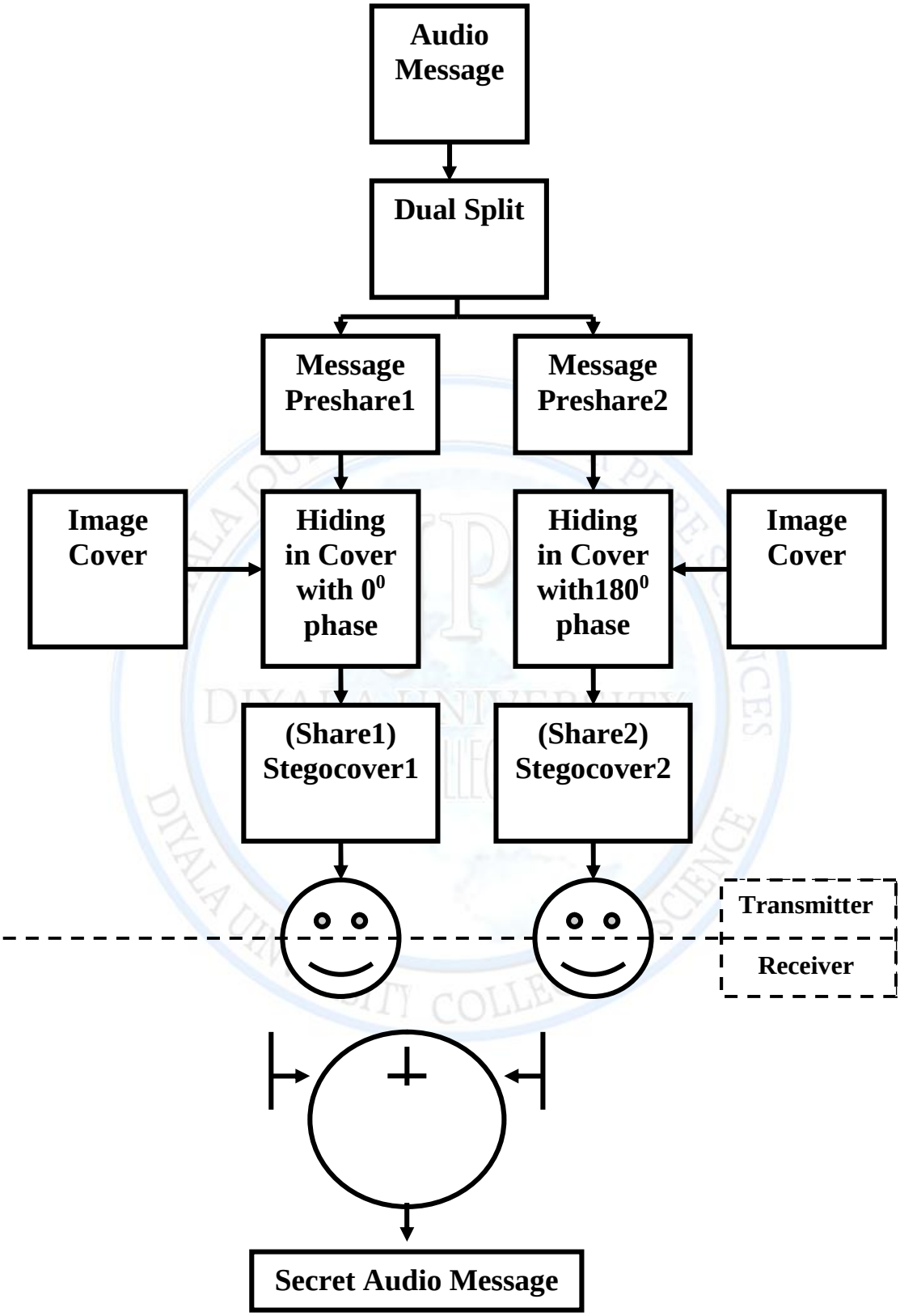


Fig.(1) The Primitive Model

Implementation of Proposed Model:

The proposed model is shown in figure (2).

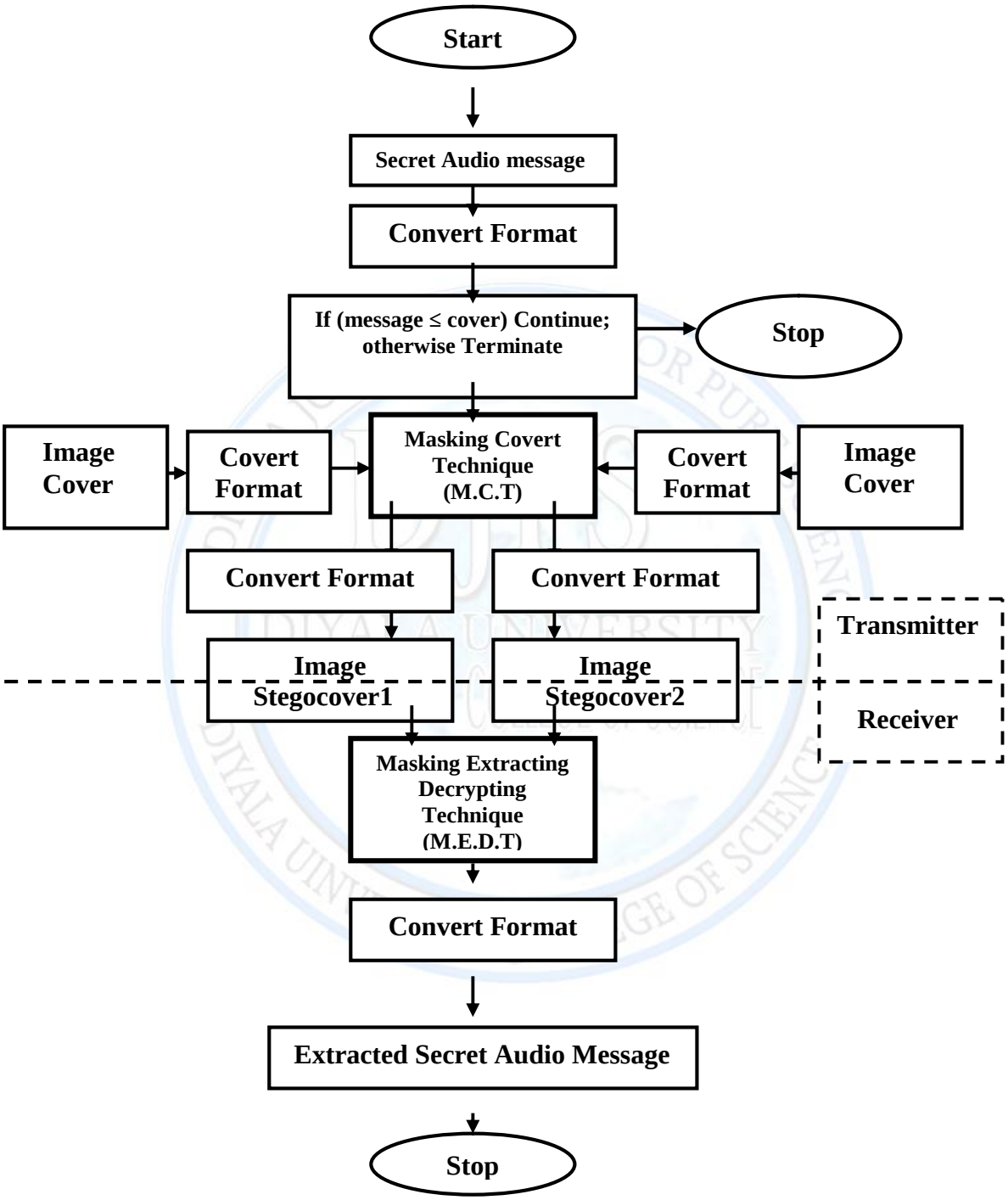


Figure (2) Block Diagram of Proposed Model

In transmitter side of this model the secret audio message is converted into stream of numbers, and the image cover is converted into stream of numbers.

At beginning, comparison process must be done to check if the secret audio message size is smaller than or equal to the cover size in order to continue. Otherwise, termination is accomplished in order to change the message or the cover. Inside the Masking Covert Technique (M.C.T) which is shown in figure (3).

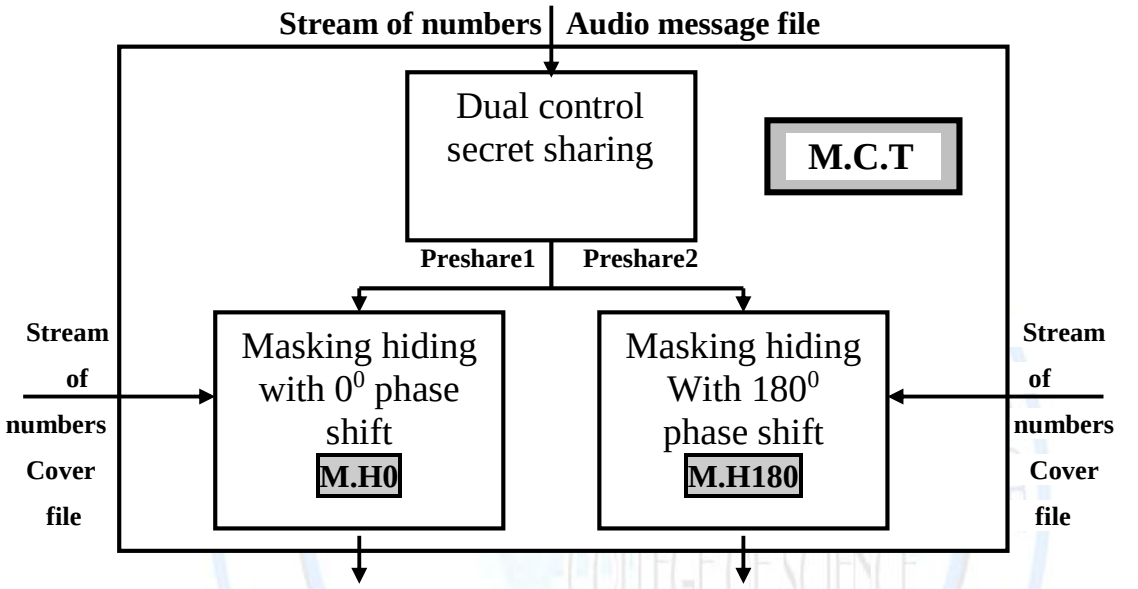


Figure (3) Masking Covert Technique (M.C.T)

the stream of numbers secret audio message is divided into 2 preshare files using dual control secret sharing process as described below.

Dual Control Secret Sharing

The principle of this technique is Dual Control secret sharing by Modular Addition. This technique is concerned with file of stream numbers of audio message. By using Dual Control Modular Addition technique, the stream of numbers audio message file is divided into two streams of random numbers preshare files.

Then, preshare1 file is masked by stream of numbers image cover with (0^0) phase shift to produce image stegocover1 using (M.H0) process as described below:

Masking Hiding with (0^0) phase shift (M.H0)

The principle of this technique is Temporal Masking. The masking technique with (0^0) phase shift is implemented by quieting the preshare1 file in comparison with stream of numbers image cover file. The implementation algorithm of masking hiding with (0^0) phase shift is shown in equation (1).

$$Stegocover1=k\times m+(1-k)\times c \quad \ldots(1)$$

Masking Hiding with (180^0) Phase Shift (M.H180)

This technique is similar to masking hiding with (0^0) phase shift technique but by quieting the stream of random numbers preshare2 file using different equation (2).

$$Stegocover2=k\times m+(k-1)\times c \quad \ldots(2)$$

The stegocover1 and stegocover2 are sent separately to the receiver side. The stegocover2 is (180^0) phase shifted in comparison with stegocover1. This difference is unnoticeable by the HVS.

The receiver side of this model is the only party which knows the relation between stegocover1 and stegocover2, in addition to transmitter side. Therefore, the image stegocover1 and stegocover2 are converted into stream of numbers.

Inside Masking Decrypting Extracting Technique (M.D.E.T), these two streams are mod added to decrypt and extract the stream of numbers secret audio message using mod-addition process inside (M.D.E.T) technique. At last, the stream of numbers extracted secret audio message is converted into audio format. The only thing that must be transmitted secretly from the transmitter side to the receiver side is (44-byte) header of secret audio message.

Results and Tests

Results

The results are calculated with following attributes:

Sample secret audio message of length (25 sec). The sample image cover (which is picture of Babylon Gate Lion) with dimensions of (1329×789) pixels.

These results are shown below:

a. Fidelity of image stegocover1:

Square Mean Square Error Ratio=0.0087%.

Mean Square Signal to Noise Ratio in dB=38.17.

b. Fidelity of image stegocover2:

Square Mean Square Error Ratio=0.0155%.

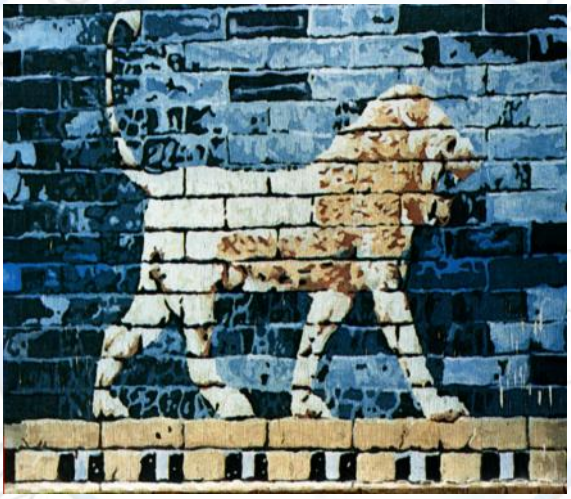
Mean Square Signal to Noise Ratio in dB=33.156.

c. Fidelity of extracted audio message:

Square Mean Error Ratio=0.6035%.

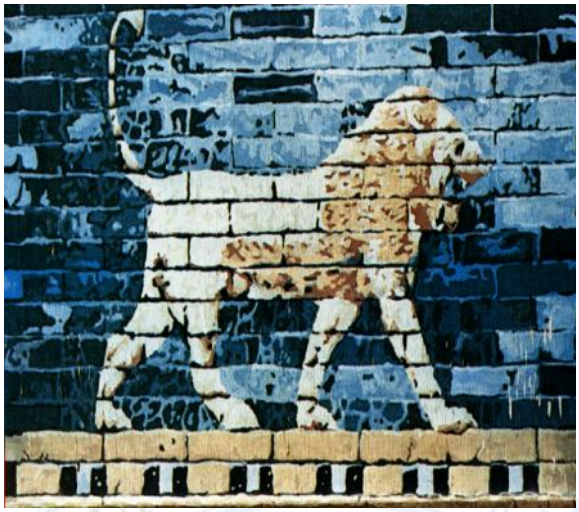
Mean Square Signal to Noise Ratio in dB=23.312.

The difference between original image cover and image stegocover1 and stegocover2 is shown in figure (4). The difference between original secret audio message and extracted audio message is shown in figure (5).



(a)

(b)

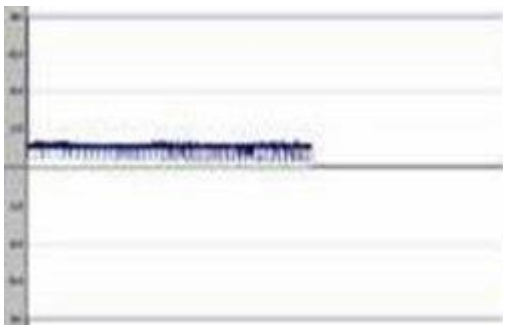


(c)

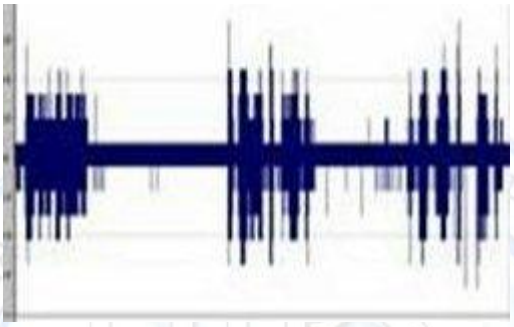
Figure (4) Proposed Model Comparison among Images of (a)Original Cover (b) Stegocover1 (c) Stegocover2

(a)

(b)



(c)



(d)

Figure (5) Proposed model Comparison among waveforms of
(a) Original Secret Speech message (b) Hidden Preshare1 in stegocover1
(c) Hidden Preshare2 in stegocover2 (d) Extracted Secret Speech message

Effect of Masking Factor on Proposed Model

These results are shown in table (1).

Table (1) Comparison Results for Proposed Model with Different Values of Masking Factor

Masking factor (k)	Cryptographic Covering				Cryptographic Extracting	
	Stegocover1		Stegocover2		Extracted Message	
	e_{rms}%	SNR_{ms} (dB)	e_{rms} %	SNR_{ms} (dB)	e_{rms} %	SNR_{ms} (dB)
k=0.9	0.257	10.117	0.325	7.9525	5.3099	-0.6823
k=0.5	0.1424	15.507	0.2629	9.8735	0.3846	27.1948
k=0.1	0.03	29.4246	0.0542	24.188	0.2853	29.8128
k=0.05	0.0153	35.3426	0.0274	30.229	0.599	23.3842

The results of table (1) are shown in figures (6).

(a)

(b)

(c)

(d)

(e)

Figure (6) Effect of Masking Factor on Proposed Model

(a) Original image and stegoimage1 when (b) k=0.9 (c) k=0.5 (d) k=0.1 (e) k=0.05

Tests

Image Conversion Test

Using proposed model with same sample tests, the image stegocover1 and stegocover2 are converted from 8-bit to 24-bit true color. The hidden audio message has not been detected in both stegos, but it could not be recovered.

Image Processing Tests

Using proposed model with same sample tests, the image stegocover1 and stegocover2 are compressed using wavelet encoder, and then decompressed using wavelet decoder. The hidden audio message has not been detected in both stegos, but it could not be recovered.

Image Printing/Scanning Test

Using proposed model with same sample tests, the image stegocover1 and stegocover2 are printed and then scanned. The hidden audio message has not been detected in both stegos, but it could not be recovered.

Conclusions

Many hiding techniques have been developed in order to secure network communications. But, the proposed system in this paper implements hardware idea (new covert cryptography) by software simulation. Therefore, we have got more secure system. Calculated results showed that the proposed system is a suitable method for hiding audio in image, because both of HAS and HVS suffer from the masking effect. However, the proposed system can be used to hide image in audio as well as audio in image, with relatively wideband method.

One important issue that must be mentioned, is masking factor which can be regarded as control factor. Therefore, it must be selected with a suitable choice.

References

1. Nedeljko Cvejic, “Algorithms For Audio Watermarking And Steganography”, Academic Dissertation, the Faculty of Technology, University of Oulu, Finland, 2004.
2. Beker H.J., "Analogue Speech Security System", Proceedings of workshop on Cryptography, Lecture Notes in Computer Science 149, Springer-Verlag, Burg Feuerstein, Germany, March 29 – April 2, 1982.
3. Fabien A.P., Ross J. A., and Markus G. K., "Information Hiding – A survey", Proceedings of the IEEE, Special Issue on Multimedia, July 1999.
4. Johnson F. N., Zoran D., and Sushil J., "Information Hiding: Steganography and Watermar king- Attacks and Countermeasures", Book from Kluwer Academic Publishers, 2001.
5. Tri L. V., "Covert Cryptography", http://www.cs.fsu.edu/~Levan/research.html, 2000.
6. Frost & Sullivan, “Audio Steganography”, Hi-Tech Security Solutions , The Journal for Security, Operations & Risk Management, produced & published by Technews ,www.technews.co.za, April 2010.
7. Naor M. and Shamir A., "Visual Cryptography", Proceedings of International Conference EUROCRYPT'94, Springer-Verlag, PP.1-12, 1995.
8. Yvo Desmedt, Shuang H., and Jean J. Q., "Audio and optical Cryptography", Proceedings of International Conference on the theory and application of cryptology and information security, China, October 1998.
9. Quisquater J.J., Desmedt Y., and Tri L. V., "Non binary Audio Cryptography", Proceedings of 3rd International workshop of Information Hiding, Dresden, Germany, 1999.
10. Yvo Desmedt and Tri L. V., "Moire Cryptography", Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece, 2000.
11. Shuang H., Desmedt Y., and Quisquater J.J., "Cerebral Cryptography", Proceedings of 2nd International workshop of Information Hiding (IH'98), USA, April 14-17, 1998.
12. Benoit M., "Visual Cryptography-A Fractal Approach", http://www.cs.rit.edu/~nrr8953/fractal.html, 2002.