Variable Length Least Significant Bits Embedding

Abbas A. Jasim

University of Basrah
College of Engineering
Computers Engineering Department

Abstract

A novel hiding system is proposed in this work which is based on Least Significant Bits (LSB) embedding of information such as speech in gray scale images.

The proposed hiding algorithm embeds the secrete information message bits in the least significant bits of the cover image pixels such that the number of secrete information bits to be embedded in least significant bits of cover image pixel is variable and determined randomly. So that cover image pixel may contain no secrete information bit, one bit, two bits , or three bits according to the pseudo random number generator that generates integer numbers randomly between 0 and 3. The resulting image (the cover image within which the secret information is hidden) is called stego_image. Stego_image is closely related to the cover image and does not show any details of the secret information. It ensures that the eavedroppers will not have any suspicion that message bits are hidden in the image and standard steganography detection methods can not estimate the locations in which the secret message bits are embedded and can not estimate the locations in which the secrete information bits are hidden nor the number of bits embedded in cover image . The proposed system achieves perfect reconstruction of the secret message.

الإخفاء متغير الطول للثنائيات الأقل تأثير

عباس عبد الأمير جاسم

جامعة البصرة–كلية الهندسة– قسم هندسة الحاسبات

الخلاصة

يتضمن البحث تصميم نظام حديث لإخفاء المعلومات معتمد على تضمين الثنائيات الأقل أهمية (LSB) يقوم بإخفاء معلومات الكلام في الصور ذات التدرج الرمادي بحيث يكون عدد ثنائيات المعلومات السرية المضمنة في كل نقطة صورية (pixel)من الصورة الغطاء(cover image) هو عدد متغير محسوب عشوائيا بالاعتماد على مولد أرقام عشوائية. و بهذا فان أي نقطة من نقاط الصورة الغطاء قد لا تحتوي على ثنائيات عائدة للمعلومات السرية أو قد تحتوي على ثنائية واحدة، ثنائيتين ، أو ثلاث ثنائيات منها. وذلك بالاعتماد على سلسلة الأرقام الشبه عشوائية المولدة والتي يكون قيمة كل رقم فيها اما 0 او 1 او 2 أو 3. تسمى الصورة الناتجة بالصورة المختزلة(stego_image) و هي عبارة عن الصورة الغطاء مخفي بداخلها المعلومات السرية.تكون الصورة المختزلة مشابهة جدا للصورة الغطاء بحيث تضمن عدم إثارة شك المتطفل الخارجي بوجود بيانات سرية مضمنة.وكذلك فان هذه الطريقة تضمن عدم تمكن طرق الكشف من تخمين مكان وجود البيانات السرية او عدد الثنائيات السرية المضمنة في كل نقطة من نقاط الصورة الغطاء. فيما يحقق نظام الاخفاء المقترح استرجاع تام للمعلومات السرية.

1.Introduction

The internet and the world wide web have made a revolution in the way in which digital data is distributed. The widespread and easy access to multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Techniques and applications for information hiding have become increasingly more sophisticated and widespread. Such applications include military and intelligence communication, covert private communication, and the protection of civilian speech against opponents [1].

Information (or data) hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright[1]. Data hiding refers to the nearly invisible embedding of information within a host data such as text, audio, image or video [2]. The process of hiding secret information in a manner such that the existence of secret information is concealed is called stagenography [3].It prevent outside observer from recognizing that hidden information is present. If a steganography method causes someone to suspect that there is secret information in the carrier medium, then this method fails [4]. So that hiding a message with stagenography reduces the chance of secret information being detected [5].

With high-resolution digital images as carriers (covers), detecting the presence of hidden messages has become considerably more difficult and messages embedded into an image are often imperceptible to the human eye [6][7]. Insignificant area of cover image can be used to embed secret data. One can replace the least significance bit of the original cover image with the secret bits and the resultant image is not distorted. For most pixels, changing the pixel values by a small amount will not be noticeable [8].

Least significant bit (LSB) embedding is very frequently used in data hiding and there are many existing data hiding techniques to insert the secret data into the least insignificant bits (LSB) of the cover image [9][10][11]. The used LSB embedding replace fixed number of bits of the cover image pixels with the secret information. The proposed hiding algorithm embeds the secrete information message bits in the least significant bits of the cover image pixels such that the number of secrete information bits to be embedded in least significant bits of cover image pixel is variable and determined randomly. The proposed algorithm is applied on speech signal as secret information.

2. Key Stream Generation

The proposed approach for hiding uses the well known key stream that is used for encryption not to encrypt information, but as random number for allocating the secret information in cover image and to determine the number of bits to be embedded in each cover image pixel. The key stream is a well known in encryption especially for stream cipher. One way for its use in encryption is done by making bitwise XOR function between the plain text and the key.

linear feedback shift registers (LFSRs) are widely used in key stream generators because they are well-suited for hardware implementation, produce sequences having large periods and good statistical properties. A (general) feedback shift register (FSR) of length L consists of L stages $[s_0, s_1, \ldots, s_{L-1}]$ (or delay elements) numbered 0, 1, ..., L − 1, each capable of storing one bit. FSR having one input and one output, and a clock which controls the movement of data. During each unit of time the following operations are performed:

(i) The content of stage 0(s_0) is output and forms part of the output sequence;
(ii) The content of stage i is moved to stage i − 1 for each i, 0< i < L ; and
(iii) The new content of stage L − 1 is the feedback bit $s_j = f(s_{j-1}, s_{j-2}, ..., s_{j-L})$.
Hence, if the initial state of the LFSR is $(s_0, s_1, ..., s_{L-1})$, then the output sequence $s = s_0, s_1, s_2, ...$ is uniquely determined by the recursion: $s_j = f(s_{j-1}, s_{j-2}, ..., s_{j-L})$ for $j > L-1$. The feedback function f is determined as :

$$f = (c_1 s_{j-1} + c_2 s_{j-2} + ... + c_L s_{j-L}) \bmod 2 \quad ...(1)$$

where each of the coefficients Ci is constant either 1 or 0 ,
f : is the feedback function which is a Boolean function, and
s_{j-i} : is the previous content of stage L_i.

For non zero initial function and primary feedback function, the LFSR will produce a pseudo random sequence of bits with period 2^{L-1} [12]. The block diagram of LFSR is shown in Figure 1.

3.Gray Scale Images Structure

In gray scale image (so called intensity image), each image is represented as a data matrix of (M×N) elements. Each element of the matrix corresponding to one image pixel. The elements in the intensity matrix represent various intensities ,or gray levels. Intensity 0 represents black, while intensity level 255 usually represents full intensity, or white.

4.The Proposed Hiding System

One of the methods that are used to hide data on an image is to replace fixed number of least significant bits (LSB) of each pixel at the cover image sequentially in the scan lines across the image in raw image format with the binary data. An attacker can easily recover the hidden message by repeating the process. To add better security, the secret message bits to be hidden are embedded as chunks of different (variable) length distributed randomly by a pseudo random number generator (PRNG) across the image. So that cover image pixel may contain no secrete information bit, one bit, two bits , or three bits according to the pseudo random number generator PRNG that generates numbers randomly between 0 and 3. In the proposed hiding system a key stream is generated as with encryption, and used as mask to distribute the secret information in the cover image and to determine the number of bits to be embedded in each cover image pixel. Simple treatment is performed on the secret key beyond using it as random number generator RNG.

4.1 The Procedure of the Proposed Hiding System

The steps of the proposed hiding approach are:

1- Generate the secrete key using the predefined key stream generators that are previously used for encryption. The key in this step is in the form of bit stream
2- Decode the secret key as two bits numbers by taking each two adjacent bits and replace them by their decimal value. For example :
K = 011100101101
PRN= 1 3 0 2 3 1
3- Arrange the resulting RNG in two dimensional form to produce RNG(i,j). Such that RNG has (M×N) numbers as the same as the image. The arrangement is implemented by take the first N numbers of 1-D RNG to form the first row of 2-D RNG then take the next N numbers of 1-D RNG to form the second row of 2-D RNG and so on.

4- Use the RNG to allocate and distribute the secret information on the cover image. As if RNG (i , j)=0, then no bit from the secret information will be embedded in pixel (i , j) in the cover image. If RNG (i , j)=1 then one bit of the secrete message bits will be replaced with the least significant bit of pixel (i , j) in the cover image. If RNG (i, j) =2, two bits of the secrete message bits will be replaced with the two least significant bits of pixel (i , j) in the cover image. And if RNG (i, j) =3,then three bits of the secrete message bits will be replaced with the three least significant bits of pixel (i , j) in the cover image.
5- Step 4 is repeated until all secret information bits are embedded in cover image. And the result is the stego_image that is the cover image within which the secret information are embedded.

4.2 The Procedure of the Reconstruction

The reconstruction steps, that reconstruct the secret information from the stego_image, are:

1- Generate the secrete key using the same algorithm used in the hiding process.
2- Decode the secret key as two bits numbers by taking each two adjacent bits and replace them by their decimal value.
3- Arrange the resulting RNG in two dimensional form to produce RNG(i,j) in the same way of hiding process.

4- Use the RNG to extract the secret information from the stego_image. As if RNG (i , j)=0, then pixel (i , j) in the cover image contain no secret information bit. If RNG (i , j)=1, then one bit from the secret information will be extracted which is the least significant bit of pixel (i , j) in the cover image. If RNG (i , j)=2, then two bits from the secret information will be extracted which are the two least significant bits of pixel (i , j) in the cover image. And if RNG (i , j)=3, then three bits from the secret information will be extracted which are the three least significant bits of pixel (i , j) in the cover image.
5- Step 4 is repeated until all secret information bits are extracted from the stego_ image.
6- Rearrange the extracted bits in the original secret information form to obtain the reconstructed information by taking each eight consequent bit to form byte of speech signal (one sample).

Figure2 shows the block diagram of the proposed hiding system.

5. The Results

The proposed hiding system is applied on digital speech signal as secret information to be hidden within the gray scale cover image. The speech signal is recorded using Cool Edit Pro software and stored as wave file. The speech signal is represented in Pulse Code Modulation PCM with sampling rate 16000 Hz and 8 bits per sample. The hiding system is to be hiding speech signal bits within the cover image pixels. The gray scale cover image can be of any size. Images that are taken in this experiment is of size (512×512) pixels. The proposed procedures are applied on several cover images and secret speech arranged in four groups two of them are shown Figures 3 and Figures 4. The secret speech is to be hidden in the cover image of the same group.

The ratio of speech signal size to image size is approximately 0.2. In (512×512) image size , 52428 (512 * 512 * 0.2) byte of speech signal can be hidden. In general, suitable image size should be used for hiding speech signal that can carry the speech signal information or more than one

image can be used to hide very long speech signal

Three factors are used to measure the similarity between the cover image and the stego_image resulting from hiding a secret speech within which. They are Mean Square Error (MSE), Energy, and correlation. The equation that is used in evaluating the energy is [13]:

$$E = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I^2(r,c) \qquad \ldots (2)$$

The MSE is evaluated as:

$$MSE = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} [I_1(r,c) - I_2(r,c)]^2 \ldots (3)$$

And the correlation equation is:

$$corr = \frac{\sum_{r=1}^{N} \sum_{c=1}^{M} (I_1(r,c) - \bar{I}_1)(I_2(r,c) - \bar{I}_2)}{\sqrt{[(I_1(r,c) - \bar{I}_1)^2][(I_2(r,c) - \bar{I}_2)^2]}} \ldots (4)$$

Where:

E: is the energy, MSE: Mean Square Error

I : is an Image,

I_1 : The cover image,

I_2 : is modified image (stego_image),

M×N: Is Image size in pixel,

and $\bar{I}$: is the mean of an image such that:

$$\bar{I} = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I \quad (r,c) \qquad \ldots (5)$$

The same three factors are used to measure the similarity between reconstructed and original secret speech. These factors are evaluated as [14][15] :

The Energy:

$$E = \frac{1}{K} \sum_{n=1}^{K} [s(n)]^2 \qquad \ldots (6)$$

The Mean Square Error:

$$MSE = \frac{1}{K} \sum_{n=1}^{K} [S_1(n) - S_2(n)]^2 \qquad \ldots (7)$$

And the Correlation equation:

$$corr = \frac{\sum_{n=1}^{K} (S_1(n) - \bar{S}_1)(S_2(n) - \bar{S}_2)}{\sqrt{[(S_1(n) - \bar{S}_1)^2][(S_2(n) - \bar{S}_2)^2]}} \ldots (8)$$

Where:

S : A speech signal

K : The size of speech signal in samples

S_1 : The original speech signal

S_2 : The reconstructed speech signal

$$\text{And} \quad \bar{S} = \frac{1}{K} \sum_{n=1}^{K} S(n) \qquad \ldots (9)$$

Table 1 lists the MSE between cover and stego_image, the correlation between cover and stego_image, the energy of cover image, and stego_image energy for the four groups.

Table 2 listing the MSE between reconstructed and original secret speech, the correlation between reconstructed and original secret speech, energy of secret speech , and reconstructed speech energy for the four groups.

6. Conclusions

The procedure of the proposed information hiding system has a good algorithm to hide speech or any information within gray scale images. The secrete information message bits are embedded in the least significant bits of the cover image pixels such that the number of secrete information bits to be embedded in least significant bits of cover image pixel is variable and determined randomly. So that cover image pixel may contain no secrete information bit, one bit, two bits, or three bits according to the pseudo random number generator that generates numbers randomly between 0 and 3. For this reason, it provides high level of security since

external eavesdropper can not estimate the location of secrete information bits nor the number of secret information bits that are embedded within any cover image pixel. The result stego_image is very close to the cover image so that outside observer cannot recognize that the hidden (secret) information is present. This can be shown from Table 1, since the values of the energy of the stego _image and the cover image in each group is very close, MSE is very small, and the correlation between cover and stego image is very closed to 1. The proposed approach ensure perfect reconstruction of the secret information since the MSE between the secret speech and reconstructed speech is 0 for all the four groups as shown in Table 2. Other measures of similarity are the energy, which is the same for each of original and reconstructed speech, and the correlation which is equal to 1 that indicates the perfect reconstruction of the hidden information.

8. References

[1] W. Bender , W. Butera , et al , "Applications for data hiding", IBM Systems Journal ,Vol. 39, pp 547-568,2000

[2] W. Niblack, et al., "The QBIC project: querying images by content using color, texture, and shape," Proc SPIE, Storage and Retrieval for Image and Video Database, vol. 1998, pp. 173-187, Feb. 1993.

[3] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2001

[4] D. Artz, "Digital Steganography: Hiding Data within Data" ,IEEE Internet Computing, pp. 75-80, May-June 2001.

[5] F. N. Jhonson , Z. Duric , and S Jajodia , "Information Hiding : Steganography and Water Marking Attacks and Counter Measured", Klwer Academic Publishers,2001 .

[6] N. Provos. "Defending against statistical steganalysis. In 10th USENIX Security Symposium", Washington, DC, 2001.

[7] A. Westfeld and A. P_tzmann." Attacks on steganographic systems. In Proceedings of Information Hiding", Third International Workshop, Dresden, Germany, 1999.

[8] Min Wu, and Bede Liu "Data Hiding in Binary Image for Authentication and Annotation", IEEE Transaction on Multimedia, pp 528-538, August 2004.

[9] W. Bender, et al., "Techniques for Data Hiding", Proc. of SPIE Conf. on Storage and Retrieval for Image and Video, Vol. 2420, pp. 40, Feb. 1995.

[10] N. Nikolaidis, I. Pitas, "Copyright Protection of Images using Robust Digital Signatures", Proc. of, IEEE Int. Conf. on Acoustics, Speech, Signal Processing, Vol. 4, pp. 2168-2171, May 1996.

[11] P.H.W. Wong, O.C. Au, et al., "Image Watermarking Using Spread Spectrum Technique in Log-2-Spatio Domain", Proc. of IEEE Int. Sym. on Circuits & Systems, Jun. 2000

[12] A. Menezes, P. vanOorschot, and S. Vanstone, "Handbook of Applied Cryptography" , CRC Press, 1996.

[13] H. H. Al _Obaidy ,"Encryption Using Wavelet Coded Image Data", MSc Thesis,

Computer Engineering Department ,College of Engineering ,University of Basrah,2004.

[14] R. E. Ziemer, " Signals and Systems: Continuous and Discrete ", Fourth Edition, Prentice Hall, 1998.

[15] L. Rabinar and R. W. Schafer," Fundamental of Speech Recognition ", Prentice Hall 1993.

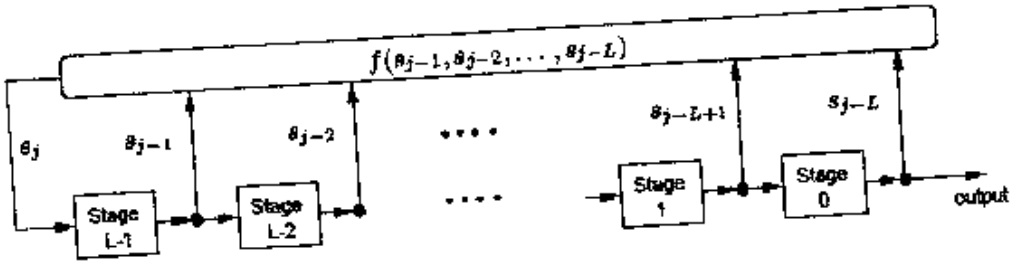
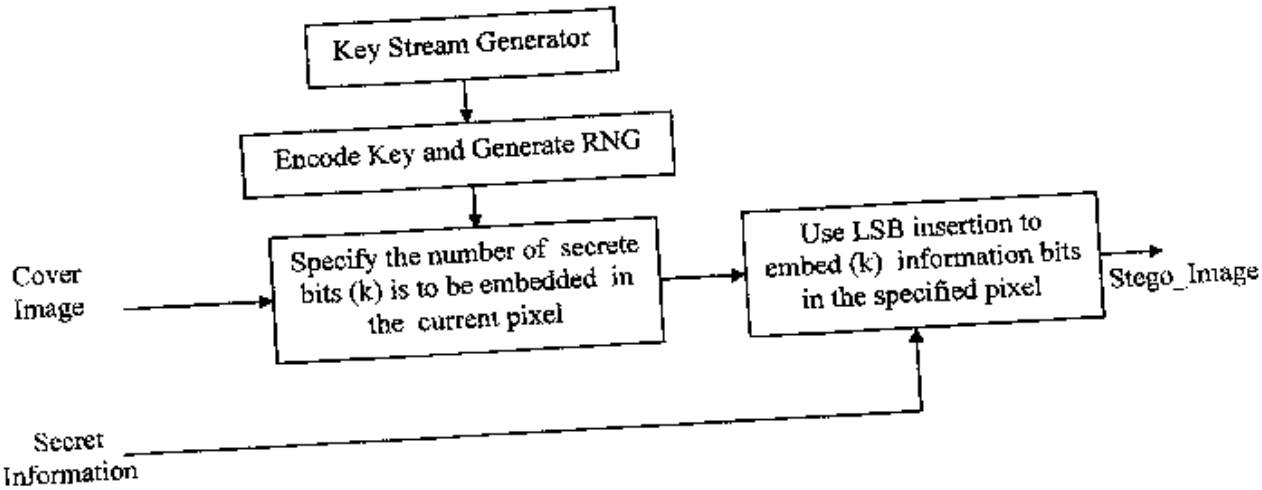
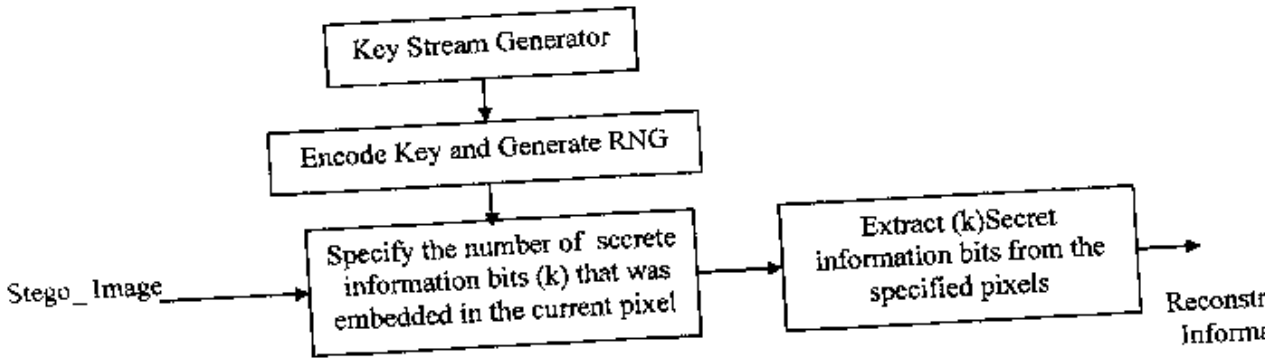


Figure 1: The Block Diagram of LFSR Key Generator

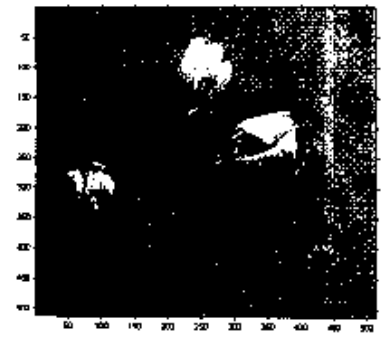


a- Embedding

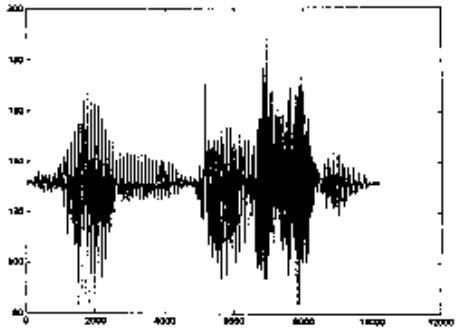


b- Reconstruction

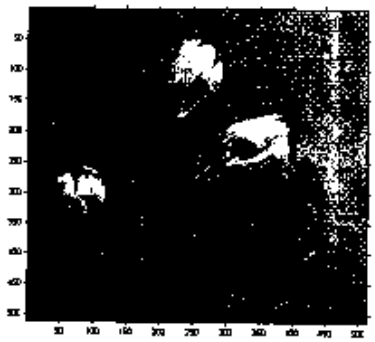
Figure 2: The block diagram of the proposed hiding System



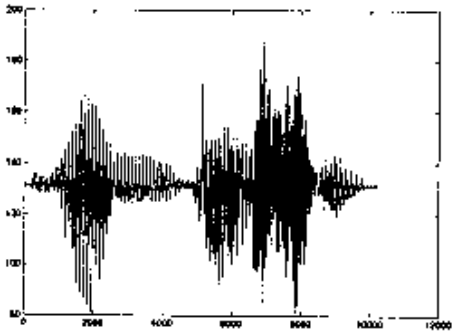
a- Cover Image



b- Secret Speech

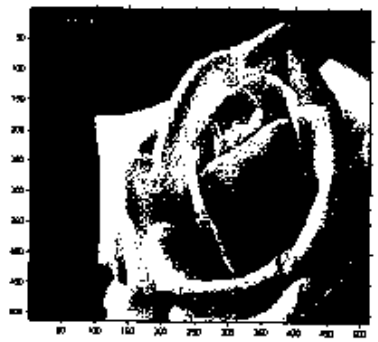


c- Stego_ Image

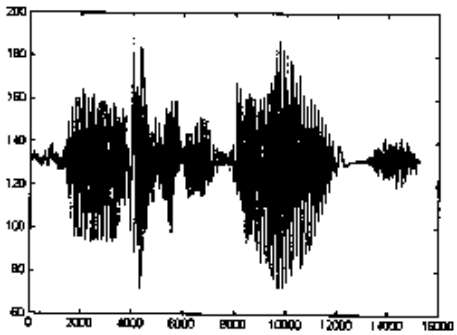


d- Reconstructed Speech

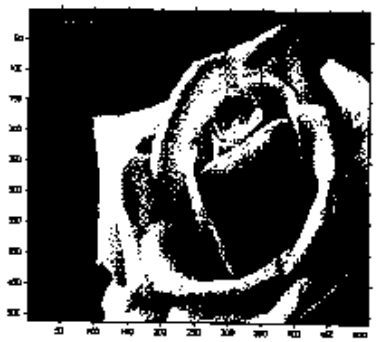
Figure 3: Group1 Cover Image , Secret Speech, stego_image and Reconstructed Speech



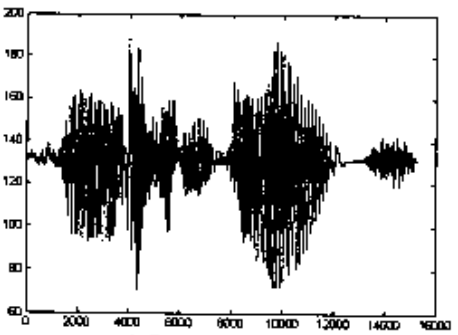
a- Cover Image



b- Secret Speech



c- Stego_ Image



d- Reconstructed Speech

Figure 4: Group2 Cover Image , Secret Speech, Stego_image and Reconstructed Speech

Table 1

Group	MSE between Stego_Image And Cover Image	Correlation Between Stego_Image And Cover Image	Cover Image Energy	Stego_Image Energy
Group 1	$8.656268209642773\times 10^{-6}$	0.99999999999976	0.45424024717552	0.45403689556402
Group 2	$6.029362955353782\times 10^{-6}$	0.99999999999982	0.49841437615850	0.49819690667654
Group 3	$2.896940648579218\times 10^{-6}$	0.99999999999986	0.28430493523096	0.28437847455712
Group 4	$4.991284245392803\times 10^{-6}$	0.99999999999989	0.33397306437124	0.33416815517589

Table 2

Group	MSE Between Secret and Reconstructed Speech	Correlation Between Secret and Reconstructed Speech	Secret Speech Energy	Reconstructed Speech Energy
Group 1	0	1	0.00771577092711	0.00771577092711
Group 2	0	1	0.00608293740893	0.00608293740893
Group 3	0	1	0.00175659456490	0.00175659456490
Group 4	0	1	0.00273766803881	0.00273766803881