Encrypting Audio Data Hiding by Visual Secret Sharing

Dr. Nidaa F. Hassan* , Dr. Rehab F. Hassan*
& Akbas E. Ali *

Received on:1/4 /2009
Accepted on: 3/ 9/2009

Abstract

Steganography and cryptography are usually used to ensure information safety in today's data communication. This paper makes use of audio steganography technique and encrypted secret sharing to increases the security level of hidden data. The proposed schema can hide digital data in audio file; the resulted stego audio file is separated then into 2- shares encrypted random secure images, which can be transmitted or distributed separately over an threaten communication channel. Using multilevel of security techniques increases the security level of hidden data, and makes it more robust to attack since secret data is not hidden in one cover media but it is separated across two images, that they will be encrypted and appear completely random.

Keywords: Steganography, cryptography, visual cryptography, secret share, random images.

تشفير البيانات المخفية في الصوت باستخدام التقسيم السري المرئي

الخلاصه

علم الاخفاء والتشفير يستخدمان عادة لتأمين أمنية المعلومات في اتصالات الوقت الحاضر. هدا البحث يستخدم تقنيه اخفاء البيانات والتقسيم السري المشفر لزياده مستوى الامنيه للبيانات المخفيه . الطريقه المقترحه ممكن ان تخفى نوع من البيانات الرقمية في ملف صوت, بعدها يتم تقسيم الملف الصوتي المضيف الى اثنان من الصور العشوائيه المشفره والتي من الممكن ارسالها او توزيعها بشكل منفصل عبر قنوات الاتصال التي من الممكن ان تكون غير امنيه او معرضه للاختراق. ان استخدام مستويات متعدده من التقنيات الامنية تزيد من مستوى الامنية للبيانات المخفية وتجعل هده البيانات صامدة ضد الاختراق لانها ليست مخفيه في غطاء واحد فقط وانما قسمت ووزعت على صورتين والتي بالنتيجه ستكون مشفرة وعشوائية الشكل .

1. Introduction

The growing possibilities of modern communications require a special means of confidential and intellectual property protection against unauthorized access and use. Steganography and Cryptography provide important tools for the protection of information and they are used in many aspects of computer security.

Steganography is not to keep others from knowing the hidden information; it is to keep others from thinking that the information even exists. Cryptography encodes data such that an unintended recipient cannot determine its intended

* Computer Sciences Department, University of Technology / Baghdad

PDF created with pdfFactory Pro trial version www.pdffactory.com

meaning. Steganography, in contrast, does not alter data to make it unusable to an unintended recipient [1].

In digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Together they are excellent means to accomplish this, but neither technology alone is perfect, where it can be broken. For this reason most experts suggest merging these two techniques in different ways to add multiple layers of security [2].

Visual Cryptography is a type of cryptography which encodes a number of images shares in a way that when theses images are stacked on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is done directly by the human visual system with no special cryptographic calculations [3].

2. Steganography

Steganography, coming from the Greek words stegos, meaning roof or covered and graphia which means writing, it is the art and science of hiding the fact that a communication is taking place. Using Steganography, you can embed a secret message inside a piece of unsuspicious information and send it without letting anyone knows the existence of the secret message. Secret messages could be hidden inside any sorts of cover information: text, images, audio, video and more. Most steganographic utilities nowadays, hide information inside images, as this is relatively easy to implement [4].

2.1 Hiding Data in Audio

Hiding data in audio, exploits how the human auditory system (HAS) interprets sounds. This method becomes especially challenging, since the HAS is extremely sensitive. The goal of Steganography in audio is to exploit this weakness. Bits that encode sound outside the range of human hearing can be encoded with covert data. The following paragraphs discuss steganographic methods using audio.

1. Low-bit encoding encodes a binary string in the least significant bit (LSB) of an audio file.
2. Phase coding substitutes the phase of an audio segment with a reference phase that represents the data.
3. Spread-spectrum encodes streams of information by spreading data across as much of the frequency spectrum as possible.
4. Echo data hiding embeds data into a host audio signal by introducing an echo [5].

As mentioned previously, Steganography is an effective means of hiding data, thereby protecting the data from unauthorized or unwanted viewing, but it's best to be used in conjunction with cryptography. Such a combination increases the security of the overall communication process, as it will be more difficult for an attacker to detect embedded secret

PDF created with pdfFactory Pro trial version www.pdffactory.com

message.

3. Visual Cryptography (VG)

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [6].

Secret Sharing Scheme is a method of distributing a secret data among a set of participants so that only qualified subsets are able to recover the data. Shamir and Blakly independently introduced (k, n)-threshold schemes (Blakly, G.R., 1979; Shamir, A., 1979) in which a secret S is distributed to n participants in such a way that k or more participants can recover the original secret S and k - 1 or fewer participants have no information on S. (A piece of information held by a participant is called his share.) A special kind of secret sharing scheme is visual cryptography scheme (VCS) [7].

The visual cryptography scheme is a perfect secure method that encrypts a secret image by breaking it into shadow images. A distinctive property of VCS is that one can visually, without computation, decode the secret by superimposing shadow images [8].

Visual Cryptography was proposed by Naor and Shamir in 1994[9], Naor and Shamir devised the scheme, illustrated in the figure (1), this figure explains how to encode a single pixel, and it would be applied for every pixel in the image to be shared. A pixel P is split into two sub pixels in each of the two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row. Every pixel is encrypted using a new coin toss .

So visual cryptography scheme "splits" the original image into two "shadow images" called "shares." Every pixel in the original image is expanded to a 2x2 pixel matrix with a different version in any of the two shares. Any share contains uniformly distributed random black-and-white pixels. By analyzing only a single share, you can't obtain information about the original image, no matter how much computing power or analysis method is used. The whole point of visual cryptography is that in the decryption process, the original image has to be visually reconstructed. Each share is printed on a separate transparency and passed to a participant at the scheme. When the two participants come together, the secret can simply (and theoretically instantaneously) be reconstructed by stacking the two transparencies. Figure (2) is an example of the visual cryptography scheme [10].

4. The Proposed Secret Sharing Schema

In this research, a new schema is proposed which concentrates on adding more secrecy to the hidden

PDF created with pdfFactory Pro trial version www.pdffactory.com

data, it makes use of one of the audio steganography method and visual encrypted sharing scheme, that generates encrypted random image shares from the stego file. Several steps have been taken to provide more than one layer of security to protect secret information from being accessed by an unauthorized user. The secret data is passed through the following stages:

- **a.** Embedding Process: Embedding of the secrete data into an audio file and constructing of stego audio file.
- **b.** Splitting Process: Splitting the resulted stego cover into two random image shares.
- **c.** Extracting Process: Extracting the original data and regenerating the original audio file.

After applying step (b) the resulted image shares will be transferred to the destination as a separate image, so it would be impossible to regenerate the original data from one share, the destination should get the two shares images together.

4.1 Embedding Process

At this stage, the secret data is embedded in an audio media file (.WAV), where the following sub stages will be followed:

1. Secret message is converted to binary form.

2. The header of the original audio file (cover) is extracted. Then the audio data cover will be loaded into Wav vector to be ready for embedding process.

3. The bit stream of secret data is embedded within audio data cover using Least Significant Bits (LSB) technique. This approach is justified by the simple observation that changing the LSB results in the smallest change in the value of the byte. The advantages of this method are it's simplicity to be understood, and a binary sequence with high data rate could be embedded, but the hidden data can be easily destroyed and detected. This disadvantage of LSB technique is overcomes by secret sharing schema.

Three types of audio files (speech, song and music) are used as host files, where a secrete data equal to 4,096 bytes are embedded in these three types of file, and because of using the LSB technique for embedding, no big difference can be notice at the files before and after the embedding process. Figure (3) shows the audio cover file signals before and after embedding secret data.

4.2 Splitting Process

The obvious limitations of LSB are overcome in this research by adding one of the cryptography techniques, to ensure strength of the secure communication; n – secret sharing concept which is derived from visual cryptography is applied to the stego cover file.

The stego cover which is constructed by embedding secrete data within audio file is splitted into 2- shares of random digital image (.BMP), so that getting one of the images by any intruder will not be useful to him unless getting

PDF created with pdfFactory Pro trial version www.pdffactory.com

the second image, and knowing the construction algorithm and the type of masks used to reconstruct the audio file and regenerate the secrete message. The proposed schema make use of the idea of visual cryptography that proposed by Naor and Shamir [Nao95], but it uses a different and special method of splitting the original audio file into two random images shares. These random images are:

1. Visually decoded by superimposing a qualified subset of shares, but no secret information can be obtained from the superposition of a forbidden subset
2. Carrying, both, significant secret information.

   The split process is implemented using two masks, Mask1= 15 and Mask2 =240, these two masks are ANDed with two successive bytes of stego audio file as follows:

4.3 Extracting Process.

The two participants share random images obtained from pervious stage send to receiver thorough a communication channel. The receiver must obtain the two participants share random images together to obtain and reconstruct the secret data. This module is used for extracting stego audio file, and it consists of the following steps:

1. Extraction of stego audio file by mixing the received 2-shares random digital image in the same way of the shares construction i.e., by using the same two masks, where mask1=15 and mask2=240, and applying the following steps:

a. Each two successive byte of stego-cover is converted into Binary stream,.

b. These two successive binary streams are ANDed with Mask_1, and then is ANDed with Mask_2 interchangeably, The output of masking process is merged in a crossover manner to produce new two successive bytes

c. The first merged byte is stored in the first share random image, while the second merged byte is stored in the second share random image. The size of the resulting 2-shares image is half the size of the stego-cover. Figure (4) and Algorithm (1) illustrates this process.

Different masks could be applied in different ways to get different image sharers.

a. Get the current byte of the first image share and the second image share.

b. Each one of the two bytes are ANDed with Mask_1, and then is ANDed with Mask_2 interchangeably, The output of masking process is merged in a crossover manner by using XOR to produce new two bytes

c. The resulted two bytes are entered at the current position in the audio file; these three steps are repeated until reaching the end of the images shares.

2. Extraction secret stream of bits from stego audio file by extracting the low significant bit form each byte of stego

PDF created with pdfFactory Pro trial version www.pdffactory.com

file. This stream of bits is converted to ASCII code to produce secret data.

Algorithm (2) shows the main steps of the extraction process, an example of the extraction process is explained in Figure(5), which is an inverse of the split process shown in Figure(4). Figure (6) shows the general diagram of the proposed schema provide additional layer of security by applying new algorithm that separates the host audio file into two encrypted image, there are some issues to be discussed here:

1. The secret data can not be extracted unless the receiver knows masks configuration, and the 2- share random images together must be existed.
2. JPEG compression attack was applied on the 2-share images,

5. Security Issues and Future Works

The proposed schema provide additional layer of security by applying new algorithm that separates the host audio file into two encrypted image, there are some issues to be discussed here:

1. The secret data can not be extracted unless the receiver knows masks configuration, and the 2- share random images together must be existed.
2. JPEG compression attack was applied on the 2-share images, where
3. The result secret data can be relieved correctly after converting JPEG images to BMP images.

The idea of the secret sharing schema can be extended along

where the result secret data can be relieved correctly after converting JPEG images to BMP images.

3. Using different masks in different configurations results in different shares with different level of encryption and randomness.

The idea of the secret sharing schema can be extended along several interesting directions, among these are:

1. Improving the hiding techniques by applying hiding in frequency domain which adds another layer of security.
2. Hiding different type of multimedia such as (Audio, Images and even video), so the schema isn't limited by hiding text only.

several interesting directions, among these are:

1. Improving the hiding techniques by applying hiding in frequency domain which adds another layer of security.

2. Hiding different type of multimedia such as (Audio, Images and even video), so the schema isn't limited by hiding text only.

3. Improving the suggested algorithms to survive against other types of attacks.

6. Conclusions

This paper proposes a scheme to hide secret data in Audio file. The hiding process is based on the idea which is derived from secret sharing of visual cryptography. The secret data is hidden in stego

PDF created with pdfFactory Pro trial version www.pdffactory.com

audio file; this stego file is separated into the 2-share random images according to a new proposed algorithm, which is very simple to implement. The proposed scheme is effective in protecting information from unwanted parties, since the binary patterns obtain of one share image have no meaning, unless the second share image is mixed with first one.

7. References

[1] Donovan Artz," Digital Steganography: Hiding Data within Data", IEEE Internet Computing, 2001.

[2]Dunbar B., "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", SANS Institute 2002.

[3] Giuseppe Ateniese, Carlo Blundo, AlfredoDe Santis, and Douglas R. Stinson, "Extended capabilities for visual cryptography", Theoretical Computer Science,250:143–161, 2002

[4] Krenn J. R., "Steganography and Steganalysis", School of Technology & Computer Science, Tata Institute of Fundamental Research, India, January 2004.

[5] Whitiak D., "Art of Steganography", SANS Institute 2003, as part of GIAC practical repository.

[6] Alfred J. M., Paul C. O. and Scott A. V. "Handbook of Applied Cryptography ", fifth Addition, 2001.

[7] Massoud H. Dehkordi 1 and 2Abbas Cheraghi,"Visual Cryptography Schemes with Veto Capabilities", Australian Journal of Basic and Applied Sciences, 2(4): 1239-1245, 2008
ISSN 1991-8178.

[8]Ching-Nung Yang*, Chung-Chun Wang and Tse-Shih Chen ," Visual Cryptography Schemes with Reversing", Computer Journal ,National Dong Hwa University, Department of Computer Science and Information Engineering, Taiwan,2008 .

[9] Naor M. and Shamir A., "Visual cryptography", Advances in Cryptogoly Eurocrypt '94, Lecture Notes in Computer Science, vol. 950, pp. 1-12,Springer-Verlag, Berlin,1995

[10] Daniel Stoleru," Visual cryptography and bit-plane complexity segmentation", Video Imaging Design Line, Teconline Community,2007.

PDF created with pdfFactory Pro trial version www.pdffactory.com

Algorithm (1) Generate two share random images from audio file.

Input : Stego audio file, Mask_1=15, Mask_2=240.
Output : Two share random image (Share-1 & Share-2) .

```
Step 1 : Open stego file (cover) as cover file for reading,
         Open Share_1 (image) as cover file for writing,
         Open Share_2 (image) as cover file for writing.
Step 2 : Set Len_stego  to the length of the stego file .
Step 3 : For I = 0 to Len_steg step 2
              Byte_1= Wav (I):      Byte_2= Wav (I+1)
              Convert Byte_1, Byte_2 to binary stream Bin_1 and Bin2.
              Bin_11=Bin_1 AND Mask_1:   Bin_12=Bin_1 AND Mask_2
              Bin_21=Bin_2 AND Mask_1:   Bin_22=Bin_2 AND Mask_2
              Bin_3 = Bin_1 OR Bin_22
              Bin_4 = Bin_12 OR Bin_2
              Convert Bin_3 and Bin_4 to an ASCII code
              Write Bin_3 into Share_1 image : Write Bin_4 into Share_2 image
         Next I
```

Algorithm (2) Extract secret data from 2-Share random images.

Input : Two share random image (Share_1 & Share-2).
Output : Secret Data .

```
Step 1 : Open Share_1 (image) as cover file for reading.
         Open Share_2 (image) as cover file for reading.
         Open stego file (cover) as cover file for writing.
Step 2 : Set Len _Share  to the length of the Share_1 image file .
Step 3 : For I = 0 to Len _Share
              Byte_1= Share_1 Image (I) :Byte_2= Share_2 Image (I)
              Convert Byte_1, Byte_2 to binary stream Bin_1 and Bin2.
              Bin_11=Bin_1 AND Mask_1:   Bin_12=Bin_1 AND Mask_2
              Bin_21=Bin_2 AND Mask_1:   Bin_22=Bin_2 AND Mask_2
              Bin_3 = Bin_11 OR Bin_22
              Bin_4 = Bin_21 OR Bin_12
              Convert Bin_3 and Bin_4 to ASCII code
              Write Bin_3 into Stego Audio file.
              Write Bin_4 into Stego Audio file.
         Next I
Step 4 : Open Stego Audio File for reading.
Step 5 : Parse the header of the stego file.
Step 6 : Extract stream of hidden bits.
Step 7 : converted to secret data.
```

PDF created with pdfFactory Pro trial version www.pdffactory.com

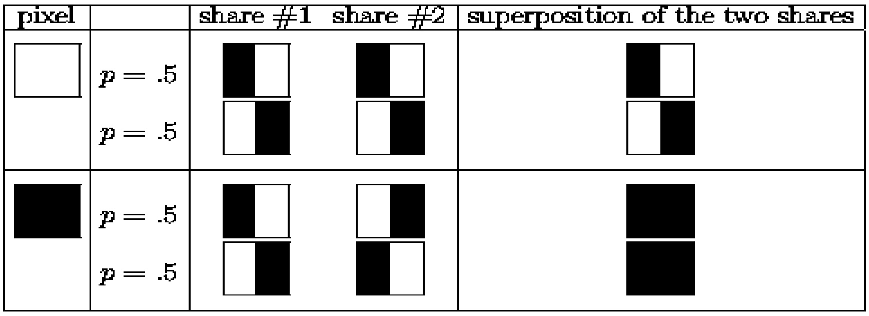


Figure (1): Naor and Shamir devised Visual Cryptography [10].

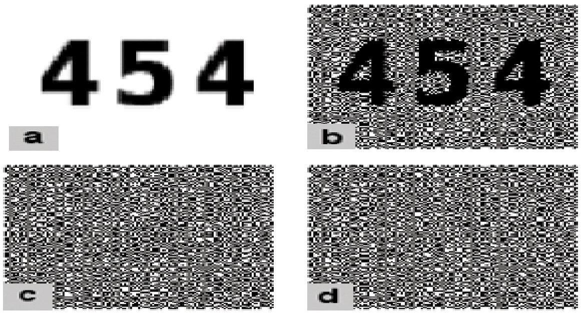
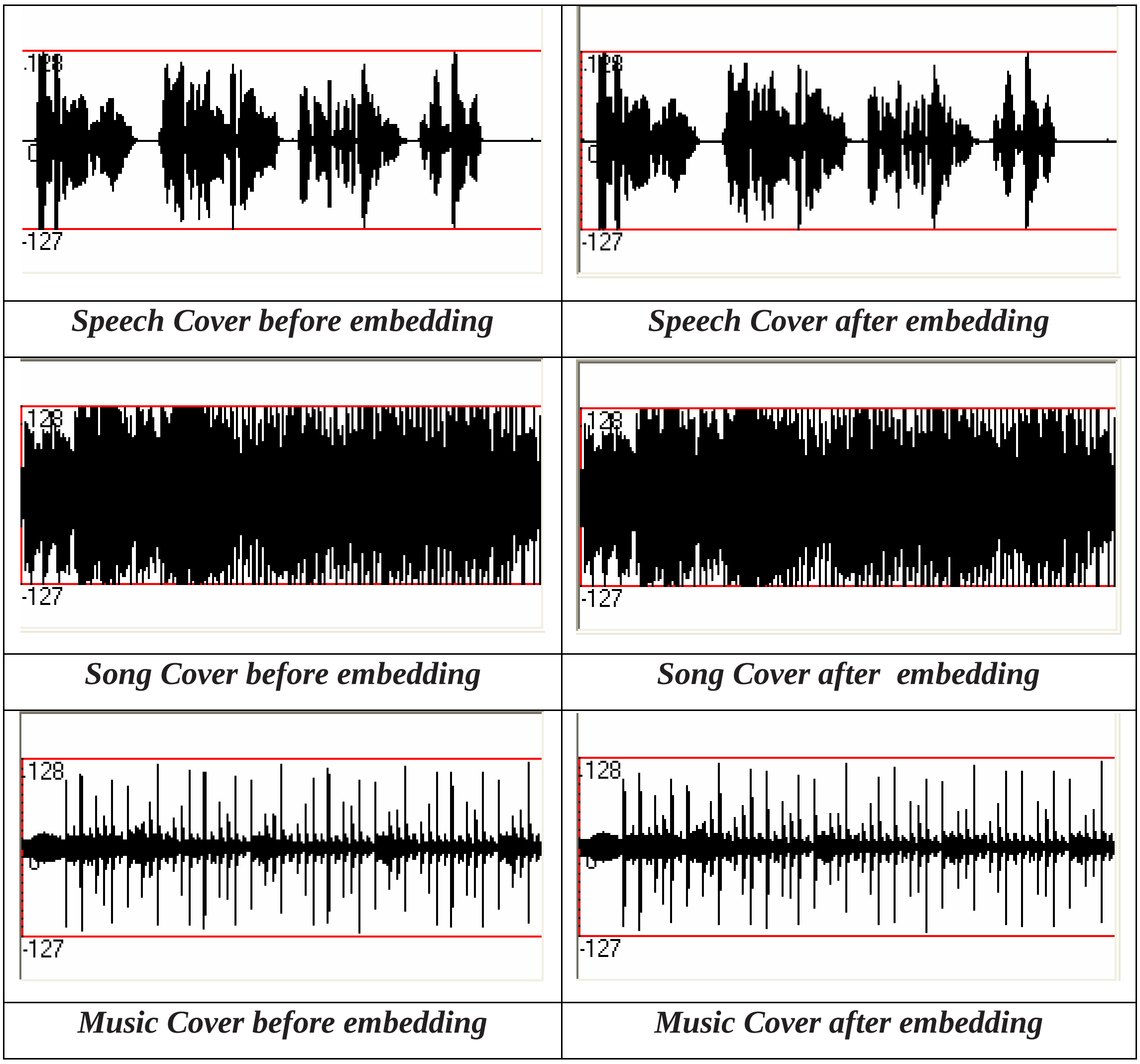


Figure (2): (a) Secret message; (b) Recomposed message; (c) First share; (d) Second share [10].

PDF created with pdfFactory Pro trial version www.pdffactory.com



Speech Cover before embedding

Speech Cover after embedding

Song Cover before embedding

Song Cover after embedding

Music Cover before embedding

Music Cover after embedding

Figure (3): Audio files Signal Before and After Embedding Process.

PDF created with pdfFactory Pro trial version www.pdffactory.com

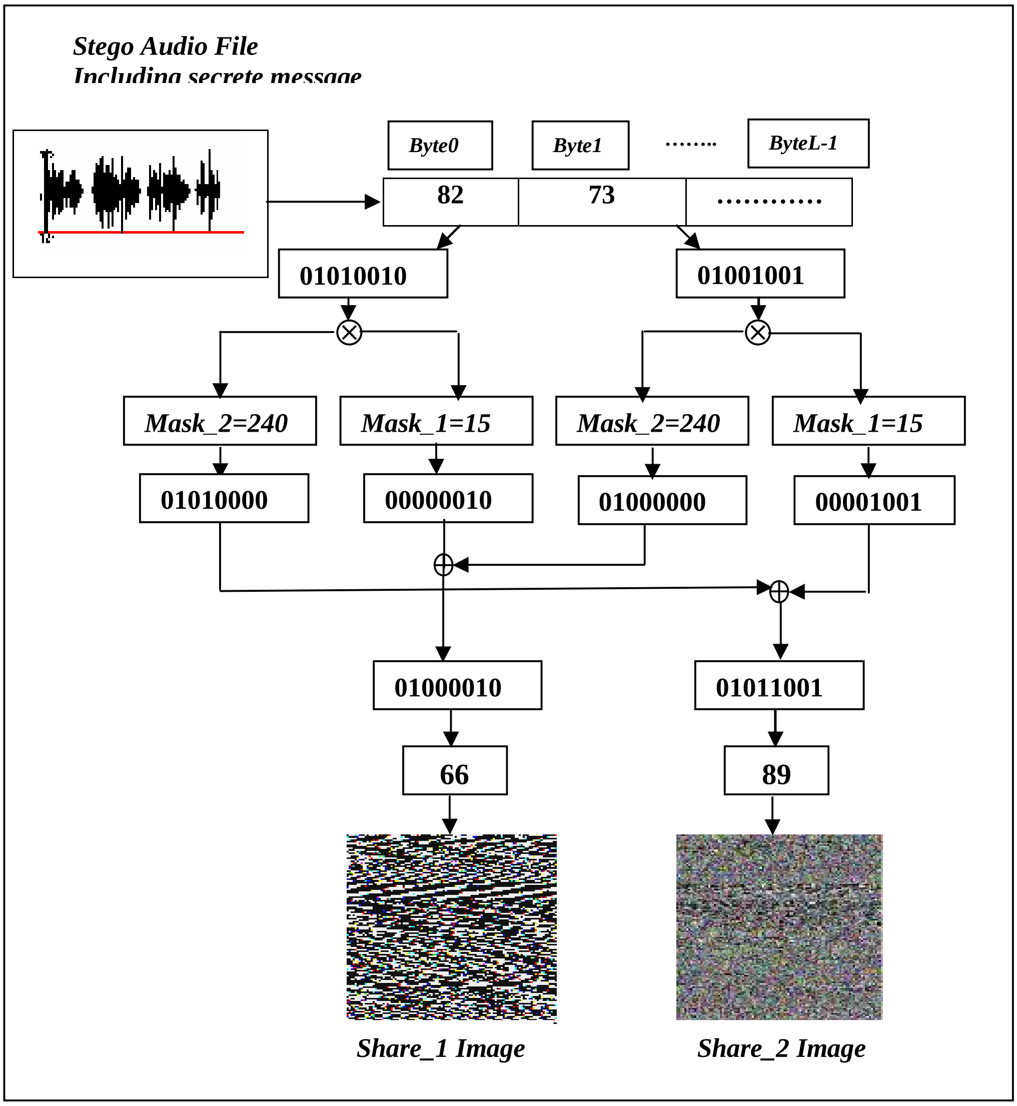


Figure (4): Example of Splitting Stego cover into 2-share two random images

PDF created with pdfFactory Pro trial version www.pdffactory.com

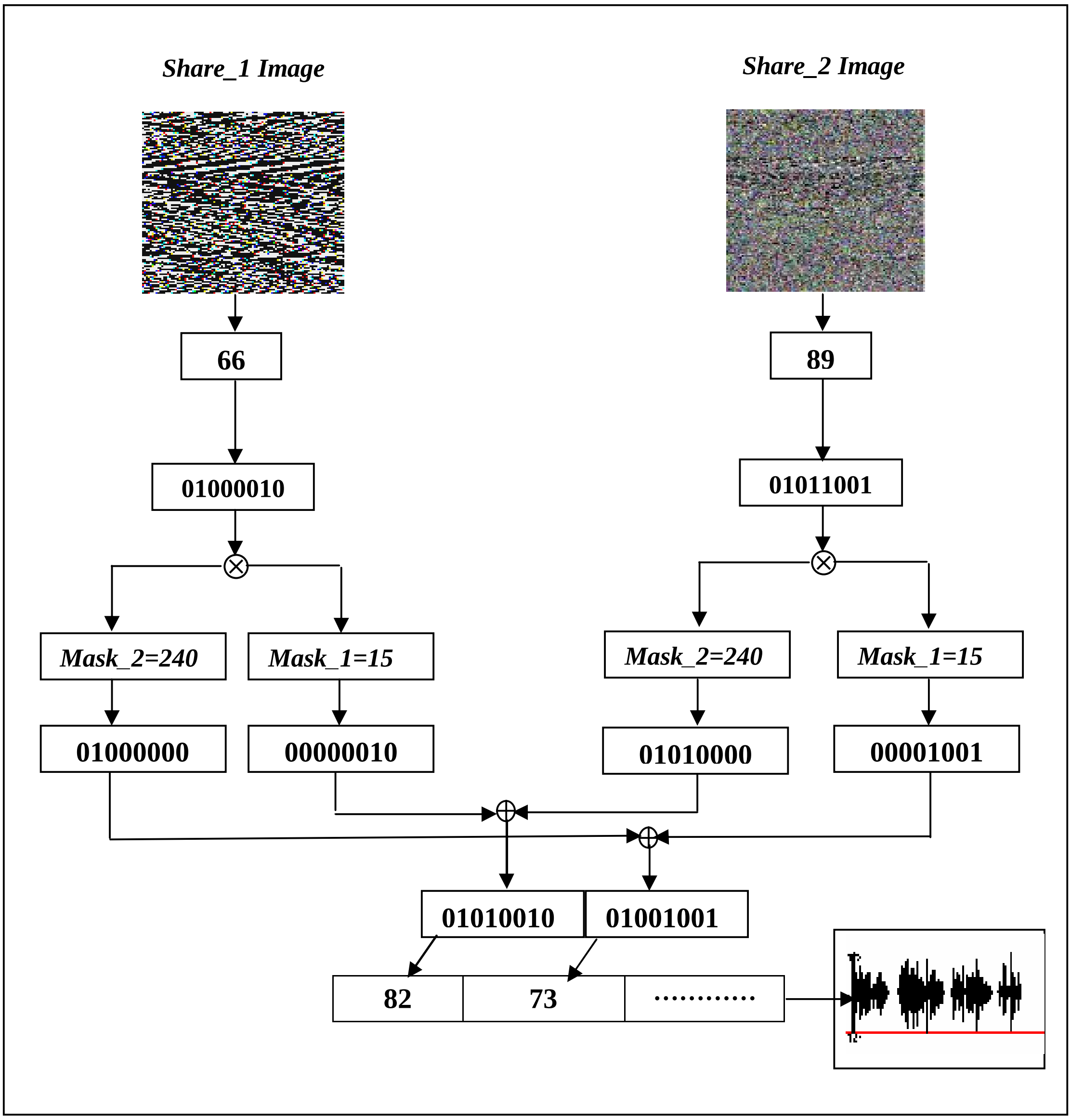


Figure (5): Example of Extraction process

PDF created with pdfFactory Pro trial version www.pdffactory.com

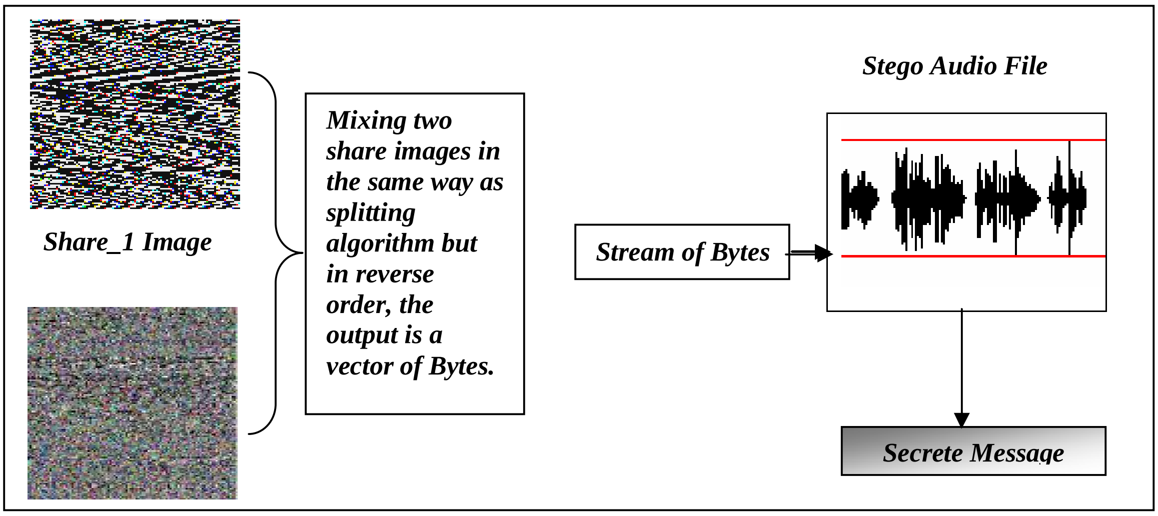

Share_1 Image
Mixing two share images in the same way as splitting algorithm but in reverse order, the output is a vector of Bytes.
Stream of Bytes
Stego Audio File
Secrete Message

Figure (6): General Diagram of Extraction Process.

PDF created with pdfFactory Pro trial version www.pdffactory.com