Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 10 (2017) pp. 2973-2983
© Research India Publications
http://www.ripublication.com

Steganography: A method To Hiding the Binary Text in Wave File

Dr. Mustafa Raheem Neamah

Computer Science and Information Technology College,
Wassit University , Wassit, Iraq.

Abstract

Steganography has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. In This research it we will explore steganography from its earliest instances through potential future application. In this research the uses of the a algorithm to load and hide data.

Keywords : Memory card , Personal Computer , Human visual system , Discrete cosine transform , Bitmap , Graphics interchange format , Hypertext Markup language , Human auditory system .

1.1 introduction

At the point when people borne, extraordinary and mystery things and data are borne with them. Some of these mystery data should be transmitted between them. These requirements invigorate the question about how mystery data can be transmitted between individuals without find. Likewise, when wars happened on the planet, the mystery key information had expanded, and the systems to ensure these information are produced. These days, two sorts of procedures were utilized to cover data, they are: Encryption and data stowing away(Files 2010)

The significance of these two assurance strategies was tremendously expanded since the disclosure of phone, fax, electronic correspondence and PC. Likewise its significance was detonated when the web enter individuals lives and turn into the best, quick and normal approach to correspondence on the planet. Web gives the offices to trade content, picture, sound, and video amongst clients, and it's get to achieve touchy areas (like, military areas, political areas) for every administration on the planet, likewise it is the most open approach to interface with vast organizations and banks in world. Every one of these realities energized a few people (or organizations) to created approaches to take data, and to get a few apparatuses (programming) to make un-approved access to shut areas. Still, it is basic issue to secure interactive media substance against unlawful utilize, such computerized substance can be effortlessly replicated or altered on a PC and conveyed through the system by outsider without consent of the copyright proprietor(Bassil 2012). With a specific end goal to tackle this issue, information covering up has got awesome consideration as a promising strategy that assumes a corresponding part to the ordinary cryptographic procedures.

1.2 Information Hiding

Now and then it is preferred concealing messages rather over enciphering them. Actually, the primary reason for cryptography is to make message limitless, so that individuals, who don't groups mystery keys, can't recuperate the message, instead the information concealing uses parallel documents with certain level of immateriality and repetition to shroud information(Of and Education n.d.). Advanced books, pictures, recordings, and sound tracks are perfect for this reason Digital representation of signs conveys many favorable circumstances when contrasted with simple representation and these points of interest are:

1. Lossless recording and duplicating.
2. Advantageous conveyance over system.
3. Simple altering and change.
4. Effortlessly searchable recorded.
5. Sturdy.
6. Shoddy.

Against these preferred standpoint some major issues were showed up:

1. Far reaching copyright infringement.
2. Illicit replicating and appropriation.
3. Dangerous confirmation.
4. Simple producing.

The general meanings of concealing information in other information can be described as takes after: the implanted information is the message that a man wishes to send furtively. This message must be hidden in an ordinary message as a cover-content, or cover-picture, or cover-sound, or by and large a cover-question, creating the stego-protest or the checked protest. Specifically,(Allteef 2007) a stego-key is important to control the concealing procedure, to limit recognition and recuperation of the installed information to un-approved individuals. The concealed information may have no association with (or may give essential data about) the cover-protest, in which it is, inserted.

1.3 problem statement

The aim of this work implement hiding software, which is able to protect the messages in network environment .This system based on hiding these messages in audio files by least significant bit (LSB) jumping algorithm technique.

1.4 Steganography

Steganography is one of the classes (applications) of data hidings.(Sewisy and Mohammed 2015) The word steganography is elusive in any lexicon. It originates from the Greek word "steganos" (implies secured) and the "graphy" (implies composing), so steganography actually signifies" secured composing".(Atoum, Rababah, and Al-attili 2011) This means to transmit a message through a channel where some different sorts of data are as of now being transmitted. The general standard of steganography is delineated in figure (1), from this figure the following definitions are needed to understand the involved components of any steganography system

l. Cover Medium: is the host medium in which the mystery information is shrouded, it can ba honest looking bit of data, or some essential media that must be ensured against copyright or trustworthiness reasons.

Spreads should contain information that uninteresting to the adversary and will be probably not going to be liable to any kind of investigation Also, cover ought to never utilized twice, since an assailant who has admittance to the two adaptations of the cover can without much of a stretch distinguish and recreate he shrouded message. To keep away from inadvertent reuse, both sender and beneficiary ought to pulverize all spreads they have effectively utilized for data exchange(Pitropakis and Lambrinoudakis n.d.)

2. Embedded Message: is the shrouded message that needs to be placed in the cover. It could be a few information for steganography copyright data, or some additional substance for computerized watermar3. Stego Key: It is spoken to by some mystery data, which is Needed with a specific end goal to extricate the inserted message from the stego-protest A stego key is a touch of additional data that the recipient must know keeping in mind the end goal to recoup the message from the holder king.

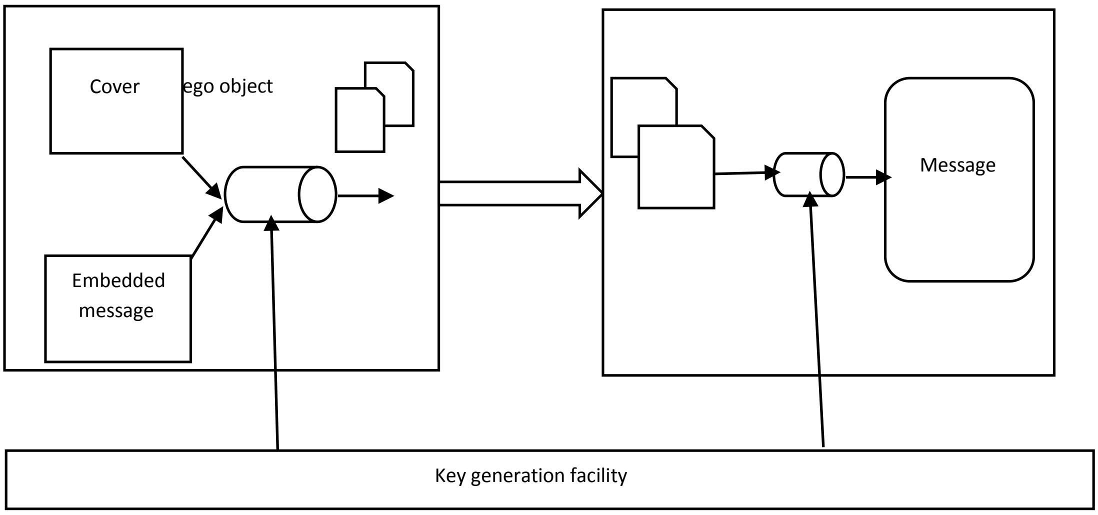

Fig 1: General schema of steganography

The utilization of a stego key is attractive for two reasons ;(l) it might make concealed information measurably harder to identify, and (2) the stego key baffle unapproved endeavors to acquire the concealed message from the cover(Sakthisudhan and Prabhu 2012).

4. Stego Object: is the yield part created from steganography motor. Steganography could be communicated as takes after

Cover medium + Embedded message + stego- key= Stego Object

At the point when the stego protest is created then the sender transmits it over a shaky channel to collector. Beneficiary can remake mystery message from stego protest, since he know the implanting technique and stego-enter that utilized as a part of the inserting process. In an impeccable steganography framework the first cover ought not to be recognizable from a stego question, neither by human nor by a PC searching for factual example.

1.5 How Does Steganography Work

There are various techniques used to conceal data within Picture, (Seetha and Eswaran 2013)Audio and Video records. The web gives an expanding wide band of correspondence administration as a way to appropriate data between the clients. Such data incorporates content, picture and sound .and so forth. Such sort of dispersed data gives incredible transporters to shrouded data. A wide range of methods have been acquainted with use these bearers as hosts for concealing data, additionally some other sort of transporters where utilized. As indicated by the kind of cover media the steganography systems are delegated segment underneath:

1.5.1 Hiding in Image

(Lavanya, Smruthi, and Elisala 2013)Data hiding in still images presents a variety of challenges that arise due to the way the human visual system (HVS) works and the typical modifications that images undergo A standout amongst the most essential preferences in utilizing still pictures for information stowing away is that they speak to a no causal medium, since it is conceivable to get to any pixel of the picture aimlessly. There are different procedures for information stowing away in still pictures:

l. LSB inclusion.

2. Spread range.

3. Surface square.

4. Interwoven.

5. Orthogonal projection coefficients control.

6. Different techniques: dithering control, perceptual veiling, DCT coefficients control

At the point when concealing data inside pictures the LSB (Least Significant piece) technique is typically utilized. To a PC a picture document is essentially a record that shows diverse hues and forces of light on various territories of a picture. The best kind of picture record to shroud data within is a 24 Bit BMP (Bitmap) picture. The reason being is this is the biggest kind of document and it regularly is of the most noteworthy quality.(Journal and Engineering 2013) At the point when a picture is of high caliber and determination it is a considerable measure simpler to stow away and cover data within Although 24 Bit pictures are best to hide data within because of their size a few people may utilize 8 Bit BMP's or potentially another picture arrangement, for example, GIF, the reason being is that posting of substantial pictures on the web may stimulate doubt. It is imperative to recall that in the event that you shroud data within a picture document and that record is changed over to another picture arrange, it is in all probability the concealed data inside will be lost.

1.5.2 Hiding in Documents

(Patil 2012)Information covering up in content is a practice in the revelation of changes that are not saw by peruses. For instance, HTML documents can be utilized to convey data since including space, tabs, undetectable characters and additional line breaks are overlooked by web programs. The utilization of Steganography in archives works by basically adding white space and tabs to the closures of the lines of a record. This sort of Steganography is to a great degree compelling, on the grounds that the utilization white space and tabs is not unmistakable to the human eye by any means, at any rate in most content/archive editors. White space and tabs happen actually in reports, so there isn't generally any conceivable way utilizing this strategy for Steganography would make somebody be suspicious

1.5.3 Hiding in video

(Gupta 2014)Video records are for the most part an accumulation of pictures and sounds, so the majority of the displayed methods on pictures and sound can be connected to video documents as well. The considerable favorable circumstances of video are the substantial measure of information that can be covered up inside and the way that it is a moving stream of pictures and sounds Therefore, any little however generally detectable twists may go in secret by people on account of the nonstop stream of data

Hiding in Audio

Installing mystery message in advanced sound is for the most part more troublesome than inserting in arrangement in computerized picture in light of the fact that the human sound-related framework (HAS) is greatly delicate (Lavanya, Smruthi, and Elisala 2013).

Sensitivity to added substance irregular commotion is additionally intense. The annoyances in a sound document can be distinguished as low as one section in ten million (80 dB beneath surrounding level). In any case, there are a few "gaps" accessible. While the has an extensive Dynamic range, it has a little differential range. Thus, uproarious sounds tend to veil out calm sounds. Also, the HAS is significantly less touchy to the stage segments of sound. At last, there are some ecological bends so regular as to be overlooked by the audience much of the time. The transmission medium of a sound flag alludes to nature in which a flag may experience to achieve its goal. Drinking spree and his associates classify the conceivable transmission situations into the accompanying four gatherings:

1. Advanced end-to-end environment where the sound records are duplicated straightforwardly starting with one machine then onto the next.
2. Expanded/diminished e examining environment where the flag is re-inspected to a higher or lower testing rate.
3. Simple transmission and re-examining where a flag is changed over to a simple state, played on a spotless simple line, and re-tested.
4. "Over the air" environment where the flag is played into the air and re-tested with a receiver.

2.1 problem mythology

The proposed system consist hide the binary text into the wave file .The general structure of the proposed system is illustrated in figure (2). It consists of two basic modules: hiding and extraction modules. The input to this system are the cover file (wave file), and secret file (binary file). These inputs are processed in the hiding part with various operations to produced stego wave file. The stego audio entered to extraction stage is processed through a set of operations to retrieve the secret data

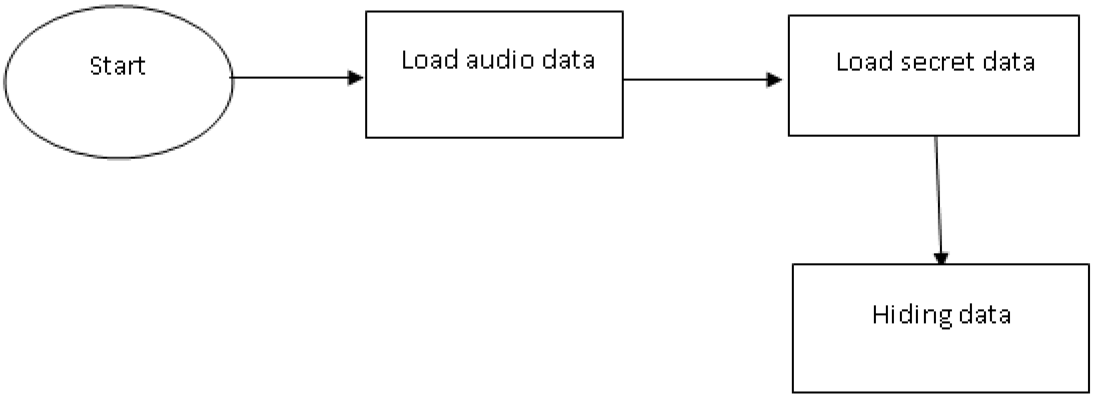

Fig. 2: general system model

2.2 Load Audio Data

We need to convert the input text into binary representation. So that each character takes 8-bits length of binary. The following algorithms depict the conversion from character text into binary text.

<u>Algorithm (4.1): Binary conversion</u>

```
Input:
OrgScrt: Secret data as an array byte OrgScrtLen: Size of secret file
Output:
Scrt: Binary secret data as an array byte ScrtLen: New size of secret data
Begin
  Set K ««—0
  For each byte value i in OrgScrt
```

```
   For each bit j in byte                                  //from 0 to 7
   Set Scrt(K+j)     OrgSecrt(i) AND ($2^A$ j)
   Set K    —K + 8 End loop
   Set ScrtLen «— OrgScrtLen x 8
End.
```

4.3 Load The Secret Data

After preparing the binary text, we can now embed this binary into the wave file, the following algorithms depicts the operator.

```
Algorithm (4.2) Load the secret file
Input:
ScrtName: Secret file Name
Output:
OrgScrtLen: Size of secret file
OrgScrt: Secret data as an array of bytes
Begin
   Open the secret file " ScrtName"
   Get OrgScrtLEN                               //*The length of secret file.
   Get secret data OrgScrt                      //*OrgScrt[0...OrgScrtLen] as an
array
   Of bytes.
End.
```

4.3 The Hiding Phase

In this phase, the hiding of secret block is done on the voiced blocks, exclusively. So, the implementation of process (to prepare the slack space) are done on the voiced blocks. The embedding process is done by adding or subtracting a (A) value to the quantized phase coefficients. The application of addition or subtraction processes depends on the value of the secret bit (whether it is 0 or 1). The value of(A) should be less than half the value of quantization step, in order to avoid the occurrence of a jump-fro* certain quantization bin to the one of the adjacent (pervious or next) quantization bins. To make the process of determining the suitable values of (A) more easy and consistent parameter called slack step ratio (R) is proposed, it is a ratio parameter define as follow:

$R = \Delta$ (4-1)

Q

The value of R should be (0 < R < 0.5). In this research work, the value of R was taken either (1/3) or (1/4). Both the values of (Q) and (R)are predefined by the user.

The quantity (A) is added to phase (pht) if the secret data value (Scrt) is one 1, or it is subtracted if (Serf) is 0, as follows:

$PH_H(U) = phs_q(u) - \Delta \quad ifScrt(i) = 0$

$phs_g(\mathbf{u}) + \Delta \quad ifScrt\{i) = l$ (4_2)

Where,

$phs_{q(U)}$ is the j^{th} phase coefficient in the block.

$phs_{H(u)}$ is the u^{th} host phase coefficient in the block.

Scrt(i) is the i^{th} secret bits.

u=l,2,3, (N/2)-l

Algorithm (4.3): Hiding Stage

Input:

Cov: The original samples of cover audio file of length DataSize.
Scrt: An array of secret bits of size ScrtSiz.
N: The block size. //N : 8, 12, 16, 21, 32

Str: Start block position of Overlnfo bits vector in Cov. Ed: Ending block position of Overlnfo bits vector in Cov.

Output:

Steg: Array of stego wave data of length DataSize.

Step 1: Divide Cov into blocks of size N samples.

step2:check if (block position<str) or (block position>Ed) then go to Step 9.

step 3: check each block is it unvoiced block, if it is unvoiced go to step 8.

Step 4: Apply dynamic located jump on this unvoiced block to produce B, and BB, Coefficients then construct Phs and Mag .

Step 5: Insert secret bits Scrt in the quantized phase coefficients.

step 6: Reconstruct F ,and Fi coefficients and pass the result through IDFT to construct the stego block, then round the_values to the range [0..255].

step 7: put the produced block in Steg array, which represents the stego data.

Step 8: If there are (secret bits of Scrt And cover block) go to Step 2.

Step 9: End.

CONCLUSION

As said in some conclusion comments that the created concealing strategies require a few upgrades to enhance their execution and to abrogate some of their powerless viewpoints. In this way, these techniques require advance improvement in future, and in the accompanying a few proposals are inferred as future work advancements:

1. Build up the framework to be competent to handle stereo sound record as a cover media.
2. Build up the framework to utilize another sound document designs like (MP3. DPCM...).

REFERENCES

[1] Allteef, Salwa K Abd. 2007. “Proposed Steganography Method to Hide Image Data in Wav File.” : 360–67.

[2] Atoum, Mohammed Salem, Osamah Abdulgader Al- Rababah, and Alaa Ismat Al-attili. 2011. “New Technique for Hiding Data in Audio File.” 11(4): 173–77.

[3] Bassil, Youssef. 2012. “A TWO INTERMEDIATES.” 3(11): 7–12.

[4] Files, Audio. 2010. “CHAPTER 7 INFORMATION HIDING IN AUDIO FILES.” : 203–46.

[5] Gupta, Nishu. 2014. “Three Layer Data Hiding Using Audio Steganography.” 3(6): 7086–88.

[6] Journal, Iosr, and Computer Engineering. 2013. "Enhancement of Data Hiding Capacity in Audio Steganography." 13(3): 30–35.

[7] Lavanya, Budda, Yangala Smruthi, and Srinivasa Rao Elisala. 2013. "Data Hiding in Audio by Using Image Steganography Technique." 2(6): 2–5.

[8] Of, Ministry, and Higher Education. "Hend Abdul Amir Hadi Yeqeen Salah Hameed Safa Hamid Mahmood Makki J . Radhi."

[9] Of, Ministry, and Higher Education. "Hend Abdul Amir Hadi Yeqeen Salah Hameed Safa Hamid Mahmood Makki J . Radhi."

[10] Patil, Swati A. 2012. "Hiding Text in Audio Using LSB Based Steganography." 2(3): 8–15.

[11] Pitropakis, Nikolaos, and Costas Lambrinoudakis. "A Practical Steganographic Approach for Matroska Based High Quality Video Files."

[12] Sakthisudhan, K, and P Prabhu. 2012. "Secure Audio Steganography For Hiding Text And Audio Files." (1): 3–14.

[13] Seetha, D, and P Eswaran. 2013. "A Study on Steganography to Hide Secret Message inside an Image." 3(June): 277–81.

[14] Sewisy, Adel A, and Amal A Mohammed. 2015. "Hidden Text into Audio Files." 2(5): 33–39.