Hiding Information Using Circular Distribuition

M.Sc.Rajaa Ahmed Ali
rajaaahmed52@yahoo.co.uk

M.Sc.Muntadher Khamees Mustafa
freefox79@yahoo.com

Ali A. Alani
Alialani@ sciences.uodiyala.edu.iq

University of Diyala, Collegek, of sciences, Diyala, Iraq

ABSTRACT

The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The important of reducing a chance of the information being detected during the transmission is being an issue now days. Therefore, different methods have been proposed so far for hiding information in different cover media. The carrier medium can be image, audio or video. Of the different carrier media, image is best chosen as the carrier due to its frequency on the internet. This paper proposes technique to hidden data in another medium. This technique hides an encoded audio message in the pixels of the carrier image using circular distribution algorithm. To measure the qualities of the cover file (stego image) after hides process used Peak Signal–to-Noise Ratio (PSNR). Only minor changes in the contents of the image file occur, which are indiscernible to human eyes.

Keywords- circular distribution, hide audio file, Steganography.

I. Introduction

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypted the data. A solution to this problem is steganography [1]. Steganography is an art of sending hidden data or secret Messages over a public channel so that a third party cannot detect the presence of the secret messages [2]. The goal of steganography is different from classical encryption, which Seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages [3]. In steganography the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information to be hidden, anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image fig.1 [1][2].

A possible formula of the process may be represented as: cover medium + embedded message + stego key = stego-medium.

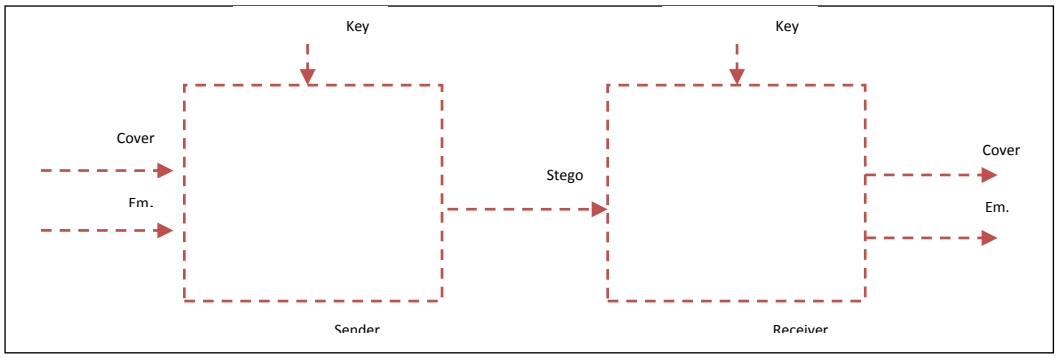


Fig.1 Graphical Version of the Steganography System

Where is the

F_E: Consider the steganography function "Embedding".

F_E^{-1}: Consider the steganography function "Extracting".

Cover: Consider the cover data in which "Em." will be hidden. Em.: Consider the message to be hidden.

Stego: Consider the cover data with the hidden message.

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. The main goal of this paper was to find a way so that an image file can be used as a host media to hide audio message without affecting the file structure and content of the image file. Because degradation in the perceptual quality of the cover object may leads to a noticeable change in the cover object which may leads to the failure of objective of

steganography. In the proposed method the replacement is done by using circular distribution algorithm as a novel way to hide the message.

The rest of the paper is organized as follows: Section 2 discusses the brief overview of steganography method applications and a desired characteristic Section 3 describes the proposed method. Section 4 shows experimental setup and result. Finally in Section 5 the conclusion and future work is described.

II. Applications of Steganography

Steganography is used for wide range of applications such as, in defense organizations for safe circulation of secret information, in military and intelligence agencies, in smart identity cards where personal details are embedded in the photograph itself for copyright control of materials. In medical imaging, patient's details are embedded within image providing protection of information and reducing transmission time and cost [4][1] , in online voting system so as to make the online election secure and robust against a variety of fraudulent behaviors [5], for data hiding in countries where cryptography is prohibited, in improving mobile banking security [6], in tamper proofing so as to prevent or detect unauthorized modifications and other numerous applications.

III. Desired Characteristics of Stegnography

A steganography system, generally, is aims to accomplish three key requirements, these are, indiscernible of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end user at the destination) [1]. In a steganography method, the way for embedding the message is unknown to anyone other than the sender and the receiver. An effective steganographic scheme should possess the following desired characteristics [7]:

Secrecy: A person should not be able to extract confidential data from the host medium without the knowledge of the correct secret key used in the extraction procedure.

Imperceptibility: the medium after being embedded with the covert data should be imperceptibility from the original medium.

High capacity: the maximum length of the covert message that can be embedded should be as long as possible [3]. **Resistance**: the covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme [8].

Reliable extraction: the extraction of the covert data from the medium should be reliable and accurate.

IV. Circular distributions

Circular distributions play an important role in modeling directional data which arise in various fields. In recent years, several new uni-modal circular distributions capable of modeling asymmetry also symmetry have

been proposed. The circular random variables is measured in degrees or radians and the value is in the range of ([0,2π] or [–π, π]) [9].

In this paper, we have proposed a method to hide an audio file (mp3) within the image file (bmp) throughout using the circular distribution algorithm fig.2. to do that, first we convert the two files "audio and image" to data in binary form. then after this transformation process we applied the circular distribution algorithm to chose random location from the image file to hide the bits of audio file, this locations selected depending on the radius and angle of circular and the algorithm chose this points based on the values of (x, y). Where it chooses the start point and then select the rest of points randomly by using below equations.

$$X = Xc + r \cos(\Theta) \qquad (1)$$

$$Y = Yc + r \sin(\Theta) \qquad (2)$$

Where (r) is the radius of the circle and (θ) represent the angle of the circle and both of them will be selected randomly. Show in fig (2).

V. SIGNAL PEAK -TO-NOISE RATIO

The peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have a very wide dynamic range, the PSNR is usually expressed in terms of the logarithmic decibel scale. In our propose system we use the PSNR quality measure proposed by [6] to measure the similarities between the original image (cover image) and the image after

hiding process. A higher PSNR indicates more similarity between the two images. The PSNR value is defined as follows:

$$PSNR=10 \log_{10} R^2/MSE \quad (1)$$

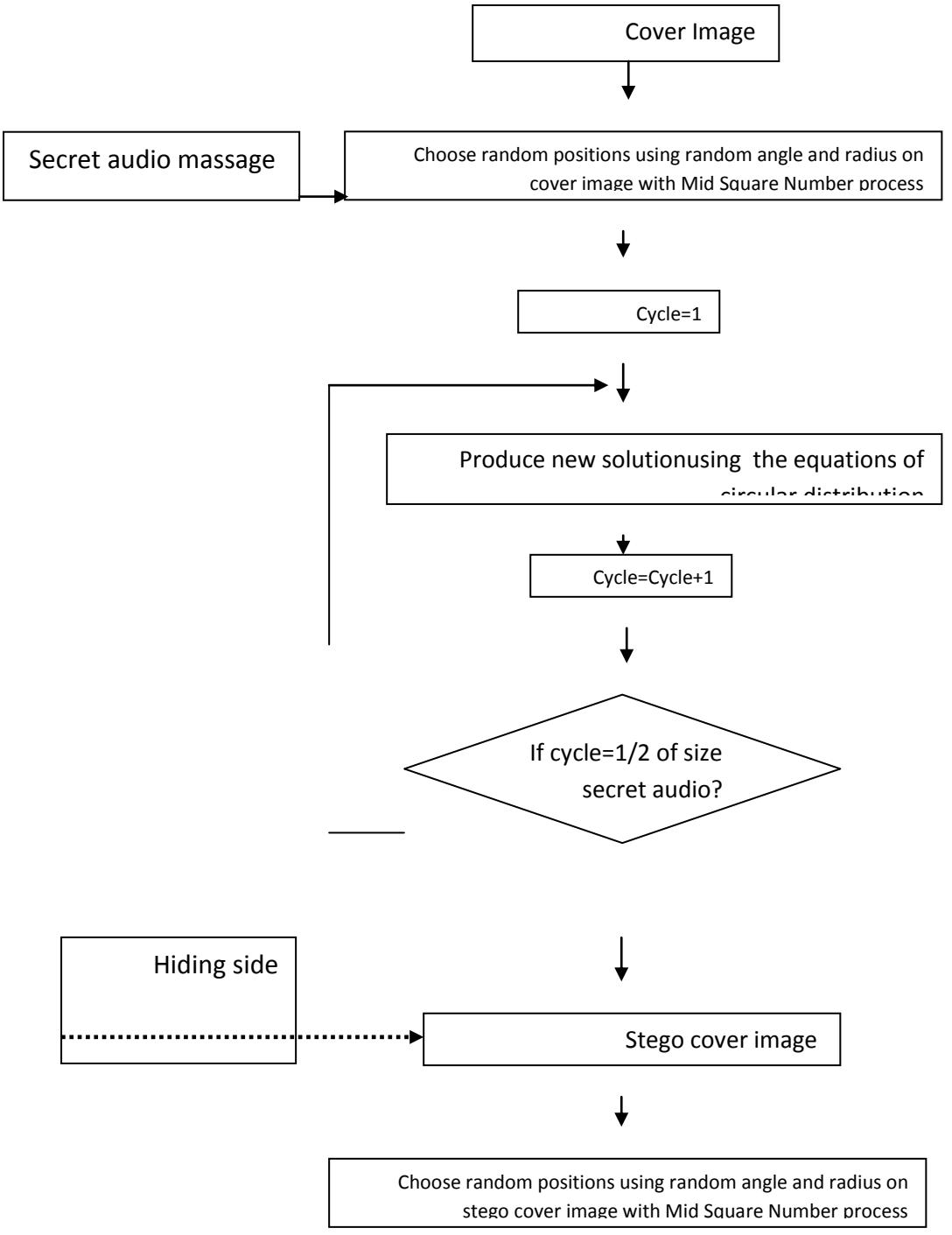
In the previous equation, R is the maximum fluctuation in the input image data type. The PSNR value used to measure the peak error, therefore If the value of the PSNR is high the hiding operation will be accepted else it will be rejected. In order to compute the PSNR value, first should be calculates the mean-squared error (MSE) by using the following equation:

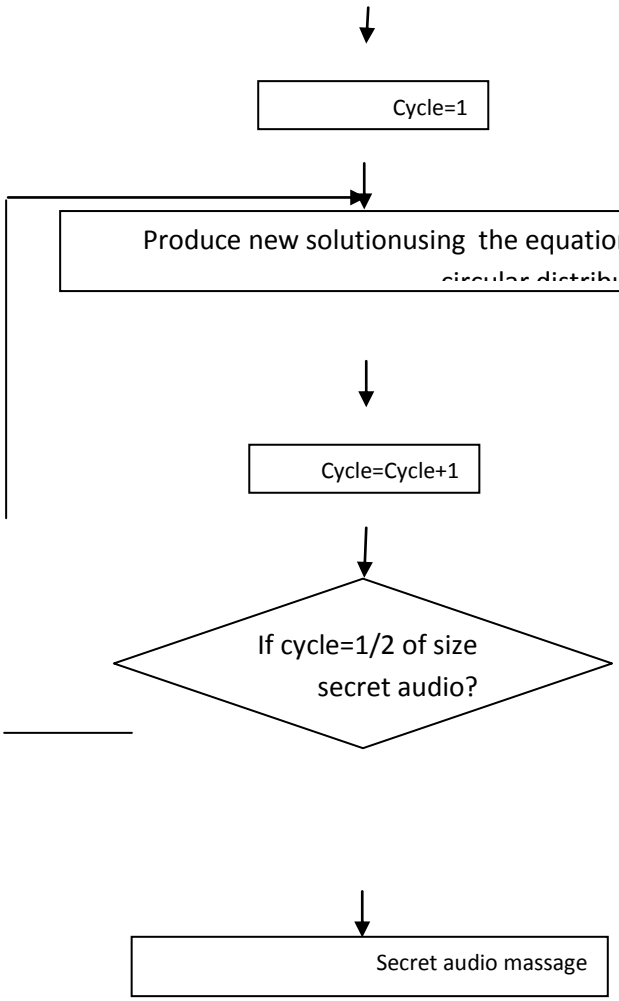
$$MSE = \frac{1}{NxM} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2$$

The mean square error (MSE) is an error metrics used to compare image hiding quality, also it represents the cumulative squared error hiding image and the original image, Therefore If the MSE is between the low hiding operation will be accepted else it will be rejected.

VI. PROPOSED ALGORITHM

The audio message in .mp3 format was successfully sampled and converted to its binary format. The binary message was hidden in the cover image using the proposed circular distribution technique and transmitted. The message is retrieved using the same technique at the receiver side. The block diagram of the proposed system is shown in Fig (2).


Cover Image
Secret audio massage
Choose random positions using random angle and radius on cover image with Mid Square Number process
Cycle=1
Produce new solutionusing the equations of
Cycle=Cycle+1
If cycle=1/2 of size secret audio?
Hiding side
Stego cover image
Choose random positions using random angle and radius on stego cover image with Mid Square Number process



Fig(2): Block Diagram of Proposed Algorithm

a. *Algorithm for hiding using (Circular distribution)*

The input in the hiding algorithm is the secret audio file using sequential and cover image file that select the locations by using circular distribution algorithm in cover image. The Output will produce the stego image file. The steps are described in as follows.

- Apply circular distribution for initialized population on cover image for initialize the population of solution xi=(xij), i=1,2,….SN, j=1,2,…,n. // number of distributed points =1/2 *

size of secret image. Using mid square number to generate random number that chosen to find radius randomly and chosen angle randomly.

- cycle =1.
- Repeat
- Produce new solution using the equations of circular distribution $X=X_c +r *\cos \theta$ for X-axis and $Y=Y_c +r * \sin \theta$ for Y-axis based on R and θ.The source position that is chosen refered to it as false flag.
- cycle= cycle+1.
- Stop until cycle= 1/2 size of secret image.

b. Algorithm of restore audio

- Input: Image file contain MP3.
- Output: MP3 file.
- Using circular distrubution for restoring (chosing) position that contain mp3 file.
- Take a pixel from stego cover image according to coordinates and Saved in two array (init ().loci , init().locj).
- Take the least bit of red and green and blue colors.
- Store the array in an audio file

VII. Results

The audio message in .mp3 format was successfully sampled and converted to its binary format. The binary message was hidden in the cover image using the proposed circular distribution technique and transmitted. The message is retrieved using the same technique at the receiver side.

A group of test cover images are shown in Fig.3 before and after hiding short audio files using the previously mentioned method.

Moreover, the short audio messages have been extracted from the stego-images and saved to new mp3 files. It has been verified that modulating the cover image with the short audio message does not result in a human-perceptible difference because the amplitude of the change is trivial. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. the extracted audio messages are compared to original audio files and were identical with them.

a. A 6.33 KB MP3 file has been hidden inside the 580 KB left image yielding to the right one.

b. A 5.33 KB MP3 file has been hidden inside the 524 KB left image yielding to the right one.

c. A 5.33 KB MP3 file has been hidden inside the 660 KB left image yielding to the right one

Fig.3 Cover (left) and stego (right) images

In order to evaluate the image quality after embedding the audio into image file, the proposed system analyzed the PSNR (peak signal to noise ratio) and MSE to measure the quality of the carrier file after hiding process. The results show there is a little change in the quality of the cover image after the hiding process completed as presented in table 1.

Table (1): Results of PSNR and MSE

Cover image size	**Mp3 size**	**PSNR**	**MSE**
524KB	5.33 KB	74.8461315	2.624080828
580KB	6.33KB	75.4049946	3.744747474
660KB	5.33KB	75.91287208	3.333333333

VIII. Conclusion

This paper discusses the possibility of hiding short mp3 audio file inside digital image. The embedding process applied by using the novel circular destruction algorithm to create a stego-image by replacing these redundant bits with data from the hidden audio message. The proposed method provided a higher similarity between the cover and the obtained stego pictures. the new approach provides a secured means of secret communication between two parties.

The future work could be to extend to embed audio messages within video files. Moreover, by using the proposed method first the secrete data is embedded into the image and that image is embedded into the video. So the secrecy is increase. This is mainly used in military applications and defense applications.

أخفاء المعلومات باستخدام التوزيع الدائري

١-م.م رجاء أحمد علي /جامعة ديالى /كلية العلوم
٢-م.م منتظر خميس مصطفى / جامعة ديالى/ كلية العلوم
٣-المبرمج علي عبد الرحمن العاني / جامعة ديالى / كلية العلوم

الخلاصة

الانترنت يستخدم روابط قد تكون غير امنة، وبالتالي المعلومات التي يتم نقلها قد تكون عرضة للهجوم. ولذلك يجب التقليل من فرصة اكتشاف المعلومات المنقولة غبر الانترنت. هناك طرق مختلفة تم تقديمها لاخفاء المعلومات في وسائل تغطية مختلفة. في هذه الورقه تقترح اخفاء البيانات داخل وسيلة تغطية اخرى. الوسائلة الناقلة قد تكون صور، صوت او فيديو. من الافضل اختيار الصورة كوسط ناقل بسبب زيادة ترددها عبر الانترنت. في هذا التقنية تم اخفاء صوت مشفر داخل صورة باستخدام خوارزمية التوزيع الدائري. لقياس نوعية الملف المتمثل كغطاء وذلك باستخدام نسبة الاشارة الى الضوضاء. وتم اكتشاف تغيرات طفيفة في محتويات ملف الصورة والتي تكون غير مدركة بالنسبة للعين البشرية .

الكلمات المفتاحية: التوزيع الدائري، اخفاء الملف الصوتي، اخفاء المعلومات.

REFERENCES

1.A. Kumar and K. Pooja, "Steganography-A Data Hiding Technique," *Int. J. Comput. Appl.*, vol. 9, no. 7, pp. 19–23, 2010.

2.H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, Oct. 2014.

3.B. Lavanya, Y. Smruthi, and S. R. Elisala, "Data hiding in audio by using image steganography technique," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 2, no. 6, pp. 2–5, 2013.

4.U. C. Nirinjan and D. Anand, "Watermarking medical images with patient information," in *In the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China*, 1998, pp. 703–06.

5.S. Katiyar, K. R. Meka, F. A. Barbhuiya, and S. Nandi, "Online voting system powered by biometric security using steganography," in *In the 2nd International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India*, 2011, pp. 288–291.

6.M. Shirali-Shahreza, "Improving mobile banking security using steganography," in *In the 4th International Conference on Information Technology, ITNG, Las Vegas*, 2007, pp. 885–887.

7.B. Chen, "Design and analysis of digital watermarking, information embedding, and data hiding systems," , MIT, Cambridge,.

8.et al. J. Zollner, H. Federrath, H. Klimant, "Modelling the Security of Steganographic Systems," 1998.

9.C. Distribution, "Finding the Best Circular Distribution for Southwesterly Monsoon Wind Direction in Malaysia," *Sains Malaysiana*, vol. 39, no. 3, pp. 387–393, 2010.