УДК 004.415.24

СКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ С ИСПОЛЬЗОВАНИЕМ КРУГОВОГО РАСПРЕДЕЛЕНИЯ

Аль-Ани А. А.

ФГАОУВО Уральский федеральный университет имени первого Президента России Б.Н.Ельцина, Екатеринбург, Россия (620002 Россия, г. Екатеринбург, ул. Мира,19), e-mail:ahmedalani80@gmail.com

Аннотация: В статье рассматриваются метод скрытия информации при передаче сообщений через сеть Интернет. Основой метода является скрытие информации в носителе другого типа, или стеганография. Предлагается метод скрытия звуковых сообщений, в котором в качестве носителя выбран файл изображения в формате bmp. Алгоритм основан на применении кругового распределения.

Ключевые слова: стеганография, скрытие звуковых сообщений, круговое распределение.

HIDING INFORMATION IN IMAGE USING CIRCULAR DISTRIBUITION

Alani-A. A.

Federal State Autonomous Educational Institution of Higher Professional Education «Ural Federal University named after the first President of Russia B.N.Yeltsin», Yekaterinburg, Russia (620002, Russia, Yekaterinburg, street Mira, 19), e-mail: ahmedalani80@gmail.com

Abstract: Today the art send & reserve the hidden information become largely used in information security system especially in public places. Because the Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. Therefore, different methods have been proposed so far for hiding information in different cover media. The data in one medium can be hidden in another medium. 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 project aim to hiding audio file in the pixels of the carrier image using the Steganography "circular distribution algorithm" in image type BMP. The hiding audio is manipulated in way to keep host image with same size and without producing any significant distortion, also this project aim to extracting hiding audio from image without affect any problem in image and audio.

Key words: circular distribution; hiding audio file; steganography.

The aim of project

The aim of the project is hide audio (.mp3) by using circular distribution in image type BMP.the hiding audio is manipulated in way to keep host image with same size and without producing any significant distortion, also this project aim to extracting hiding audio from image without affect any problem in image and audio.

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 unencrypt the data. A solution to this problem is steganography.

Steganography

Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication". In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security. Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are.bmp,.doc,.gif,.jpeg,.mp3,.txt and.wav. Mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message. Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the internet.

How data is hidden in pictures

All computer-based pictures are composed of an array of dots, called pixels, that make up a very fine grid. Each one of these pixels has its own color, represented internally as separate quantities of red, green and blue. Within Windows, each of these color levels may range between 0 (none of the color) and 255 (a full amount of the colors). A pixel with an RGB value of 0 0 0 is black, and one with a value of 255 255 255 is white .

S-Tools works by 'spreading' the bit-pattern of the file that you want to hide across the least-significant bits (LSB's) of the color levels in the image .

For a 24 bit image this is simple because 24 bit images are stored internally as RGB triples, and all we need to do is spread our bits and save out the new file. The drawback to this is that 24 bit images are uncommon at the moment, and would therefore attract the attention of those whose attention you are trying to avoid attracting! They are also very large as they contain 3 bytes for every pixel (for a 640x480 image this is 640x480x3=921600 bytes) .

It is considerably more difficult to hide anything within a 256-colour image. This is because the image may already have over 200 colors which our meddling will carry to way over the absolute maximum of 256.

Looking at a little theory it is easy to see that an image with 32 or less colors will never exceed 256 colors, no matter how much we meddle with it. To see this, visualize the 3 LSB's of an RGB triple as a 3-bit number. As we pass through it in our hiding process we can change it to any one of 8 possible values, the binary digits from 000 to 111, one of which is the original pattern.

If one color can 'expand' to up to 8 colors, how many distinct colors can we have before we are in danger of exceeding the limit of 256? Simple, 256/8=32 colors. There is no guarantee that 32 colors is our upper limit for every file that you want to hide though. If you're lucky the file will not change a color to all of its 8 possible combinations and then we are able to keep one more of the original colors. In practice, however, you will often find pictures being reduced to the minimum of 32 colors. S-Tools tries to reduce the number of image colors in a manner that preserves as much of the image detail as possible.

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]).

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. 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 choose 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 choose the start point and then select the rest of points randomly by using below equations.

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

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

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

How Does the System work

It consists operations as the following:

1). Select Cover File

If we choose circular distribution then we must choose cover image (.bmp). It's pixels number >=1000*1000 pixel.

2). Select Embed File

The project select the file that you want hiding it and from type (.mp3). We need to convert the input audio file into binary representation after open audio as random. So that each byte takes 8-bits length of binary.

References

1. Shuichi TAKANO Data hiding via steganographic image transformation. IEICE TRANS. FUNDAMENTALS, VOL.E83–A, NO.2 FEBRUARY 2000
2. Smith, A. Information hiding, Proceeding Of First International Workshop Lecture Notes In Computer Science, Springer, Verlag, vol.1174, 1996.
3. Hana, H., Marza "Techniques for text steganography in image using JPEG compression method", MSC. Thesis, Baghdad University, 2001.
4. Lala, Z., A., Image in image steganography, Ph.D.thesis, University Of Technology, Computer Dept., Baghdad, Iraq, 2000.
5. Raid S. Information hiding in wave media file byusing low bit encoding, MSC. Thesis, University Of Technology, Computer Dept., Baghdad, Iraq, 2001.