



Steganography Using Album Cover in the Mp3 Audio File

Shaminder Singh

Research Scholar

Department of Computer Science, JCD Vidyapeeth
Affiliated to Guru Jambheshwar University, Hisar, India

Krishan Kumar

Assistant Professor

Department of Computer Science, JCD Vidyapeeth
Affiliated to Guru Jambheshwar University, Hisar, India

Abstract— With the increasing demand of data on internet, The important issue is to provide security for this data. So the attractive solution for this problem is Steganography. Steganography is the art and science of writing hidden messages in data so that no one except from the sender and intended recipient even realize that there is a hidden message. The hidden message may be text, image, audio, video, etc. In this paper, we mainly discuss about how to hide text data in mp3 file by using album cover or album art.

Keywords— mp3, album cover, digital audio, steganography, LSB

I. INTRODUCTION

The term “Security through Obscurity” or “Security by Obscurity” is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms. So Steganography is about security by obscurity. We can say that Steganography is the art and science of writing hidden messages in data except the sender and intended recipient [6]. The proposed steganography technique requires a message string that will be inserted and a MP3 that contained Tag ID3v2 in the form of the album cover figure as a medium. In this tool, firstly the message shall be encrypted which apply public key that take the form of matrix. Subsequently the encrypted message is inserted to the MP3 file by using the Before All Frames method where message partition stored in each before the MP3 file frame MP3, whereas the public key is inserted into the album cover figure stored in the ID3v2 tag by using Least Significant Bit (LSB) method.

II. STEGANOGRAPHY APPLICATION

An To write hidden messages in data ,the sender use Steganography application.

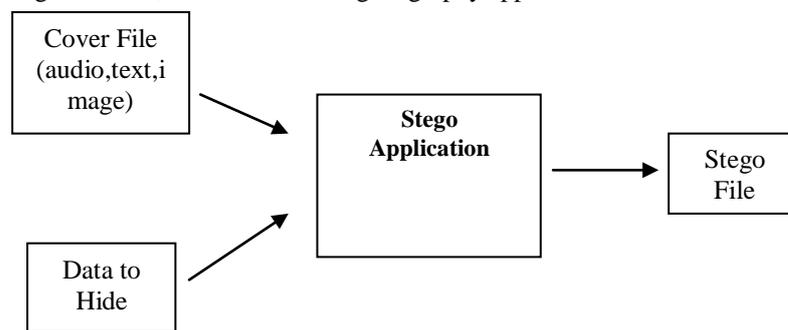


Fig 1. Steganography application

The steganography application hides different types of data within a cover file. The resulting stego file also contains hidden information, although it is virtually identical to the cover file

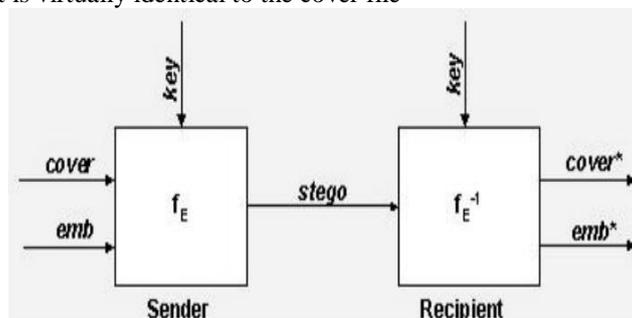


Fig 2 A Generic Steganographic System[1]

Figure shows the block diagram of a secure steganographic system. Input messages can be images, texts, video, etc. The components of steganographic system are [10]:

emb: The message to be embedded.

Cover: The data in which emb will be embedded.

Stego: A modified version of cover that contains the embedded message emb.

Key: Additional secret data that is needed for the embedding and extracting processes and must be known to both, the sender and the recipient.

f_E : A steganographic function that has cover, emb and key as parameters and produces stego as output.

f_E^{-1} : A steganographic function that has stego and key as parameters and produces emb as output. f_E^{-1} is the inverse function of f_E in the sense that the result of the extracting process f_E^{-1} is identical to the input E of the embedding process f_E . [1].

III. HUMAN AUDITORY SYSTEM

An Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected. [9]

IV. MP3 STEGANOGRAPHY METHODOLOGY

An The main purpose of data hiding, are the secrecy of the hidden message, robustness of the approach and data hidden size. Several audio steganography and audio watermarking approaches have been developed in literature using different domains like time domain, frequency domain, and wavelet domain to achieve the above purposes. The process of selecting the domain depends on the purpose of developing the approach, for example, the target of the developer is to achieve high rate data hidden, and in this case they need to use time domain or compressed domain.

In time domain steganography techniques, watermark is directly embedded into audio signal, where no domain transform is required in this process. Watermark signal is shaped before embedding operation to ensure the robustness

Transforming audio signal from time domain to frequency domain enables steganography system to embed the watermark into perceptually significant components. According to [4] this technique offers high level of robustness, due to that any attempt to remove the watermark will result in introducing a serious distortion in original audio signal fidelity.

Compressed domain audio steganography has removed the perceptually irrelevant parts of the audio and makes the audio signal distortion inaudible to the human ear. MPEG audio compression is a lossy algorithm and uses the special nature of the HAS, these type of systems are suitable for “pay audio” scenario, where the provider stores audio contents in compressed format. During download of music, the customer identifies himself with his unique customer ID, which therefore is known to the provider during delivery. In order to embed the customer ID into the audio data using a steganography technique, a scheme is needed that is capable of steganography compressed audio on the fly during download.[5]

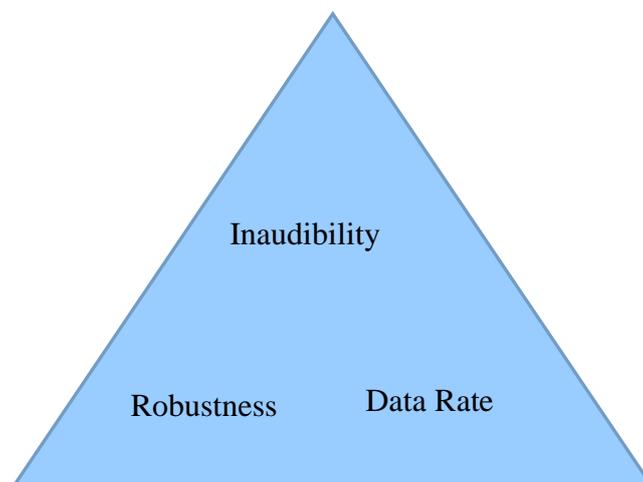


Fig 3 three contradictory requirements of mp3 steganography.

V. IMPLEMENTATION

This steganography tool in broad terms is divided into some stages as follow:

1. Designing MP3 application program.
2. Applying the steganography album cover technique .

The Flowchart for Steganography process is shown below:

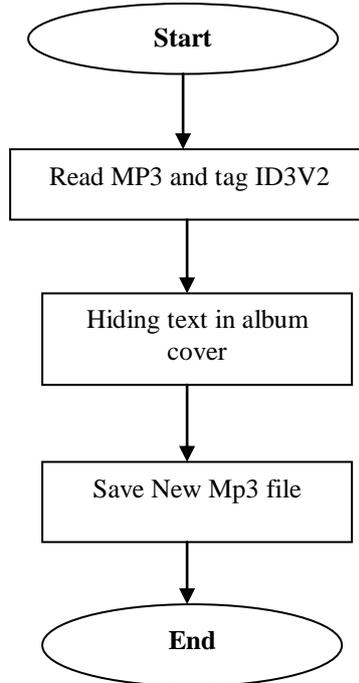


Fig 4: Message Hiding Process

In the first step, we design a tool using C# for steganography. The tool firstly takes the address of mp3 file from the user in a textbox. After that it reads the mp3 file ID3v2 tags. Then it fetches album cover from ID3v2 tags as shown in the figure below:



Fig 5: tool fetching album cover from ID3v2 tags

Then it takes the text from the user to hide into the album cover. The text is hidden by the tool in the album cover. The album cover's LSB bits are removed. These LSB bits are the parity bits.

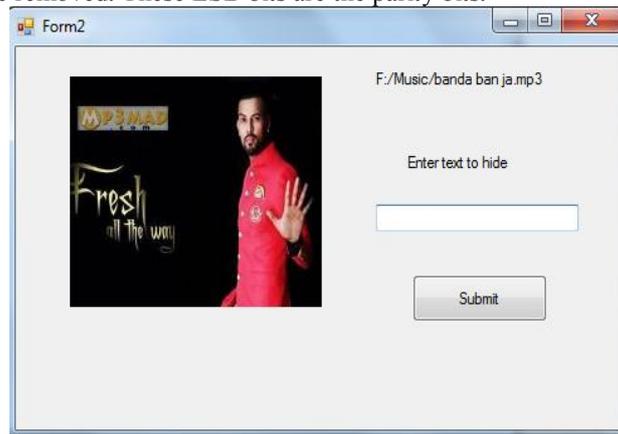


Fig 6: Text to hide into album cover

The Flow chart for revealing the secret message is shown below:

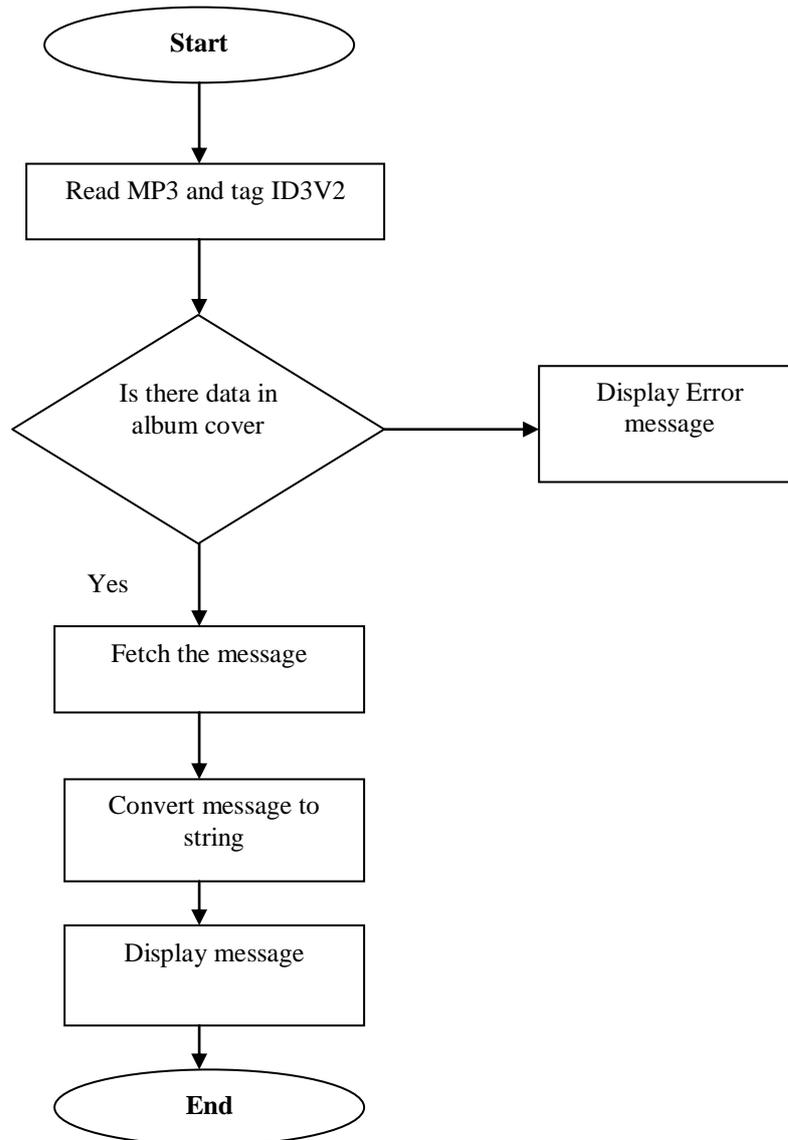


Fig 7: Message revealing process

VI. RESULTS

Discuss and analyse the results of this steganography tool which uses the album cover of mp3 file to hide data. Analysing the size of mp3 file, there is no change in the size of mp3 file after steganography. The message can be reveal from the file without any slightest change. Based on human hearing the sound is not changed at all, there is no any disturbance or noise. The sound quality doesn't change because there is not any changes into the audio part of mp3 file , All changes are made into the album cover or in ID3v2 tags.

VII. CONCLUSION

Album cover of mp3 file can be used in steganography. Data hiding in the album cover of mp3 file will not change the resolution of album cover. LSB of album cover can be used for hiding the message in mp3 file. There is no any changes in the size of mp3 file after steganography . The data can be hidden in the mp3 file without making any changes into the audio part of the mp3 file. There is no any disturbing spoiled sound such as noise or crackling.

REFERENCES

- [1] The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011
- [2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.
- [3] I. Paraskevas and E. Chilton, "Combination of Magnitude and Phase Statistical Features for Audio Classification," Acoustical Research Letters Online, Acoustical Society of America, vol. 5, no. 3, pp. 111 – 117, July 2004.
- [4] Zhang Y, Lu ZM, Zhao DN (2010). "A blind image watermarking scheme using fast hadamard transform".

- [5] Alsalami MAT, Al-Akaidi MM (2003). "Digital Audio Watermarking:Survey", 17th European Simulation Multi-conference, UK.n.
- [6] Kumar V., Kumar D. (2010). "Performance evaluation of dwt based image steganography", IEEE International Conference on Advance Computing. pp.223-228.
- [7] Kumar V., Kumar D. (2010). "Digital image steganography based on combination of DCT and DWT", Information and Communication Technologies, Springer Berlin Heidelberg, pp. 596-601.
- [8] Kumar D., Kumar V. (2011). "Contourlet transform based watermarking for colour images", International Journal of Multimedia and its Applications, vol 3. no. 1, pp. 119-127.
- [9] Kumar D., Chahar, V. (2011). "Digital image watermarking: a review of SVD, DCT and DWT based approaches", Journal of Computer Science, Vol. 10, No. 3, pp. 25-35.
- [10] Kumar D., Kumar V. (2011). "Improving the performance of color image watermarking using Contourlet transform", Advances in Computer Science and Information Technology, Springer Berlin Heidelberg, pp. 256-264.