South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 235–241

ISSN No: 2454-9614

Communications using a Unique Approach to Steganography by Audio Enhancing the Security of Mobile

S. Logarasi , G.S. Manickavasagam*

Department Of Computer Science and Engineering, Surya Engineering College,
Erode - 638107, Tamilnadu, India.

*Corresponding Author: S. Logarasi

E-mail: logurocks2626@gmail.com,

Received: 10/11/2015, Revised: 11/12/2015 and Accepted: 14/03/2016

Abstract

Secure communication needs has become imperative by using steganography is the most reliable source of critical information exchange mechanism and publicly available communication channels. There are a variety of more and more sensitive data such as encryption and steganography techniques, such as the transfer of the proposed model is usually applied through the entrance of the hidden data communication for audio steganography with text steganography, it is calculated by the byte values.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

The fast growth of internet has made digital media very popular. Digital media have many advantages in communication field but it also has increased the digital duplication, tampering and hacking. So, information security is an inseparable part of data communication. Steganography is a technique to hide data into resources. In this paper, the authors have explained how this technique can be used in android based smart phone. There are some limitations on implementing steganography. Steganography is a process of hiding text or information in existing content. Mostly images or multimedia (audio/video) is used to hide the content. In simple terms one can say that using steganography one can hide text or other content into text or multimedia file. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of Information within Computer Files. In Digital Steganography, Electronic Communications may include Steganographic Coding Inside Of a Transport Layer, Such as a Document.

2. Stegnography Techniques

2.1 Physical

- Hidden messages on messenger's body—also used in ancient Greece. Herodotus tells the story
- Of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and restrictions on the number and size of messages that can be encoded on one person's scalp.
- During World War II, the French resistance sent some messages written on the backs of couriers in invisible link.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages
- Messages written in Morse code on yarn and then knitted into a piece of clothing worn by a courier.
- Messages written on envelopes in the area covered by postage stamps.
- In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters in one typeface. Because of this, a message could be hidden using two (or more) different typefaces, such as normal or italic.
- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute (less than the size of the period produced by a typewriter). World War II microdots were embedded in the paper and covered with an adhesive, such as collodion. This was reflective, and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
- During WWII, vulvae Dickinson, a spy for Japan in New York city, sent information to accommodation addresses in neutral south America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the doll woman.
- Jeremiah Denton repeatedly blinked his eyes in Morse code during the 1966 televised press conference that he was forced into as an American pow by his north Vietnamese captors, spelling out "to- r-t-u-r-e".
- This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that the north

Vietnamese were torturing American pows. The USS pueblo intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors, but captives of the north Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

2.2Digital Message

Modern steganography entered the world in 1985 with the advent of personal computers being applied to classical steganography problems. Development following that was very slow, but has since taken off, going by the large number of steganography software available:

- Concealing messages within the lowest bits of noisy images or sound files.
- Concealing data within encrypted data or within random data. The message to conceal is encrypted, then used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates ciphertexts that look perfectly random without the private key).
- Chaffing and winnowing. Mimic functions convert one file to have the statistical profile of another. This can thwart statistical methods that help brute-force attacks identify the right solution in a ciphertext-only attack.
- Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
- Pictures embedded in video material (optionally played at slower or faster speed).
- Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in key presses in some applications (telnet orremote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
- Changing the order of elements in a set.
- Content-aware steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a nonhuman adversary/warden.
- Blog-steganography. Messages are fractionalized and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.
- Modifying the echo of a sound file (echo steganography)
- Steganography for audio signals
- Image bit-plane complexity segmentation steganography
- Including data in ignored sections of a file, such as after the logical end of the carrier file.

2.3 Digital Text

I. Making text the same color as the background in word processor documents, e-mails, and forum posts.

II. Using UNICODE characters that look like the standard ASCII character set. On most systems, there is no visual difference from ordinary text. Some systems may display the font differently, and the extra information would then be easily spotted, of course.

III. Using hidden (control) characters, and redundant use of markup (e.g., empty bold, underline or italics) to embed information within html, which is visible by examining the document source.

2.4 Social Steganograph

In communities with social or government taboos or censorship, people use cultural steganography hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers. Examples include:

- Hiding a message in the title and context of a shared video or image
- Misspelling names or words those are popular in the media in a given week, to suggest an alternate meaning.

2.5 Network

All information hiding techniques that may be used to exchange steganograms in telecommunication networks can be classified under the general term of network steganography. This nomenclature was originally introduced in 2003. Contrary to typical steganographic methods that use digital media (images, audio and video files) to hide data, network steganography uses communication protocols' control elements and their intrinsic functionality. As a result, such methods are harder to detect and eliminatetypical network steganography methods involve modification of the properties of a single network protocol. Such modification can be applied to the pdu (protocol data unit),[13] to the time relations between the exchanged pdus, or both (hybrid methods). Moreover, it is feasible to utilize the relation between two or more different network protocols to enable secret communication. These applications fall under the term inter-protocol steganography. Network steganography covers a broad spectrum of techniques, which include,

Among others:

- Steganophony — the concealment of messages in voice-over- ip conversations, e.g. the employment of delayed or corrupted packets that would normally be ignored by the receiver (this method is called lack — lost audio packets steganography), or, alternatively, hiding information in unused header fields.
- Wlan steganography – transmission of steganograms in wireless local area networks. A practical example of wlan steganography is the hiccups system (hidden communication system for corrupted networks).

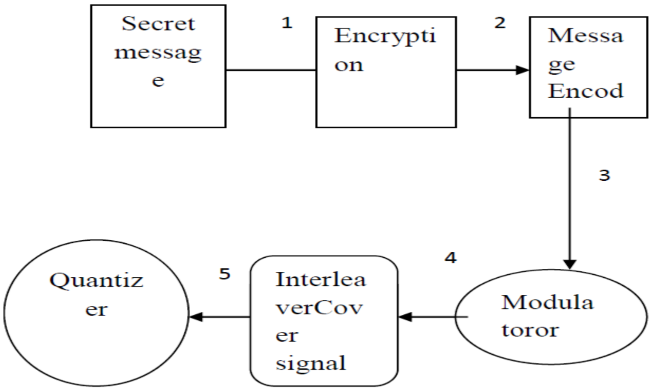

Fig 1 Architecture and Components

The word steganography comes from the Greek Steganos, which means covered or secret and – graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding secret information in a cover file such that only sender and receiver can detect the existence of the secret information .A secret information is encoded in a manner such that the very existence of the information is concealed. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not only prevents others from knowing the hidden information, but I also prevents others from thinking that the information even exists.

If a steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed. The basic model of Audio steganography consists of carrier (audio file), message and password. Carrier is also known as a cover-file, which conceals the secret information. Basically, the model for steganography is shown in figure. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

Spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key. The technique has been used by the military since the 1940s because the signals are hard to jam or intercept as they are lost in the background noise. Spread spectrum techniques can be used for watermarkingby matching the narrow bandwidth of the embedded data to the large bandwidth of the medium.

Two versions of SS can be used in audio Steganography: the directsequence and frequency-hopping schemes. In direct-sequence SS, the secret message is spread out by a constant called the chip rate and then modulated with a pseudorandom signal. It is the interleaved with the cover-signal. In frequencyhopping SS, the audio file's frequency spectrum is altered so that it hops rapidly between frequencies.

Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss. They have the potential t perform better in some areas than LSB coding, parity coding, and phase coding techniques in that it offers a moderate data transmission rate while also maintaining a high level of robustness against removal techniques.

3. Literature Survey

The paper "Pooja P. Balgurgi and Sona K. Jag tap 2013 proposes information hiding technique" is a new kind of secret communication technology. The majority of today's information hiding systems uses multimedia objects like image, audio, video. Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics. Embedding secret messages in digital sound is a more difficult process. Varieties of techniques for embedding information in digital audio have been established. This paper presents comprehensive survey of some of the audio steganography techniques for data hiding. Least Significant Bit (LSB) technique is one of the simplest approaches for secure data transfer. In this work, different data hiding methods used to protect the information are

The paper "Gunjan Nehru, Puja Dhar 2013 proposes the study of various techniques of audio steganography using different algorithm "is like genetic algorithm approach and LSB approach. We have tried some approaches that help in audio steganography. As we know it is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. In steganography, the message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stegomessage. In other words, stego message is combination of host message and secret message. Audio steganography requires a text or audio secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography, stego message after steganography remains same for information hiding.

4. Conclusion

As explained above, the approach used for hiding crucial information is one which is unique as the data is divided and hidden into Audio and text cover files if text + Audio option is chosen. Also, if only Audio cover file is chosen, the entire secret message can be hidden in the music itself. The comparison shows various devices taking the amount of time that they use in encoding a particular message in a cover Audio file. Thus, this approach is unique and secure for communicating secret data through smart phones.

References

[1] Pooja P. Balgurgi and Sona K. Jagta p “Audio Steganography Used for Secure Data Transmission” Proceedings of International Conference on Advances in Computing Volume 174 of the series Advances in Intelligent Systems and Computing pp 699-706, 2013

[2] Gunjan Nehru, Puja Dhar “A Detailed look of Audio Steganography Techniques using LSB and Genetic Algorithm Approach “IJCSI International

[3] Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2013

[4] Jayaram P, Ranganatha H R, Anupama “Information hiding using audio Steganography – a survey”, The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, 2014

[5] AnkitChadha, NehaSatam, RakshakSood, Dattatray Bade,” An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution” International Journal of Computer Applications (0975 – 8887) Volume 77– No.13, September 2013