International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Cloud Security using Steganography

Ms. Hina & Ms. Nidhi Sharma
[1,2]Assistant Professor, Department of computer science & Applications
S.D. College, Ambala Cantt
[1] hina.sdc@gmail.com,[2]nidhi.sdc@gmail.com

Abstract

As data is rapidly increasing day by day we need more and more space to store that data and our computers are not able to store and process such a huge data. We need to buy additional memory in form of CD, DVD, and hard disk Drive etc. and store our data, the other option is to store your data on cloud. Not only storage but we can also use the software and platforms online rather than installing at our site. This whole thing is known as cloud computing. Cloud Computing is an emerging technology that is changing the way of data storage and computing.Although Cloud Computing is very useful these days but it also some cons. As your data is lying at remote location, security is the most alarming issue. In this paper we are going to describe security issues related to cloud and securing data while transmitting and at rest in cloud computing. Steganography is one such method of securing information in cloud.

Key words

Steganography, Text Steganography, Image Steganography, Audio Steganography

1. Introduction

Cloud computing is a cost-efficient way of proving online availability of resources remotely located to consumers and business organizations through internet on pay per use basis.Cloud computing is known as a practice to use remote located system to store, process and manage data rather than using our local system. As name specifies cloud computing offers computing services like storage, software, analytics and more over the internet.Cloud services models are divided into three categories: Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS).

Data Security is the point of focus while using cloud computing. Now-a-days internet availability has become very cost effective and a lot of videos on internet are available on how to hack data. Steganography is the technique to provide security of data lying on cloud. There are many privacy and security concerns that cloud users are facing today, mainly related to data security at rest i.e. at data centers and security of data during transmission from client to cloud, it can be hacked while transmitting. Storing our personal or crucial data is a matter of risk. As there may be many unauthorized users who want/try to access your data. So, to store the data at secure location is one of major responsibilities of the cloud. Not only the storage location but cloud also provides security mechanisms to secure your data from any unauthorized access. This is managed by cloud Administrators but cloud administrators may also be hackers of your data, to which no security is provided by the cloud.

2. Steganography

Steganography is derived from two Greek words “stegos” mean “cover” and “grafia” mean “writing” that defines “covered writing”. It is the practice of writing data into hidden form which is known as Steganography. The data is hidden in media files such as images, so that other people are not able to know the presence of data behind image file. Steganography is different technique as compared to cryptography, as cryptography encrypts the data in unreadable form which a user can identify that this is an encrypted message but in case of Steganography, data is hidden so the user is completely unaware about the presence of data.

Below are two images one is original and in other the message is hidden behind the image using steganography.

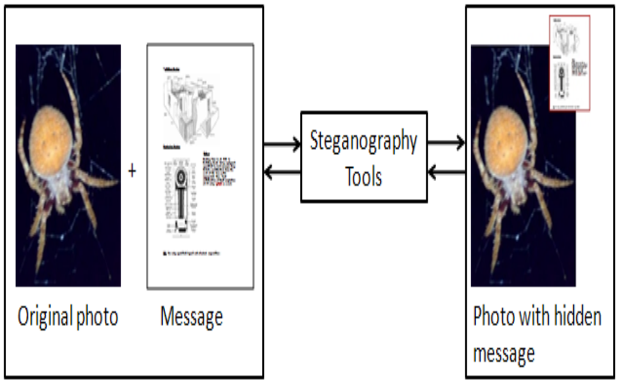

Fig 1. Original image fig 2:stego image

2.1. Method:

Two things are required in Steganography:

First, the message you want to hide and the second is cover media that will contain the message in it. The resulted file is called Stego file. There are various kind of media to hide data using steganography such as image, audio, Text, Video as shown below:

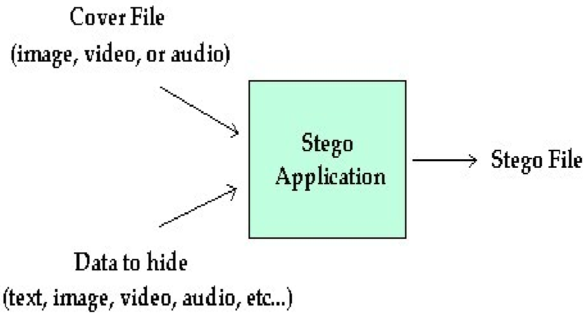

Fig 3.

2.2. Types of Steganography:

As people use to transmit multimedia (text, images, audio video) over the internet, most of the stenographic systems use these media objects as cover media for transmitting the secret message embedded within these objects. According to the type of media, stenography can be divided into following types:

1. Text Steganography
2. Image Steganography
3. Audio Steganography
4. Video Steganography
5. Protocol Steganography

We will have a short look of following kind of steganography methods in this paper:

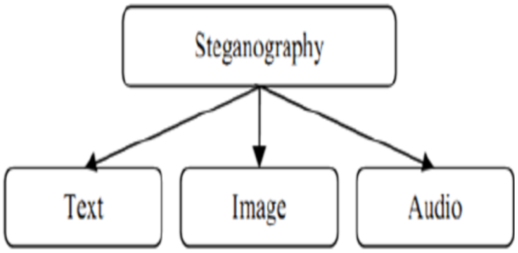

Fig. 4

2.2.1. Text Steganography

This method is used to hide text behind other text file. This is one of the difficult methods of Steganography as vast amount of text is required to hide the data in secret files.

Following are the different coding techniques for text steganography. Depending upon the user requirement, these can be used jointly or separately. Each Technique has its pros and cons as discussed below:

1. Line-Shift Coding

In this method a document is altered by shifting the text lines locations vertically to encode a document. A line has two ends upper and lower, to encode a document these ends are marked and to hide bit 1, the line is shifted downward and to hide bit 0, line is shifted upward. The distance of the marked end is measured to identify the line shifting.

This type of coding can be applied to the bitmap of a page image or to the format file. In some cases to decode the messages original images is not needed as only the spacing of line is measured.

2. Word-Shift Coding

In this methods the words are shifted horizontally to encode a document i.e. the words are shifted within the text lines. Bit 0 represents left shift while Bit 1 represent right shift. Correlation method is used to identify. This method requires the knowledge of distance algorithms to implement successful steganography.

This type of coding can be applied to the bitmap of a page image or to the format file. Original image is used to decode the message.

3. Feature Coding

In this method some words or text is altered depending upon the code word. The image is examined and the parser identify text features to locate whether the text is altered or not. For example, length of stroke in letters t and f, points in letters j and I, or by increasing/ decreasing the height of letters d, b, n, h etc.

This type of coding can be applied to the bitmap of a page image or to the format file. Original image is used to decode the message to specify the pixel of alteration. This kind of encoding can be done in either direction i.e. either horizontally or vertically.

2.2.2. Image Steganography

Image Steganography is known as the techniques to hide the text image within an image in such a way that no one can identify the present of hidden message. Images are the most popular cover media used to hide a message. For image Steganography, compression techniques play an important role. Lossy compression techniques can embed more data as they have very small size as compared to lossless compression. Asimagefiles have different file formats, so different kind of techniques are used for image Steganography. These techniques are: Image Domain and Transfer Domain.

1. Image Domain

Image domain is also known as spatial domain. An image consists of pixels and number of bits are required to represent each pixel. Image domain technique uses these pixel intensities to embed secret messages. This techniques encompasses bit-wise method to apply steganography. Bits are inserted to encode a message and noise manipulation is used to detect the secret message.

2. Transform Domain

Transform Domain is also known as frequency domain. Images are transformed to embed and a message and after transformation the message is embedded.This kind of technique requires the knowledge of image transformation and manipulation of algorithms. Transfer domain is independent of image file formats.

2.2.4. Audio steganography

Audio Steganography is used to transmit a hidden secret message by altering an audio signal.Basic model is shown below in Fig. 5.

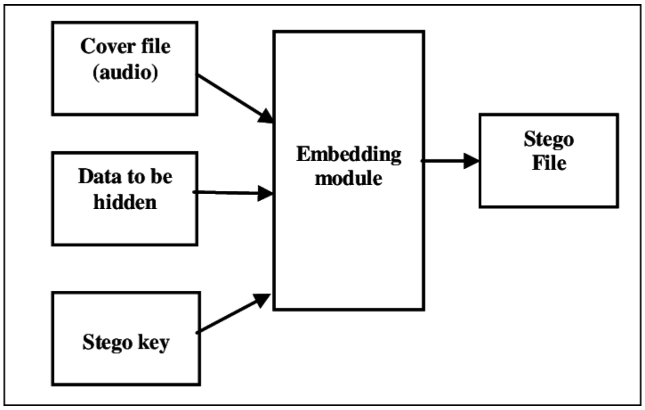

Fig. 5

The model consists of following:

Carrier (Audio file)- It is also known as stego file which consist of embedded message.

Message (Data to be hidden)-Message is the data that user wants it to be secret or confidential. It can be plain text, image or any kind of file.

Stego Key (Password)- It is an unique key to ensure that the authorized recipient decode the message. Because the receiver who has the corresponding decoding key will only be able to extract the message.

Message hiding process in audio files consists of following two steps:

i. Identify the redundant bits in a cover-file. These bits are those bits that do not affect the quality or of audio file after modification.
ii. Embed the secret message in the cover-file by modify or replace these redundant bits with the bits of secret message.

3. Conclusion

Steganography is a techniques to hide a secret message within a media file and Cryptography is the technique to encode a message into some non-readable form. These two technologies can be combined together to provide more security and privacy of data. A double level of security can be provided as the message is hidden using steganography and again is encrypted using some kind of cryptography like DES or AES.

Combining Steganography and cryptography techniques ensure double level of security. This may enhance the security but quality of signal or data may be degraded. So, this demand extra efforts to ensure the quality of the data. Alternate method is to use Steganography with an embedded key known as stego key. In future we can develop algorithms to cover huge amount of data in cover files.

4. References

[1] Patidar , S "Survey on cloud computing" , in Advanced computing and communication technologies , IEEE , Jan-2012..
[2] M. Vijayapriya, "Security algorithm In Cloud Computing: Overview"/ International Journal of Computer Science & Engineering Technology (IJCSET)
[3] Rashmi Nigoti, Manoj Jhuria & Dr. Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing. In International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (print) 2279-0047, ISSN (online):2279-0055.
[4] B.Arun & S,K. Prashanth, " Cloud Computing Security Using Secret Sharing Algorithm" in Indian Journal of Research, ISSN- 2250-1991, Volume:2|Issue: 3| March 2013.
[5] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan & Bhavani Thuraisingham, "Security Issues for Cloud Computing" in International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.
[6] Ew Approach to Hide Text in Images Using Steganography" in International Journal of advanced Research in Computer Science and software Engineering, ISSN:2277 128X, Volume 3, Issue 4, April 2013. [7] V.K. Zadiraka & A. M. Kudin, " Cloud Computing In Cryptography And Steganography", in Cybermetics and Systems Analysis, Vol. 49, No. 4, July-2013, UDC 681,3;519,72;003,.26
[8] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing ", Journal of Network and Computer Application, vol. 34, issue 4, pp 1113-1122, July 2011, Academic Press td London, UK.
[9] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. of ICDCS '08, pp. 411–420, 2008.
[10] Sandeep Sahu Aditi Bhadoria, " Survey on Cloud computing security using steganography",International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 8, August 2015