Data Hiding Images Using Spread Spectrum in Cloud Computing

Mr.S.S.Aravinth, Assistant Professor / CSE, 6112-Knowledge Institute of Technology, Salem, Tamilnadu, India. Mail: ssacse@kiot.ac.in Mobile: 98944 – 48683
Mr.B.Rajkumar. Assistant Professor / CSE, 6112-Knowledge Institute of Technology, Salem,
Mr.M.Ramkumar, Assistant Professor / CSE, 6112-Knowledge Institute of Technology, Salem,
Miss.M.Kavipriya, III / CSE, 6112-Knowledge Institute of Technology, Salem, Tamilnadu, India.
Miss.M.MohanaPriya,III / CSE, 6112-Knowledge Institute of Technology, Tamilnadu Salem.India
Miss.M.Kalaivani,III / CSE, 6112-Knowledge Institute of Technology, Tamilnadu Salem.India

Abstract

Communication is the god given gift that enables intellectual and cultural exchange and builds up our competence in social behaviour. So now we are living in the information age. The internet and cloud computing has taken communication to unimaginable attitudes. Cloud computing entrusts remote services with a user's data, software and computation. But many questions arise when we think of security. Is Cloud computing communication private and security? But encrypted messages can still be tracked revealing who is talking to whom. The term Cloud Computing refers to the concept where the shared servers provide resources such as data, software to the clients. In order to use a Cloud service all you need is a web browser and an internet. The biggest Disadvantage in cloud computing is the data security. Because the data that is being stored in the cloud will be stored in the cloud provider's server and hence this results in hacking of data by unauthorized person. In the business model using software as a service, users are provided access to application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run.

In this paper we gave our proposal, how we can secure our data in cloud computing. Our idea is based on implementing the Spread spectrum Image. Steganography's (SSIS) in cloud computing platforms .we hope it will be very beneficial for the user who loves cloud platform but hesitating to use because of the data security issue.

Keywords: Unauthorized person, Cloud computing security, Spread spectrum Image, steganography's

Introduction

Cloud computing" is the next natural step in the evolution of on-demand information technology services and products. As we said earlier the biggest issue in the cloud computing is its data security. Since, the data that is being uploaded will be available only in the cloud provider server in some encrypted form that is made by the cloud provider. When our data is present in some one's server there is a big chance of our data is being hacked. In order to make our data secured in cloud platform the best idea according to me is to upload the data in the image encrypted form. Hence, this provides double level security since the data will be normally stored in an encrypted form in the server.

I. Top Threats To Cloud Computing

- 1: ***Account or Service & Hijacking***
- 2: ***Insecure Interfaces and APIS***
- 3: ***Malicious Insiders***
- 4: ***Shared Technology Issues***
- 5: ***Data Loss or Leakage*** **II. Our Concept**

II.I What Is Actually Happening?

- 1) When a user opens his cloud platform and creates a file in that, which may contain some essential data.
- 2) When the user logs off his cloud platform the data that is created by the user will be stored in the cloud provider's server in an encrypted form.
- 3) When the user re login into his cloud platform the data will be decrypted from the server and given to the server.

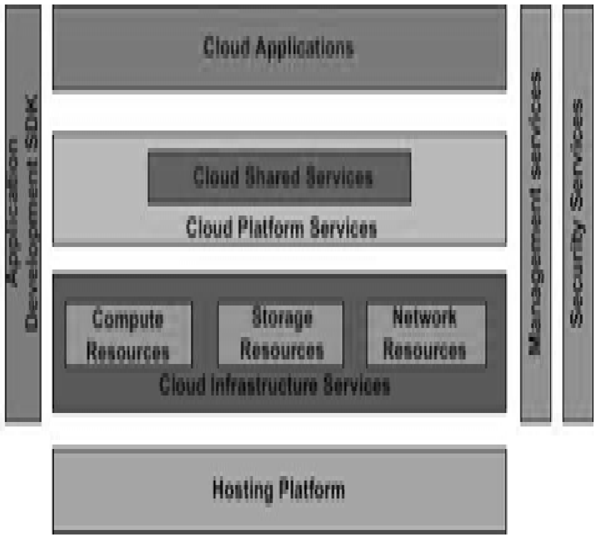


Fig1CloudArchitecture

II.II Issues

1) The biggest issue now is the server can be hacked by the hackers and the data can be decrypted. Hence, user data is lost.

2) From the above figure, it is clear that in the cloud computing each and every component such as software, data storage is provided as a service.

3) From the above figure, it is clear that in the cloud computing each and every component such as software, data storage is provided as a service.

4) Although it reduces the cost of hardware it is not much reliable because of the data that is being directly stored in provider server.

III. Spread Spectrum Image Steganography for Data Security

III.I Spread *Spectrum?*

Spread-spectrum communication describes the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. SSIS uses this technique to embed a message, typically a binary signal, within very low power white Gaussian noise.

The resulting signal, perceived as noise, is then combined with the cover image to produce the stego image. Since the power of the embedded signal is low compared to the power of the cover image, the SNR is also low, thereby indicating low perceptibility and providing low probability of detection by an observer. Subsequently, an observer will be unable to visually distinguish the original image from the stegoimage.

IV. What is Steganography?

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. More commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

IV.I *Steganography in Cloud Computing*

Steganography techniques can be used to provide a perfect tool for data exfiltration, to enable network attacks or hidden communication among secret parties.

Fig 2. Hiding data in an image [2]

The aim of these techniques is to hide secret data (steganograms) in the innocent looking carrier e.g. in normal transmissions of users. In ideal situation hidden data exchange cannot be detected by third parties

IV.II *Different Kinds of Steganography*

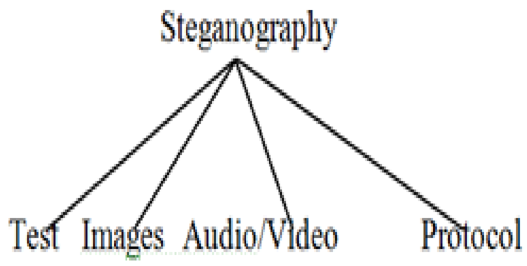


Fig 3.Variants of steganography [Morkel and Eloff (2005)]

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [Currie and Irvine]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [Anderson and Petit colas (1998)]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 4, shows the four main categories of file formats that can be used for steganography. Hiding information in text is historically the most important method of steganography. This paper will focus on hiding information in images by using spread spectrum image steganography in the next sections. To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound [7].

V. Spread Spectrum Image Steganography and Its Working Principles

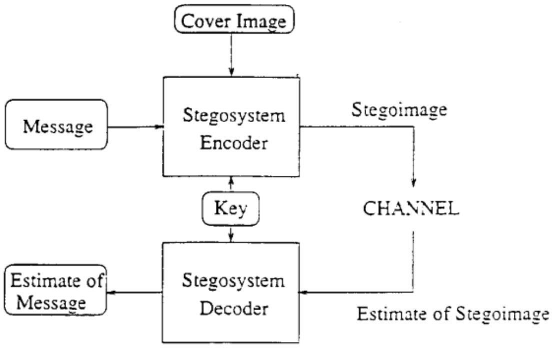


Fig 4. Steganogram Generator [Boncelet *et al* Newark and M.Marvel(2003)]

Spread Spectrum Image Steganography (SSIS) works by storing a message as Gaussian noise in an image At low noise power levels, the image degradation is undetectable by the human eye, while at higher levels the noise appears as speckles or “snow.” The process consists of the following major steps, as illustrated in figure 5 and figure 6.

1. Create encoded message by adding redundancy via error-correcting code.

2. Add padding to make the encoded message the same size as the image.

3. Interleave the encoded message.

4. Generate a pseudorandom noise sequence, n.

5. Use encoded message, m, to modulate the sequence, generating noise, s.

6. Combine the noise with the original image.

Notice that original image is not required to recover the original image. A filter is used to extract the noise from the stegoimage, resulting in an approximation of the original image.

The better this filter works the fewer errors in the extracted message.

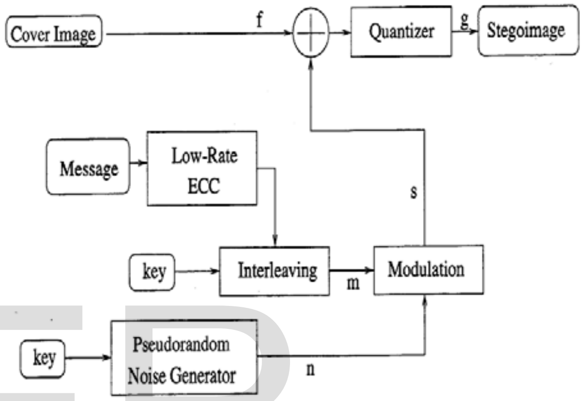


Fig 5. Simplified Steganography Embedder

VII. Implementation details

So for we have discussed about the SSIS working principles now are going to implement this SSIS concept in the Cloud Infrastructure service layer. This layer is especially for storing huge amount data,so we can store and transfer the information in the image, so it yields the essential security for data. The figure 9 shows the Layers in the cloud infrastructure as a service platform, in this the we have to implement the SSIS concept in the top of the layer, the SSIS will act as a gate keeper, and it does the job of Encoding and decoding process.

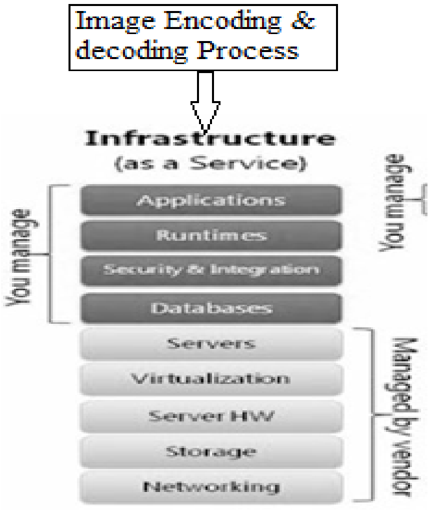
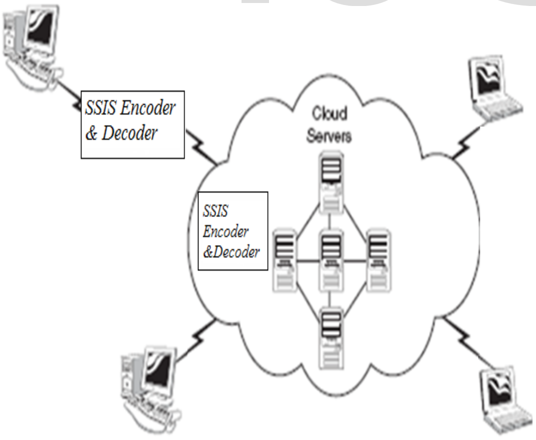


Fig 6. A view of infrastructure as a service platform

Fig 7. SSIS working overview



VII.I *Implementations Steps*

Our idea is totally based on the user point of view not from the cloud provider point of view. (i.e.) For the users who love to use cloud platform but hesitating to do that because of the data security issue.

1) When a user going to store a data in the cloud platform.

2) User going to store the data in an encrypted (Data inside the image) forms.

3) We are going to develop software that helps the user to embedded the data into the image.

4) The user is requested to run the software more than once on his data.

5) The no. of times the data is being encrypted is known only to the user. This is the key here.

6) Then, when the user log off his cloud platform. The data will be again encrypted and stored in the server.

7) Now when the hacker hacks the data in the server. He is sure that the data is stored in only one encrypted form.

8) But, the user already encrypted the data more than once with the help of the software.

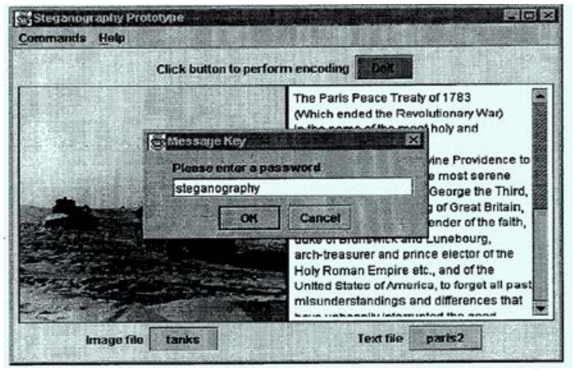
9) Even though the hacker finds out that the data is in encrypted (image) form by the user.

10) User is not sure how many times it is being encrypted.

11) When the user re login and decrypts the data key no. of times the original data is obtained in any computer.

12) Hence, this provides security to data from the user's point of view.

VII.II *Hiding a Message*

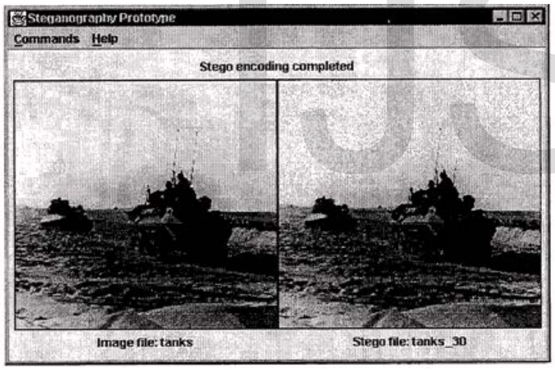


Click button to perform encoding

The Paris Peace Treaty of 1783
(Which ended the Revolutionary War)
... holy and
...ine Providence to
...e most serene
...George the Third,
...of Great Britain,
...ender of the faith,
...Lunebourg,
arch-treasurer and prince elector of the
Holy Roman Empire etc., and of the
United States of America, to forget all past
misunderstandings and differences that

Please enter a password

steganography



Stego encoding completed

Image file: tanks

Stego file: tanks_30

Image Estimation:

Pre Filtering:

VIII. Benefits of This Method

- Spread spectrum techniques satisfy most requirements and are especially robust against statistical attacks, since the hidden information is scattered throughout the image, while not changing the statistical properties.
- It can be used for all steganography application, although its highly mathematicaland intricate approach may prove too much for some.
- SSIS provides the ability to hide and recover, error free, a significant quantity of information bits within digital images, avoiding detection by an observer.
- SSIS has been shown to be a powerful way to transmit messages via normal channels without an observer detecting them.
- Easy to encode and decode the data in the image in the cloud environment.
- SSIS is a blind scheme because the original message is not need to extract the hidden message, so encoding and decoding automatically.
- Low error rate and payload, BER correcting ability.
- Resistance against both visual and statistical attacks.
- Uses a common image format and carrier medium (JPEG).

Conclusion

cloud computing as a carrier for secret communication is not very different from any other popular steganography carriers e.g. like IP telephony. The main novelty in this area when compared with known hidden data exchange opportunities is possibility of enabling secret communication between two instances of cloud services. Steganography should be treated for cloud computing environment as a rising threat to the network security as it is seen for typical networking ones.

We Presented in this paper hidden communication scenario as well as the threats that steganography methods can cause must be taken into account when designing secure cloud computing services. In order to minimize the potential threat of malicious use of steganography to public security effective steganalysis (detection) methods are needed.

This requires in-depth understanding of the functionality of particular cloud service and the ways it can be used to enable hidden communication. Considering however variety and complexity of the cloud computing services there is not much hope that a universal and effective steganalysis method can be developed. We hope it will increase the Data security of Cloud computing…

"If privacy is outlawed, only outlaws will have privacy ".

References

[1]http://technologywall.files.wordpress.com/2011/11/cloud_computing_structure.png?w=535&h=484.

[2]http://blogs.msdn.com/cfs-file.ashx/__key/CommunityServer-Blogs-Components-WeblogFiles/00-00-01-17-43-metablogapi/7317.image_5F00_6D6EC8C3.png

[3]http://3.bp.blogspot.com/-6tBPrwtmPnM/T97yncHGnLI/AAAAAAAAAGs/sJnJ7xhvhH4/s1600/spy-carousel.jpg

[4] T. Morkel 1, J.H.P. Eloff 2, M.S. Olivier on**"***an overview of image steganography".*

[5] Currie, D.L. & Irvine, C.E., *"Surmounting the effects of lossy compression on Steganography"*, 19th. Edition.

National Information Systems.

[6] Anderson, R.J. & Petitcolas, F.A.P., *"On the limits of steganography"*, IEEE Journal of selected Areas in Communications, May 1998

[7] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*