Steganography & Steganalysis Using Service Oriented Architecture

Dipesh Agrawal **Nishant Khare**

***Abstract* — This paper illustrates basic steganography techniques that can be organized using a service oriented paradigm, which is popularly known as a new generation distributed computing platform. Paper describes how steganography techniques can be used with distributed environment using service oriented architecture. SOA is a mechanism to develop platform independent, reusable and autonomous blocks of functionalities, called services.**

***Key Words* — Service Oriented Architecture (SOA), Steganalysis, Steganography.**

I. INTRODUCTION

As technology is growing, there is a rapid increase in use of computers by individuals. This result in large information sharing through networks among various devices like Laptops, Mobiles, Smart phones and other handheld devices. This communication among the devices having heterogeneous hardware and software platforms requires two things. One is a robust software environment which can work on existing network infrastructure and can support heterogeneous software platforms of various devices. Second is, a secure way of communication which can keep users data secure from intruders while it is transmitted through a network.

II. RELATED WORK

A. Steganography

To provide security over such heterogeneous platform, we have two information hiding mechanisms with us, Cryptography & Steganography. In cryptography, at sender side, an original message is encrypted using any encryption algorithm along with some special keys and the same message is decrypted at receiver side using relevant decryption algorithm along with some keys that are provided with receiver[1]. Another mechanism, steganography, refers to hiding information by embedding within unremarkable cover media. So, if intruder gets the message, it can see only the cover media and not the original message. Various steganography algorithms are proposed for different kinds of media and for different kinds of accuracies.

The paper describes how various steganography techniques for different media and some steganalysis methods that can be used with a new generation distributed computing environment – SOA. An online, service oriented steganography environment is described.

For this, web service mechanism is used to develop basic unit called Services, to communicate over the network in a heterogeneous platform.

Steganography can be used with various media like – Text, Images, Audio and Video. There are various techniques for each media.

For text steganography – A secret message can be hidden in a formatted text cover for ex. SMS texting [2].

For image steganography – LSB (Least Significant Bit) [3], Masking and Filtering methods can be used.

For audio steganography – techniques like Low Bit Coding (LBC) [4], Bit Modification Technique [5] can be used.

For video steganography – Least Significant Bit (LSB), data can be hidden into video streams [6].

B. Steganalysis

It is a technique of detecting secret messages embedded in original information. There are two types of steganalysis – Blind Steganalysis and Targeted Steganalysis.

In blind steganalysis, an algorithm which is used for steganalysis can detect all forms of steganography.

Some techniques used for blind steganalysis are: Blind steganalysis of JPEG image using calibration and Blind Steganalysis in Spatial Domain.

In Targeted Analysis, algorithm which is used for steganalysis can detect some specific forms of steganography.

Techniques used for this are – LSB Embedding and the Histogram Attack, Simple Pair Analysis.

C. Service Oriented Architecture

Above mentioned techniques of Steganography and Steganalysis can be implemented using service oriented environment using various tools like – Microsoft's Visual Studio 2008, Sun Microsystems's J2EE platform etc. Basic building blocks of SOA are – Web Services, Web Services Description Language (WSDL), simple Object Access Protocol (SOAP), Universal Description Discovery & Integration (UDDI), Extensible Markup Language (XML) etc [7]. These components helps to develop a platform independent environment required for various web services to communicate with each other. SOA can be treated as a new generation distributed computing environment and it can feature all the characteristics of distributed computing; like- transparency, mobility, availability, heterogeneity,

scalability, reusability and so on.

D. Implementation View

To have this Service Oriented view of above steganography techniques, we will have to consider following steps [8].

Define services for secret messages (i.e. for stego) – in this step, we can define each secret message as an independent service. So that these messages can be embedded with cover.

Define services for cover – in this step; we can define an independent service for each cover types. Using these covers, we can hide secret information.

Define service for storage – in this step; we can define services to store secret message and cover.

Define services for steganography algorithms – in this step; we can define services which can include algorithmic steps for each steganography technique.

Define services for steganalysis algorithms – in this step; we can define services to detect secret messages from available information.

III. ADVANTAGES

The proposed system provides us a new generation platform independent distributed environment steganography and steganalysis, for various media.

CONCLUSION

We can hide secret messages using various techniques and we can detect the secret messages back from the available information, using various algorithms and techniques. We can break all these things in the form of independent services, that can communicate with each other in an organized way said, to generate a customized application according to users need, by collecting required services in an application.

REFERENCES

[1] Piyush Marwaha and Presh Marwaha, "*Visual Cryptographic Steganography in Images"*, 2nd International Conference on Computing Communication and Networking Technologies 29-31 July, 2010.

[2] Mohammad Shirali-Shahreza, "*Steganography in MMS"* ,Multitopic Conference, 2007, INMIC 2007, *IEEE International.*

[3] Ming, Zang Ru, Niu XinXin, Yang Yixian, "Analysis of Current Steganographic Tools: Classifications and Features", Proceedings of the 2006 International Confrerence on Intelligent Information Hiding and Multimedia Signal Processing.

[4] Masahiro Wakiyama, Yasunobu Hidaka, Koichi Nazaki, "An audio Steganography by a low-bit Coding Method with WAVE Files", Sixth International Conference on Information Hiding and Multimedia Signal Processing, 2010.

[5] Kaliappan Gopalan, Qidong Shi, "Audio Steganography Using Bit Modification – A Tradeoff on Perceptibility and Data Robustness for Large Payload Audio Embedding", Computer Communications and Networks (ICCCN), 2-5 Aug. 2010.

[6] Daniela Stanescu, "Embedding Data in video Stream Using Steganography", Applied Computation Intelligence and Informatics,2007. SACI 2007, 4th International Symposium on, 27-28 May 2007.

[7] Sandro Geric, Neven Vrcek, "Prerequisites for Successful Implementation of Service Oriented Architecture, Proceedings of the ITI 2009, 31st International Conference on Information Technologies Interfaces, June 22-25, 2009Cavtat, Croatia.

[8] Pooia Lalbakhsh, Sepideh Ravanbakhsh, "Service Oriented Steganography*", International Conference on Signal Processing Systems 2009"*.

AUTHOR'S PROFILE

Dipesh Agrawal
Is doing M.Tech (IT) from NRI Institute of Information Sciences & Technology, Bhopal. His areas of interest are Multimedia Systems, Distributed Computing, and SOA.

Nishant Khare
Has completed M.Tech from Rajiv Gandhi Technological University, Bhopal. He is working as an Associate Professor in NRI Institute of Information Sciences & Technology, Bhopal. His area of interest are Data Mining, Distributed Computing.