International Journal of Computer Networks and Communications Security

VOL. 2, NO. 11, NOVEMBER 2014, 379–385
Available online at: www.ijcncs.org
ISSN 2308-9830

A Secure Job & Demand Based Steganography

Mustafa Alfayoumi

College of Computer Engineering & Sciences, Salman Bin Abdulaziz University, Saudi Arabia

E-mail: tariqsamad84@gmail.com

ABSTRACT

Steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. In this article, I will discuss what steganography is, what purposes it serves on and will illustrate distributed framework based on job based architecture, on which a logical transparent steganographic layer is developed and have related work on steganography and its anatomy is semantically studied and broken down into some independent services which are allocated on a network infrastructure. This structure not only distributes the overall load of the process, it also considers some important system attributes such as reusability, simplicity, outsourcing, maintainability, flexibility and availability. Because of the open structure of the system, varieties of steganography algorithms can be supported for varieties of secrets, according to an evaluation strategy which is also considered as a service on the network. To clarify the proposed approach, the related ADL model together with an example scenario is expressed.

Keywords: *Steganography, ADL Model, Network Infrastructure, Job based Architecture.*

1 INTRODUCTION

There are a large number of steganographic methods that most of us are familiar with (especially if you watch a lot of spy movies!), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding information, such as:

- Covert channels (e.g., Loki and some distributed denial-of-service tools use the Internet Control Message Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system)
- Hidden text within Web pages
- Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\winnt\system32 directory?)
- Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files.

These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and then decrypt it.

There are a number of uses for steganography besides the mere novelty. One of the most widely used applications is for so-called digital watermarking. A watermark, historically, is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function; a graphic artist, for example, might post sample images on her Web site complete with an embedded signature so that she can later prove her ownership in case others attempt to portray her work as their own.

Stego can also be used to allow communication within an underground community. There are several reports, for example, of persecuted religious minorities using steganography to embed messages for the group within images that are posted to known Web sites.

The rapidly growing of communication-based systems and the extensive injection of information age tenets into various applications from ordinary to critical areas in 21st century, caused many consequences which necessitate a great change in the way many kinds of works are performed. Although the basic concepts are identical, the thoughts and manners are totally different, particularly when the concept of value is being transformed from technology into information. The emergent improvements of networked environments such as distance shrinking and availability, together with sophisticated data manipulation strategies caused networks to be the strictly dominant infrastructures of the new age anatomy [1]. In such a planet size information cloud, information management can be considered as the most important challenge. Defining information as value, it is evident that information security against unauthorized access is also a vital aspect of the new age communication systems, on which, millions of users from humans to artificial agents are interacting [2].

Although we are talking about the information age, security issue is not a modern concern, while it has always been involved in human life as a basic need which is usually satisfied by some kinds of information hiding methods according to their existing possibilities. Making use of hidden tattoos or invisible inks are some instances of information hiding strategies used in the past.

Generally speaking, information hiding can be discussed in two major categories namely: cryptography and steganography, while each can be further divided in turn. The goal of the cryptography is concealing the context of message. It scrambles a message according to a prescribed encryption algorithm, so it cannot be understood by the interceptors [3]. The receiver then uses some special keys to decode the message, without which, the encryption process is possible, but takes a considerable length of time. This issue can be considered as the major drawback of cryptography [4]. On the other hand, steganography tries to hide the messages by embedding them within unremarkable cover media, so as not to arouse an eavesdropper's suspicion on the final composite date which is termed as stego [5]. These algorithms may also take advantage of security keys or even pre-encrypted messages to ensure the efficiency of the steganography process. Various steganography algorithms are proposed with different levels of accuracy, which require different kinds of covers and are proposed for different types of messages.

The paper focuses on steganography as one of the information hiding methods and proposes a service oriented structure to form an online steganography environment. It prepares a distributed strategy for a comprehensive and dynamic steganography process which improves reusability, facilitates system management, reduces complexity, and improves the overall security. Making use of the granular nature of the underlying service oriented architecture, the proposed strategy not only supports the current algorithms, it also provides an open architecture for the future algorithms. In addition to the mentioned benefits, our proposed strategy is able to present optimal dynamically generated steganography algorithm according to the incoming message and system possibilities and resources. In such a service oriented infrastructure, even a bit of information can be used to enrich the generated stego.

2 STEGANOGRAPHY AS AN INFORMATION HIDING STRATEGY

As an information hiding strategy, steganography has a remarkable advantage than the other methods. Unlike cryptography, steganography hides the very existence of the message itself by concealing it within another perceptible message with meaning disjoint by the original one. In computer-based applications, the original message is called secret, the second message is called the cover, and the resulted steganographic message is called stego (we use this terminology in the rest of the paper). The kinds of the secret and also the cover may be in text, picture, audio, and/or video formats. The concept of steganography can be also used in watermarking and digital fingerprints to protect copyrights particularly in multimedia products [6]. The steganography process accomplishes through a predetermined algorithm according to message types and the environment in which the communications are performed. An extensive range of steganography algorithms are proposed for network environments, and most of them focus on image formats according to their extensive use particularly on the Internet. Taking a look at some of the previously proposed algorithms would well clarify our goals.

A. Image steganography algorithms

This category of steganography algorithms tries to hide a message within an image cover. The most important factor of the cover image in such

algorithms is the fact that how many bits of noise (parts of secret message) can be injected without perceptually deteriorating the image quality, while a noisy image would arouse the interceptors' suspicion [7]. Common existing approaches of hiding information in digital images include [3]:

- Least significant bit insertion (LSB): this simple approach tries to hide information within the least significant bits of pixel colors of an image (some algorithms also modify the second least significant bits). The secret may be embedded within 24-bit or 8-bit BMP or GIF images. The main disadvantage of this method is its vulnerability to even slight image manipulations. Image conversions to lossy formats can also destroy the hidden message.
- Masking and filtering: these techniques usually restricted to 24-bit and gray-scale images, hide information by marking an image, similar to paper watermarks. Since watermarking techniques are more integrated into the image, they can be applied in applications involving lossy compression. These techniques can also be applied into other multimedia (audio/video) applications.
- Algorithms and transforming: unlike LSB which is vulnerable to data manipulation, these techniques can be applied on lossy compression formats like JPEG images. These approaches may help protect against image processing manipulations such as cropping and rotating.

The selection of such algorithms should be accomplished according to the system mission and the environment. For example a BMP steganography algorithm may not be appropriate for Internet communication, on which JPEG images are the most popular formats because of their high quality-low size attribute. Using such an algorithm may be a hint for the opponent entities.

B. Text steganography algorithms

Text steganography tries to hide a secret in a text formatted cover. The secret can be a binary message hidden between the words or follow a conceptual manner. Some other approaches consider the text cover as a simple image and try an image-based steganography algorithm [8]. Other approaches include special way of writing. For example author in [9] proposed using acronym/complete form of some predetermined words to convey a binary message. In such a case, the complete representation of a word corresponds to a 1 and the acronym form corresponds to a 0. Another simple algorithm is placing alphabets of the secret message as special alphabets of another meaningful cover message. The first paragraph of [10] includes such an interesting message. In formatted text which can support different fonts, font styles, or font sizes, the way of writing may imply a secret. The unorganized words in the poem titled Guide to Heaven [11] can be a nice example of such a method. Because of low capacity of text for hiding data, these approaches may be used only for limited applications and thin clients which use simple protocols such as SMS (short message system) or MMS (multimedia message system)[12, 13].

C. Audio/Video steganography algorithms

Although Audio and video files can also be used as steganographic media, it is mostly accomplished only for water marking for copyrighted multimedia products, because of their large sizes. Most of the proposed approaches in audio/video steganography depend on the medium format. For example some of the algorithms cannot be applied on compressed format, while some others can [14]. On the other hand, most of the proposed algorithms in this category use similar methods as image steganography such as LSB [15], or special transformations [16]. In audio files small echoes or slight delays can be included or subtle signals can be masked with sounds of higher amplitude [17]. The extensive availability of audio/video programs on radio and TV is one of the most valuable features of such media to convey confidential messages to an extensive range of companies using a kind of online steganography [8].

D. Steganography by other carriers

In addition to the mentioned carriers, some other digital entities can be applied as cover media [17]. For example HTML files (hypertext markup language) have appropriate potentials for information hiding. While processing an these files, the browser ignores spaces, tabs, certain characters and extra line breaks which could be used as locations for hiding information. Unused or reserved space on a disk can be also used to hide information. Data can be hidden in unused space in file headers. Some authors propose network protocols such as TCP, UDP, and/or IP for hiding

the messages and transmit them through the network [3].

Using any kind of medium as steganography carrier, it should be noted that the entropy of the embedded material should be much less than the uncertainty in the opponent's measurement of the entropy of the cover media [18]. Another alternative is making use of appropriate strategies to reduce the entropy of the cover media by an amount that can be made up by adding the secret. The following equation shows the relations between stego entropy H(S), secret entropy H (E), and cover entropy

$$H(C).\ H\ (S) = H\ (C) + H\ (E)$$

3 JOB ORIENTED ARCHITECTURE (JOA)

The concept of service oriented architecture or SOA deals with reducing the organizational expenses through optimizing resource management from human to other system resources in order to reduce organizational costs and increase the overall throughput and efficiency [19]. The basic tenet of SOA is reusability of the organizational resources. In a service oriented architecture, a resource can be accessed at any time, by each authorized entity, from anywhere at the system. On the other hand, the dispersed independent services can communicate to each other to make new composites for new organizational businesses. This availability and granularity makes a flexible and comprehensive environment for multidisciplinary applications such as steganography. One of the important features of service oriented architecture is using a common language among the system nodes which introduces it as an appropriate approach for distributed heterogeneous environments.

We implemented a basic version of our proposed algorithm through web services as one of the existing SOA implementation approaches with the following standards [20]. Fig. 2 shows how they work together.

- SOAP: Simple Object Access Protocol is a W3C standard defining protocols for passing objects using XML (Extensible Marked up Language). A SOAP runtime system enables a client to call methods on a SOAO-enabled service, passing objects in XML format.
- WSDL: Web Service Description Language is also a W3C standard which is used to describe a web service interface.
- UDDI: Universal Description Discovery and Integration is a protocol for web-based registries that contain information about web services such as the location of its WSDL file.

Many web service implementation tools have been developed that support the above standards. We used J2EE 1.3 (Java 2 Enterprise Edition) through Borlang Jbuilder 2006 to develop our services because of their open structure and flexibility. Apache Tomcat 5.5 is also selected as the underlying server for our standalone servers.

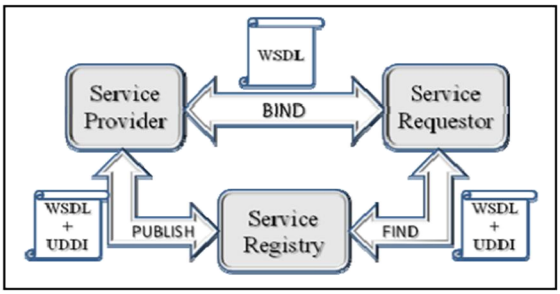

Fig. 1. Web service standards and their relations in JOA

4 JOB ORIENTED STEGANOGRAPHY

The initial step to setup a service oriented environment is defining the needed services and their relations. For this reason we tried to conceptually break down a steganography process in to atomic or near-atomic concepts which can be then implemented as services. These services are then independently allocated on an underlying network. Therefore each steganography process can be dynamically formed through service integrations according to an evaluated plan. Such a comprehensive approach can eliminate the restriction of static steganography algorithms and their necessary stovepiped components. Our system can make use of all the existing possibilities regardless of their different hardware/software platforms, languages and so on. On the other hand new features can be added to the system as a new service without any other modifications.

A. Anatomy of Steganography and Services

If we concentrate our attention to the semantics and concepts of steganography, regardless of a specific algorithm, we will find following common concepts in all the steganography algorithms:

- Secret: originally the goal of steganography is to hide secret information.

- Cover: any type of carrier to hide the secret.
- Algorithm: a sequence of predetermined manipulations to embed secret within the carrier.

According to the above concepts the system has two inputs which are a secret and a cover together with one output which is the generated stego. Since the traditional systems accomplish steganography according to a preassumed algorithm, various limitations are imposed into the system for selecting type of the cover medium or some of its detailed attributes. In the other words you cannot use every type of cover with that specific algorithm. On the other hand that specific algorithm is designed merely for a special class of secrets. The proposed strategy faced this problem by granularity and dynamic service composition. We implemented every required process as a service on the network, each are independently functioning and able to communicate to the other services, therefore a steganography process contains a sequence of service invocations. Some of these services include:

- Encryption Service: our SOA is working on a network and a complete steganography is accomplished as a result of several service interactions. Such a network is protected against the external and unauthorized accesses. To guarantee the internal security of the system we also use an encryption service to initially encrypt the secret.
- Detection and Conversion Services: these services are responsible for required secret/cover manipulations. According to the variety of types for secret and the cover, we also used four detection and conversion services for text, image, audio, and video formats (it is sometimes needed to convert a cover into another format or to change its quality for some steganography algorithms).
- Network Monitoring Service: these services monitor the network traffic and the related parameters. They are able to detect travelling formats, protocols and data packets and make use of them to improve the steganography mission. The conceived information of this service can be used to form much optimal algorithms. For example, if an appropriate cover is outgoing, this service can use it in a piggybacking process for embedding and transmitting the secret.
- Algorithm Evaluation Service: this is the pivot service of the system, while its decisions lead to the selection of the final steganography strategy. This service evaluates the attributes of secret and also negotiates with the network monitor and other related services to determine an optimal steganography solution.
- Cover Finder Service: this service is responsible for finding the appropriate covers according to the evaluation service and selected algorithm. This service can make use of online covers or previously stored covers.
- Media Store Service: this service manages a media store which is storage for saving covers. It can update the storage media store with modified covers received from conversion services or import new qualified covers from the Internet.
- Steganography Algorithm Services: these services are responsible for the algorithmic manipulations of the steganography process. According to the monitoring results (prepared by monitoring service), evaluation queries (prepared by evaluation service), and the attributes of the secret message, the needed processes are accomplished through steganography algorithm services.

We diagrammed our proposed system using Architecture Description Language (ADL) to show how dispersed services connect to each other to accomplish the required operation. In this method, system entities are showed as blocks which are connected to each other through unidirectional connectors having a user role showed by a square and/or server role showed by triangle. The number written on these shapes correspond to the defined service interfaces [21]. Fig. 2 shows a general ADL for the proposed service oriented steganography. The following is a scenario which clearly describes how the system works.

B. Steganography Scenario

In this section we are going to explain a steganography scenario and the manner in which

services interact with each other to accomplish the task.

The scenario starts from the input block. It invokes encryption service through interface 8 to encrypt the message. According to the open structure of the system, the encryption algorithm can be produced through any single algorithm, or even another encryption SOA as an outsourcing process. The cover medium may be presented by the user or may be selected by the cover finder. Suppose there is no input covers, a request query triggers the cover finder to find an appropriate cover. It invokes evaluation service for the required details about the needed cover medium. Evaluation service makes use of network monitor and steganography services to form a cover attribute query (which may contain information about size, type, resolution, entropy, etc.) for media store to retrieve (the media store may search this cover in media store, or load it from the network). On the other hand, steganography services use converter services in a parallel process to accomplish the needed modifications on the secret or the selected cover. The last station of the scenario process would be the steganography algorithm services which apply the final manipulations and embedding processes to export the results to the external network.

5 ADVANTAGES OF THE SYSTEM

Since the system is based on SOA and the concept is break down as independent (and sometimes general purpose) services, the overall reusability and flexibility would be quite high. On the other hand each of these services can be considered as an atomic service to an organization according to the open structure of such environments which is vital characteristic particularly in steganography, while some of the processes may be classified in certain organizations. In such a case a service may be invoked in a blind manner without knowing the internal manipulations from an external organization. On the other hand, such an open architecture can integrate with other service oriented structures for additional missions. For example the proposed steganography approach can be integrated with the service oriented multimedia system proposed in [19] to form a semantic sophisticated steganography environment. Another advantage of the system is its platform independency. Since services are communicating through common standards and all the request/responses are accomplished through XML, different platforms can collaborate to each other in a totally transparent environment, thus any types of clients from thin to thick clients can easily use the system. Implementation simplicity can be mentioned as another important advantage of the system because of the simple and available standards used in the implementation process.

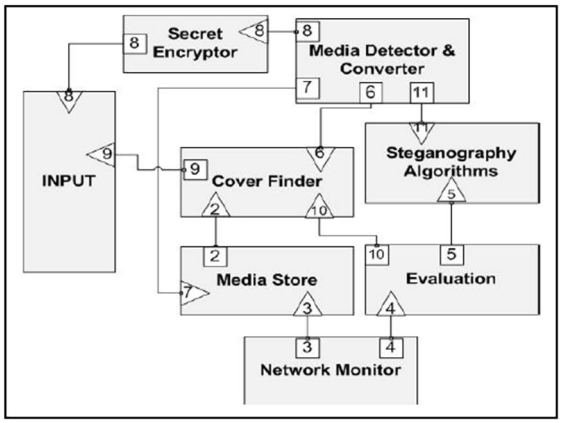

Fig. 2. General ADL diagram for job oriented steganography

6 CONCLUSION

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. But it is also quite real; this is not just something that's used in the lab or an arcane subject of study in academia. In addition to a novel approach in steganography, the authors were trying to introduce a roadmap toward future granular and distributed service oriented systems even in such special applications. Such approaches can be quite appropriate particularly when special missions are supposed to be accomplished on NGN like (next generation network) environments with different kinds of clients and servers such as NCW (network centric warfare) related systems or modern enterprise applications.

7 REFERENCES

[1] R. B¨ohme. Assessment of steganalytic methods using multiple regression models. In Information Hiding, pages 278–295, 2005.

[2] C.-C. Chang and C.-J. Lin. LIBSVM: a library for support vector machines, 2001. Software available at http://www.csie.ntu.edu.tw/_cjlin/libsvm.

[3] H. Farid. Detecting hidden messages using higher-order statistical models. In International Conference on Image Processing, Rochester, NY, 2002.

[4] J. Fridrich, M. Goljan, and D.Hogea. Steganalysis of jpeg images: breaking the f5 algorithm. in Proc. 5th International Workshop on Information Hiding(IH '02), pages 310–323, October 2002.

[5] T. Joachims. SVMLight Support Vector Machine, version 6.01, 2004. Software available at http://svmlight.joachims.org/.

[6] S. Katzenbeisser and A. P. Fabien. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

[7] S. Lyu and H. Farid. Detecting hidden message using higher-order statistics and support vector machines, 2002.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. Information hiding: A survey. Proceedings of the IEEE, special issue on protection of multimedia content, 87(7), pages 1062–1078, July, 1999.

[9] N. Provos. Defending against statistical steganalysis. 10th USENIX Security Symposium, pages 323–335, 2001.

[10] Y. Q. Shi, C. Chen, and W. Chen. A markov process based approach to effective attacking jpeg steganography. In Information Hiding, pages 249–264, 2006.

[11] K. Solanki, A. Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In 9th International Workshop on Information Hiding, Jun 2007.

[12] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210

[13] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY

[14] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[15] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[16] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[17] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[18] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[19] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[20] Dunbar, B., "Steganography techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[21] Bender, W., Gruhl, D., Morimoto, N. & Lu, A.,"Techniques for data hiding", IBM Systems Journal, Vol 35, 1996

[22] C.E., Shannon, (1949), Communication theory of secrecy systems, Bell System Technical Journal, 28, 656-715.

[23] N. F. Johnson and S. Katzenbeisser, .A survey of steganographic techniques., in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[24] G., Derrick, (2001), Data watermarking Steganography and watermarking of digital data, Computer Law & Security Report, 17 (2), 101-104.