HYBRID APPROACH TO PROVIDE STRONG AUTHENTICATION IN WIRELESS COMMUNICATION

B. Madhuravani[#1], **Dr. P. Bhaskara Reddy** [#2],**P. LalithSamanthReddy** [#3]
#1 MLR Institute of Technology, Dundigal, Hyderabad, India.
#2 MLR Institute of Technology, Dundigal, Hyderabad, India.
#3 Illinois Institute of Technology, USA.

Abstract

Security is the most important requirements to the wide acceptance of personal communication systems and authentication is the most essential procedure to ensure whether the service is properly used. In order to provide security services in wireless communication over the internet, authentication is used as an initial process to authorize a user for communication through secret credentials. Without strong authentication, mobile communication is unprotected through the release of message contents, modification of message or denial of service which can be accomplished easily by an intruder. As new services emerge, requirements for the security would be different depending on the applications. We propose a protocol that overcomes the security flaws existing in some present protocols. In addition, the proposed authentication scheme does not only protect user data, but also it prevents many kinds of attacks such as the replay attacks, guessing attacks or substitution attacks.

Key Words: *SOAP, DCT, DWT, JPEG*

1. INTRODUCTION

The Digital steganography is the art and science of hiding communications [1,2]; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent unconventional but promising steganography mediums[3]. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility).

This concept gives a general foreword to the research by primary explanation to the research background. Then, the main motivations of this study and the research problem are defined and discussed. Next, the research aim is identified based on the established definition of the research problem and motivations.

a. Information Security and Steganography

Essentially, computer and network security have some requirements that should be addressed in order to get secure systems. Thus, in order to determine the performance of a security technology, three key concepts should be analyzed: confidentiality, integrity, and availability. identifies these concepts as follows:

1. “*Confidentiality* deals with protecting, detecting, and deterring the unauthorized disclosure of information”. The main goal of cryptography is to garble a plaintext message in such a way that only the intended recipient can read it. This is precisely the goal of confidentiality[4].

2. “*Integrity* deals with preventing, detecting, and deterring the unauthorized modification of information”. An integrity attack is potentially more dangerous than a confidentiality attack. Cryptography addresses integrity by performing a digital signature check across information[5].

3. “*Availability* relates to preventing, detecting, or deterring the denial of access to critical information”. Cryptography can prevent confidentiality and integrity attacks, but it can not prevent availability attacks. Cryptography, like any other network security technology, is not a silver bullet. Therefore, it must be combined with other techniques to achieve a robust security solution.

4. *Authentication*: “In most transactions you need to be able to authenticate or validate that the people you’re dealing with are who they say they are”.

5. “*Non-repudiation* deals with the ability to prove in a court of law that someone sent something or signed something digitally”. Without non-repudiation, digital signatures and contracts would be useless.

The research motivations section has highlighted that the steganographic capacity and stego image imperceptibility are the most important aspects of image steganographic systems. Essentially, either increasing the steganographic capacity while maintaining the imperceptibility (stego image quality) or enhancing the imperceptibility while maintaining the steganographic capacity represents a contribution. This is exactly our research main aim, increasing the steganographic capacity and/or enhancing the stego image quality.

Traditional steganography uses digital files as cover of secret data. However, this carries the threat of detecting the stego file as these files are usually saved. Thus, available stego files may increase the opportunity of steganalysts to detect these stego images by applying various steganalysis techniques. Alternatively, communication protocols messages such as the ones of the Simple Object Access Protocol (SOAP) leave almost no trail as they are normally deleted after they have been received and the actual data de-serialized. Unlike the steganography methods used with conventional covers such as digital images, there are very few steganography methods that can feasibly be used with communication protocols such as SOAP[6]. Thus, our research also aims to find out an undetectable steganography method based on SOAP messages.

2. Cover Files Used For Steganography

Basically, cover files represent the container of hidden data or secret messages. Additionally, some parts or characteristics of cover files will be modified, changed, or manipulated in order to hide these secret messages. However, these manipulations, which occur during the hiding procedure, should remain imperceptible to anyone not involved in the communication process. Therefore, the appearance or format of cover files must remain intact after hiding the secret data. As a result, it is not possible to use all types of files or data as cover files of steganography since every cover file must have a sufficient redundant area to be replaced by the secret message.

There is a variety of files that can be used as cover files of steganography such as executable files (i.e. exe files), HTML files, XML files and TCP headers. Essentially, many kinds of digital media such as image, audio, text, and video files can be used as cover files of steganography. However, the ability of such files to embed secret data depends on the availability of redundant or insignificant areas within these files. Thus, the cover files represent the container of hidden data and their size may determine the secret data size that can be embedded. To this end, cover files are the fundamental component of steganographic systems. However, the relationship between cover files and the other main components of steganographic systems will be discussed in the next section.

3. Possible Attacks

Steganography attackers are the interceptors of stego files in the communication channels in order to detect hidden messages in these stego files. In the *"Prisoners' Problem"*, Simmons (1983) links these attackers to wardens mediating the communication between two prisoners (the communicating parties, Alice and Bob). Three general types of steganography attacks can be distinguished and therefore three scenarios of digital steganography can be recognized in order to meet attacks. The first technique deals only with protecting the steganographic system against message detection in a passive attack, while the second protects the message against detection and modification by an active attack. However, the third technique protects the steganographic system against the forgery of a malicious attack. The next three subsections explain these three attacks in detail.

a. Passive Attack

Passive wardens just observe the communication without any interference. Therefore, if the warden is restricted from modifying the contents of stego files during the communication process, it is called a passive warden. The passive warden only has the right to prevent or permit the message delivery. Therefore, the communication between two parties will be blocked if the warden suspects that a secret communication is taking place. Otherwise the communication will be relayed Currently, most steganography techniques consider the passive warden scenario in which the warden does not interfere with the stego file in any way. Therefore, most steganography research is concerned with such kind of scenarios

b. Active Attack

If the warden can intentionally modify the contents of stego files during the communication process, we are dealing with an active warden. An active attack is thus the process of altering stego files and introducing distortion during the communication process in order to prevent secret communication. In such kind of attacks, the attacker can capture and modify a stego file sent from Alice to Bob and then forward this modified file to Bob. Even though there is no suspicion that secret communication is taking place, the warden may modify the stego file or add random noise to the transmitted stego file in order to destroy any secret message that might be present[7,8].

c. Malicious Attack

If the warden fakes messages or acts as one of the communication partners during the communication process, it is called a malicious warden. In the malicious attack, the warden may intentionally try to remove the hidden message, impersonate one of the communicating parties, or trick them. Therefore, in this kind of attack, the warden can pass his own message to a specific communication partner as if it is sent by the other communication partner. However, this attack is the most difficult and rare among all these three main attacks since the attacker here needs to know the stego key shared between the communicating parties. Additionally, he/she may have to know the personal encryption key of the sender person. Such kind of attacks are considered infrequently in both steganography and watermarking applications since it is difficult to apply and easy to be detected by the actual receiver.

4. Classification of Methods used in Steganography

There are two general approaches to classify steganographic systems. The first approach is based on the type of cover file while the second approach is based on the hiding method or the layout of modification used in the embedding process. These two general classification approaches of steganography are explained in the next subsections.

a. Cover-Type Based Classification

Since many kinds of digital media can be used as cover files of steganography, the first approach of classification breaks down steganography according to the type of the cover file used.

However, the properties of these cover files vary from one type to another and these properties control how the secret data can be hidden inthese cover files. To this end, knowing the type of cover file can give us an indication or idea where the secret data might be hidden (Cole, 2003).
Mostly, steganographic systems are classified according to the cover file used. Accordingly, different steganography types can be distinguished such as: image, audio, video, text, and HTML steganography. For example, the steganographic system that uses digital images as cover files is an image-based steganographic system.

Hiding Method-Based Classification

Regardless of the cover type used for data hiding, steganography can be classified according to the method used to hide secret data. Furthermore, this approach of steganography classification is the most preferred approach in the steganography research community. Accordingly, there are three ways to hide secret data in cover files: insertion-based, substitution-based, and generation-based method

b. Insertion-Based Method

This method depends on finding some areas in cover files which are usually ignored by applications that read this cover file and then embedding the secret data in these areas. Since this method inserts the secret data inside the cover file, the size of the stego file would be larger than the size of the cover file. As a result, the main advantage of this method is that the contents of the cover file would not be changed after the embedding process since this method relies on accumulating or adding the secret data to the cover file.

c. Substitution-Based Method

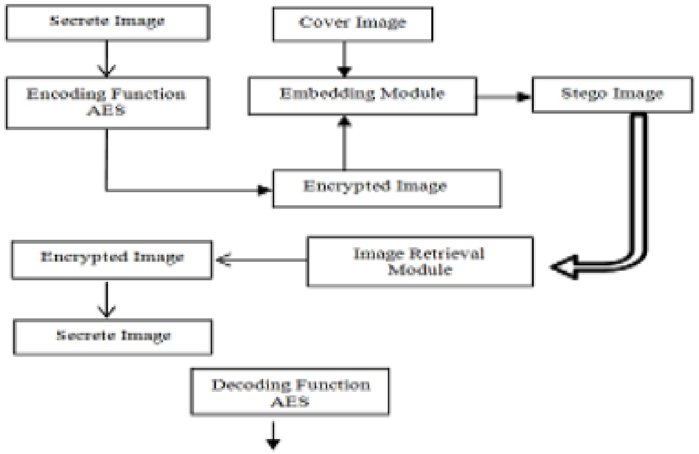
Unlike the insertion-based method, this method does not add the secret data to the cover file data. However, substitution-based method depends on finding some insignificant regions or information in cover files and replacing this information with the secret data. Therefore, the sizes of both the stego file and the cover file are similar since some of the cover data is just modified or replaced without any additional data. However, the quality of the cover file can be degraded after the embedding process. Additionally, the limited amount of insignificant information in cover files restricts the size of secret data that can be hidden

d. Generation-Based Method

Unlike both methods explained above, this method does not need a cover file since it uses secret data to generate appropriate stego files. One of the steganography detection techniques depends on comparing cover files with their stego files. Therefore, one advantage of the generation-based steganography is preventing such kind of detection since only stego files are available and there is no cover files used. The major limitation of this method is the limited stego files which can be generated. Moreover, the generated stego files might be unrealistic files for end users (e.g. an image contains different shapes and colours without any sense or a text without any meaning). Therefore, the main media for such techniques are random-looking images and English text files.

5. PROPOSED IMAGE STEGANOGRAPHY MODEL

Proposed is based on AES and Steganography



Encoding Algorithm

- Input image AES which produces the encrypted secrete image.
- Embed encrypted image into Cover Image using Steganography encoding module which produces Stego Image.

Decoding Algorithm

- Setgo Image is given to Stegography decoding algorithm to retrieve an image.
- Decrypt the image
- Produces secret image

7. Conclusion

This paper analyses and discuss the relationship between cryptography and steganography. Presents an overview of digital stegangraphy basics and describes different kinds of attacks. It is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of stego images. This study aims to increase the steganographic capacity and enhance the quality of stego images. The proposed method describes the need of crypto steganography and the weaknesses of the previous protocols and then propose an improved protocol that eliminates the vulnerabilities of the previous protocols and compares the previous protocols with the proposed protocol.

.

Acknowledgement

We thank Department of Science & Technology DST, New Delhi in funding the project under WOS-A scheme and this publication is under DST fund.

References:

[1]X. Y. Wang. The Collision attack on SHA-0. In Chinese, to appear on www.infosec.edu.cn, 1997.

[2] B. den Boer and A. Bosselaers, Collisions for the Compression Function of MD5. EUROCRYPT 1993, pp293–304.

[3] X. Y. Wang, X. J. Lai, D. G. Feng, H. Chen, X. Y. Yu. Cryptanalysis for Hash Functions MD4 and RIPEMD. Advances in Cryptology–Eurocrypt'05, pp.1-18, Springer-Verlag, May 2005.

[4] I. Damgård, A Design Principle for Hash Functions. In Advances in Cryptology - CRYPTO '89 Proceedings, Lecture Notes in Computer Science Vol. 435, G. Brassard, ed, Springer-Verlag, 1989, pp. 416-427.

[5] S. M. Bellovin and E. K. Rescorla, Deploying a New Hash Algorithm, NIST Hash Function Workshop, October 2005.

[6]B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010

[7] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, Vol. 24, 1981, pp. 770-772.

[8] A. Shimizu, "A dynamic password authentication method by one-way function,"IEICE Transactions on Information and Systems, Vol. E73-DI, 1990, pp. 630-636.

[9]. A. Shimizu, T. Horioka, and H. Inagaki, "A password authentication method for contents communication on the internet," IEICE Transactions on Communications, Vol.E81-B, 1998, pp. 1666-1673.

[10] M. Sandirigama, A. Shimizu, and M. Noda, "Simple and secure password authentication protocol (SAS)," IEICE Transactions on Communications, Vol. E83-B, 2000,pp. 1363-1365.

B. Madhuravani, Department of CSE, MLR Institute of Technology, Dundigal, Hyderabad. She is doing Ph. D in Computer Science & Engineering, JNTUH. Her research interests include Information Security, Computer Networks, Distributed Systems and Data Structures.

Dr. P. Bhaskara Reddy, B.E.(ECE), M.Tech., Ph.D., F.I.S.E.E., MCSI, MISTE, the Director MLR Institute of Technology is a young and dynamic professor of ECE, has 26 years of Teaching, Research and Administrative experience in Reputed Engineering Colleges and Industry. Recipient of Bharath Jyothi award in 2003 and Rastraprathiba award in 2004, Knowledge Award from Alumni of SVHCE for the year 2001, Published 1 Book (International Edition) “Information Technology in Technical Education – Economic Development by “LAMBERT Academic Publishing”, Published 9 Laboratory Manuals, 74 Research papers at National and International Level on Education, Electronics Communication, I.T, Computer Networks, E-Commerce etc. Guided 5 Research Scholars for their Doctorates, about 50 M.Tech., M.C.A. and B.Tech projects and Conducted 10 National Level Technical Symposiums on various topics in Electronics & Communications, Computers etc.

P.LalithSamanthReddy, currently pursuing his MS in Computer Science & Engineering, Illinois Institute of Technology, USA. He published around 6 Research papers in National and International journals. His current research interests include Network Security and Information Security, Computer Networks.