Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 10 (15): 1650-1655, 2010
ISSN 1812-5654

On the Differences between Hiding Information and Cryptography Techniques: An Overview

[1]B.B. Zaidan, [1]A.A. Zaidan, [2]A.K. Al-Frajat and [2]H.A. Jalab
[1]Faculty of Engineering, Multimedia University, Jalan Multimedia, 63100 Cyberjaya, Malaysia
[2]Faculty of Computer Science and Information Technology, University Malaya,
50603 Kuala Lumpur, Malaysia

Abstract: The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. Nowadays, protection system can be classified into more specific as hiding information (Steganography) or encryption information (Cryptography) or a combination between them. In this study, we have review the strength of the combine the steganography and cryptography techniques, since there is non-existence of standard algorithms to be used in (hiding and encryption) secret messages. As a result of this study, the two techniques have been presented and the combination between these techniques has been discussed.

Key words: Data hidden, steganography, hiding information, cryptography, information security

INTRODUCTION

It is within highly integrated technology environments and the widely usage of the internet and files sharing. New challenge has been found the information security and privacy has becoming a main point for designing, developing and deploying software applications. Ensuring a high level of trust in the security and quality of these applications is crucial to their ultimate success. Information security has therefore become a core requirement for software applications, driven by the need to protect critical assets and the need to build and preserve widely trust in computing (Anderson, 2001). However, secure software engineering is a big challenge (Allen *et al*., 2008). This is mainly due to the increasing complexity, openness and extensibility of modern applications, in addition the new techniques to attack the secure systems which make a complete analysis of security requirements very hard.

Specific requirements, whether self-imposed or proposed by an external organization or customer, are all designed to address the three fundamental objectives of computer security: confidentiality, integrity and authentication as shown in Fig. 1.

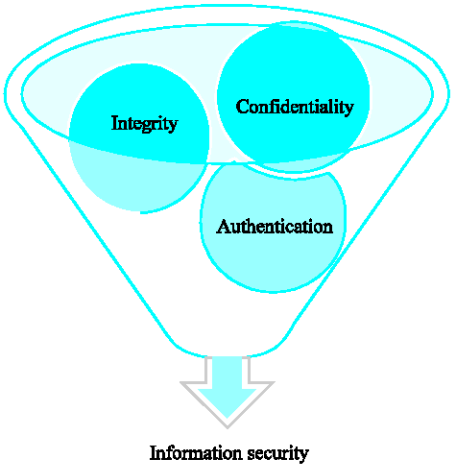

Fig. 1: Information security attributes

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and secure information. It is concern on the term of preventing unauthorized person or system from disclose the privet or secret information to ensure the privacy or security issues.

Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. Integrity is broken when another party accidentally or with malicious intent deletes or altering an important data.

Corresponding Author: B.B. Zaidan, Faculty of Engineering, Multimedia University, Jalan Multimedia, 63100 Cyberjaya, Malaysia

Authentication: Assure that the source of the message is an authorised party, or to detect any unauthorised access to or use of information.

An important aspect of information security is recognising the value of information and the expected attacks for these information from unauthorised parties then defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification where the top secret data need highly secure software and procedures to deal with this data and assign different level of authorised parties such as some parties authorised to disclose the data only while another have the ability to change it.

The general taxonomy for the security attribute depends on the context in which the attribute is addressed. Historically, there have been three main areas which have addressed security: government and military applications; banking and finance and academic and scientific applications. In each of these cases, different aspects of security were stressed and the definition of individual security attributes depended upon the stressed security aspects. Where the use of the information security in government and military applications; the disclosure of information is the primary risk and to be averted at all costs. While in banking, finance and business-related computing, the security emphasis is on the protection of assets. Where the disclosure is an important risk, the far greater risk is the unauthorized modification of information; as well as the academic and scientific computing application, the main security emphasis is on protection from unauthorized use of resources.

In order to achieve the information security goal there are number of methods which are used for information security. The cryptography is one of the methods which are used to keep the information or the data in safe against any disclose to the data.

CRYPTOGRAPHY

There are some systems designed to protect the data or information which uses the cryptography technique as a primitive. Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted (Kessler, 1998; Abomhara *et al*., 2010a). Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of data encryption is data Decryption.

In modern days cryptography is no longer limited to secure sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources and electronic financial transactions. Since, cryptography first known usage in ancient Egypt it has passed through different stages and was affected by any major event that affected the way people handled information. In the World War II for instance cryptography played an important role and was a key element that gave the allied forces the upper hand and enables them to win the war sooner, when they were able to dissolve the Enigma cipher machine which the Germans used to encrypt their military secret communications (Abomhara *et al*., 2010b).

Original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer.

Whereas the disguised data so-called cipher-text, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem (Abomhara *et al*., 2010a, b). Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data (Kessler, 1998). In the 19th century, a famous theory about the security principle of any encryption system has been proposed by Kerchhoff. This theory has become the most important principle in designing a cryptosystem for researchers and engineers.

Kirchhoff observed that the encryption algorithms are supposed to be known to the opponents (White, 2003). Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. For even though in the very beginning the opponent doesn't know the algorithm, the encryption system will not be able to protect the cipher-text once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space (Abomhara *et al*., 2010a). The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space and thus the higher the security level is. The decrypt for these data or information is done only if the correct key is at hand.

One of the most common primitives in computer security is a cryptosystem, which specifies exactly how to encrypt data with a key to produce cipher-text. Cipher-text can be thought of as data locked inside a box; the encryption makes it intractable to recover the original data from the box without the correct key. There are some standards methods which is used with cryptography such as secret key (symmetric), public key (asymmetric), digital signature and hash function.

Secret key (Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher-text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

Public key (Asymmetric): Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their study described a two-key crypto system in which two parties could engage in a secure communication over a insecure communications channel without having to share a secret key (Zaidan and Zaidan, 2009).

Digital signature: The using for digital signature came from the need of ensuring the authentication (is the data came from the original sender? Or someone has modified it?). The digital signature is more like stamp or signature of the sender (should be unique for each sender) which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature assures that any change made to the data that has been signed is easy to detect by the receiver.

Hash function: The hash function is a one way encryption, the hash function is a well defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signatures and cheap constructions are highly desirable (Bellare and Rogaway, 1997). The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols (Bellare *et al*., 1996).

The authentication and the integrity considered as main issues in information security (Alghathbar, 2010), the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it's similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

HIDE INFORMATION

The word steganography comes from the Greek Steganos, which mean covered or secret and graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening (Al-Azawi and Fadhil, 2010). Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

For example ancient Greece used methods for hiding messages such as hiding in the field of steganography, some terminology has developed. The adjectives cover, embedded and stego were defined at the information hiding workshop held in Cambridge, England (Naji *et al*., 2009a). The term cover refers to description of the original, innocent massage, data, audio, video and so on. Steganography is not a new science; it dates back to ancient times. Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger head. After allowing his hair to grow, the message would be undetected until the head was shaved again. While the Egyptian used illustrations to conceal message. Hidden information in the cover data is known as the embedded data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content (Naji *et al*., 2009b). The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret (Jalab *et al*., 2009; Shirali-Shahreza and Shirali-Shahreza, 2008).

Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. (Ahmed *et al*., 2010). This

technique has recently become important in a number of application areas. For example, digital video, audio and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed.

The term of hide information is the process of covering the secrete message or information multimedia files to make sure there is no other party can disclose or altering it (Karzenbeisser and Perircolas, 2000; Majeed *et al*., 2009). Under this topic we can drive two techniques which are used to hide information one is digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove, the signal may be audio, pictures, video or text files; its mostly used for demonstrate the intellectual property rights purpose such as adding copy right logo or text (author signature) for multimedia files. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Since, the main use for steganography is to send secure messages between parties, then it's aim to prevent the message being detected by any other party (Kawaguchi and Eason, 1998).

The digital multimedia files steganography uses code fields for unimportant bits as places to hide encoded messages or images. While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. During the process characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Capacity, confidentiality and robustness, are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Confidentiality relates to the ability of the discloser to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

The most significant weaknesses and disadvantages of steganography are as follows:

- The process of hidden data by using Least Significant Bit (LSB), which is a common method, used the image as a cover for data to be hidden, but it's mostly subjected to against from attackers. Once attackers suspect there is steganography implemented in the data, they will reproduce LBS and examine it to check whether it has a meaning or not (Johnson *et al*., 2001)
- The results of Steganography might be compressed by Lossy Compression to reduce the size of the file especially at transferring the data, which leads to destroy the hidden data in that file after the reopening (Karzenbeisser and Perircolas, 2000)
- In the case of using a cover environment with equal value spaces as in the pictures with constant value colour spaces (weak texture) or sounds with constant intensity sound intervals, that may lead to discovery or differentiation at these sectors
- One of the methods of breaking concealment in image and sound is changing the format of the file
- It requires other methods to hide the data
- The size of the output of the hidden data file is larger comparing to the encoded data. In its most efficient possible case, it may reach double the size of encoded data or a bet less (Karzenbeisser and Perircolas, 2000). In some situations output file may reach eight times larger than the encoded data, as well as certain files of media images and text, files may reach fifty times larger when they are encoded
- It is not possible to combine the (maximize/ maximum) strength of Robustness with maximize/maximum amount of hidden data comparing to data cover (Othman *et al*., 2009)

CRYPTOGRAPHY VS. STEGANOGRAPHY

Since, the advent of computers there has been a vast dissemination of information, some of which needs to be kept private, some of which doesn't. The information may be hidden in two basic ways (cryptography and steganography).The methods of cryptography does not conceal the presence of secret information but render it unintelligible to outsider by various transformations of the information that is to be put into secret form, while methods of Steganography conceal the very existence of the secret information. The following table has shown the comparison between cryptography and steganography. Table 1 shows that the cryptography and the hiding information technologies have counter advantages and disadvantages.

Table 1: Comparison between cryptography and steganography

Cryptography	Stenography
The encrypted letter could be seen by anyone but cryptography make the message not understandable	Stenography is hiding the message in another median so that nobody will notice the message
The end result in cryptography is the cipher text	The end result of information hiding is the stego-media
The goal of a secure cryptographic is to prevent an interceptor from gaining any information about the plaintext from the intercepted cipher text	The goal of secure stenographic methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data
Any person has the ability of detecting and modifying the encrypted message	The hidden message is imperceptible to anyone
Stenography can not be used to adapt the robustness of cryptographic system	Stenography can be used inconjunction with cryptography by hiding an encrypted message

DISCUSSION

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different (Stallings, 1999). In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message.

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something.

In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-image so it cannot be seen. A message in cipher-text, for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system (Petitcolas *et al*., 1999). Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message (Zaidan and Zaidan, 2009). Since then, the steganography approaches can be divided into three types:

- Pure steganography
- Secret key steganography
- Public key steganography

Pure steganography: This technique simply uses the steganography approach only without combination with other methods. It is working on hiding information within cover carrier.

Secret key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and the hide the encrypted data within cover carrier.

Public key steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier. Further direction can be done by using small size of encrypted data to hide it within multimedia cover.

ACKNOWLEDGMENTS

This research has been funded by the University of Malaya, under the Grant No. (P0033/2010A). The author would like to take this opportunity to thank and acknowledge his supervisors: Dr. Hamid Jalab and Dr. Zarinah Mohd Kasirun, for having rendered their ceaseless and unconditional support throughout the entire duration of the study. The author would also like to extend his heartfelt gratitude to all his friends and associates who had offered him the much needed assistance and encouragement from the start to the end of the research period.

REFERENCES

Abomhara, M., O. Zakaria and O.O. Khalifa, 2010a. An overview of video encryption techniques. Int. J. Comput. Theory Eng., 2: 103-110.

Abomhara, M., O. Zakaria, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2010b. Enhancing selective encryption for H.264/AVC using advance encryption standard. Int. J. Comput. Electr. Eng., 2: 223-229.

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Alghathbar, K., 2010. Code based hashing technique for message authentication algorithms. J. Inform. Assurance Security, 5: 9-20.

Allen, J., S. Barnum, R. Ellison, G. Mcgraw and N. Mead, 2008. Software Security Engineering: A Guide For Project Managers. 1st Edn., Addison-Wesley Professional, USA., ISBN-13: 978-0321509178, pp: 368.

Anderson, R.J., 2001. Security Engineering: A Guide to building Dependable Distributed Systems. 1st Edn., John Willey, UK., ISBN-10: 0471389226, pp: 640.

Bellare, M. and P. Rogaway, 1997. Collision-resistant hashing: Towards making uowhfs practical. Lecture Notes Comput. Sci., 1294: 470-484.

Bellare, M., R. Canetti and H. Krawczyk, 1996. Keying hash functions for message authentication. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, Aug. 18-22, Springer-Verlag, Berlin, Germany, pp: 1-15.

Jalab, H., A. Zaidan and B.B. Zaidan, 2009. Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J. Comput., 1: 108-113.

Johnson, N.F., Z. Duric, S. Jajodia and N. Memon, 2001. Information hiding: Steganography and watermarking-attacks and countermeasures. J. Electron. Imag., 10: 825-825.

Karzenbeisser, S. and F. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 1580530354, pp: 240.

Kawaguchi, E. and R.O. Eason, 1998. Principle and applications of BPCS-steganography. Proc. SPIE, 3528: 464-473.

Kessler, G.C., 1998. An overview of cryptography. http://www.garykessler.net/library/crypto.html#intro.

Majeed, A., M.L.M. Kiah, H.T. Madhloom, B.B. Zaidan and A.A. Zaidan, 2009. Novel approach for high secure and high rate data hidden in the image using image texture analysis. Int. J. Eng. Technol., 1: 63-69.

Naji, A.W., S.A. Hameed, M.R. Islam, B.B. Zaidan, T.S. Gunawan and A.A. Zaidan, 2009a. Stego-analysis chain, session two novel approach of stego-analysis system for image file. Proceedings of the International Conference on IACSIT Spring Conference, April 17-20, Singapore, pp: 398-401.

Naji, A.W., A.A. Zaidan, B.B. Zaidan, A. Shihab and O.O. Khalifa, 2009b. Novel approach of hidden data in the (unused area 2 within exe file) using computation between cryptography and steganography. Int. J. Comput. Sci. Network Security, 9: 294-300.

Othman, F., L. Maktom, A.Y. Taqa, B.B. Zaidan and A.A. Zaidan, 2009. An extensive empirical study for the impact of increasing data hidden on the images texture. Proceedings of the International Conference on Future Computer and Communication, April 3-5, IEEE Computer Society, Kuala Lumpur, Malysia, pp: 477-481.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Stallings, W., 1999. Cryptography and Network Security: Principles and Practice. 2nd Edn., Prentice Hall, Upper Saddle River, New Jersey.

White, B.G., 2003. Cisco Security+ Certification: Exam Guide. McGraw-Hill, New York.

Zaidan, A. and B. Zaidan, 2009. Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int. J. Comput. Network Security, 1: 1985-1993.