Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Security in E-Governance through Steganography

Hardikkumar V. Desai
Assistant Professor,
Department of Computer Science,
Naran Lala College of Professional and Applied Sciences,
Navsari, India.

Apurva A. Desai
Professor & Head,
Department of Computer Science,
Veer Narmad South Gujarat University,
Surat, India.

ABSTRACT: Government essentially refers to provide efficient, convenient and transparent services to citizens and business through information and communication technology. Governance is an alternative structure to the traditional view of government. One of the essential tasks of e-governance is the transmission of confidential information from traditional to digital on the computer networks. Although each e-government has its own networks and government can't deny using Internet. However, to protect information is prime concern for e-government and secure them with the internet attacks because Internet is creating a borderless world. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security is a set combining organizational security and IT security. This paper focuses on how to secure information using steganography .As steganography is a reliable data hiding technique , by using it is very useful not just to hide data but also helpful in identity access management .The technique is developed to hide the confidential data with the particular image. It is helpful in security of information, precision and transparency among citizens. The paper also focuses on the loopholes of other data hiding technique called cryptography. As information security is a prime concern in online world, it attracts the interest of researchers to develop new techniques and continuous evaluation of it.

Keywords: - e-government, e-governance, information security, cryptography, cryptanalysis, steganography, steganalysis, security threats.

I. INTRODUCTION

A. Information Security: Information security means protecting information from unauthorized access. As stated in (UNITED NATIONS, 2012). A central challenge of e-Government service is how the new technology can be used not only to increase efficiency for public administration, but also to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens. Three major aspects of information security are confidentiality, integrity and availability. Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. While, as per (Boritz, 2011), integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle and availability is defined as availability of information whenever required. Security of information against unauthorized access is very immense challenge for e-government .Information security is not only restricted to security of data but also to assure that data is safe against nature and different type of attacks.

B. Security Threats: Threats to computers and information systems are harmful. Security threats are as follows:-

1. Natural Threats
These can best be thought of as threats caused by nature like floods, earth quakes, temperature etc. This type of threats is unacceptable threats and it is not easy to measure natural disaster.

2. Intentional Threats
Cyber crimes are the best examples of intentional threats, or when someone purposely damages property or information. These types of threats are big challenge for e-governance as they harm the system very badly. This is most impactable threat.

3. Unintentional Threats
These threats basically include the unauthorized or accidental modification of software. It include accidentally deleted an important file or hardware failure or any technical issue. These threats are a serious matter and continue logging of system is required.

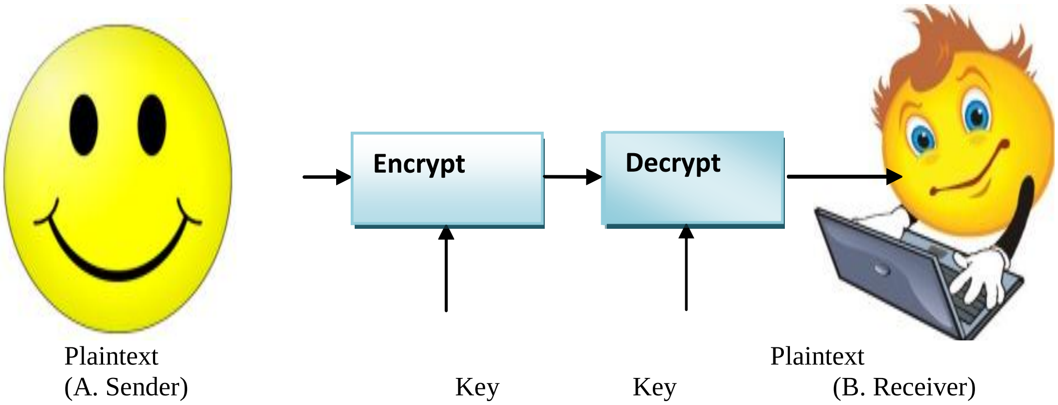
C. Security Techniques: There are many techniques use to hide or to secure data are cryptography and steganography.

The important threat is intentional threats because it’s a most impact able threat.

1. Cryptography

Cryptography means sender converts plaintext to cipher text by using Encryption key and other side receiver decrypt cipher text to plain text by using Decryption Key. The idea is to change the text in to format which is not easy to decrypt without decryption key .changing the alphabets with other alphabets or make a key to arrange the alphabets.

In following figure(3(a)) ,A is a sender who convert plaintext to cipher text by using encryption key at the other end B (Receiver) get the cipher text and by using decryption key convert to actual message(plaintext)



(a)

[Fig 1(a): Cryptography]

2. Steganography and Steganalysis

Steganography is the art of hiding information within other information in such a way that it is hard or even impossible to tell that something is there. There are many different carriers for steganography but the most popular is digital images. The analysis to find the hidden data using steganography is called steganalysis; there are various types of attacks mainly structural, visual and statistical attacks. Whereas Steganalysis is the art of identifying stegogrammes that contain a secret message. Steganalysis does not however consider the successful extraction of the message; typically, steganalysis begins by identifying any object made by human beings are exist in the suspect file as a result of embedding a message. None of the steganographic systems that are known today achieve perfect security (Cox et al., 2007), and this means that they all leave hints of embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not.Steganalysis is very important to information security, as growing interest emerges as to whether terrorist organizations use steganographic techniques to communicate with each other. In fact steganalysis is taken so seriously that it is believed that US Government agencies, including the NSA and the Pentagon are funding research for its development. If a file is considered to contain a secret message then it is possible that the entire work will be modified by the steganalyst such that the integrity of the message is removed. Blind steganalysis on the other hand is a much harder task, and means that the steganalyst has no reason to believe that secret communications is taking place. In this case, a set of algorithms are typically developed in order to check for signs of tampering. If some signs of tampering are flagged by the algorithms, then it is likely that the suspect file contains steganography.

D. Attacks on Steganographic Techniques

1. Visual Attacks: Visual Attacks are widely regarded as the simplest form of steganalysis. As the name suggests, a visual attack largely involves examining the subject file with the naked eye
to identify the difference.

2. Structural Attacks: Structural attacks are designed to take advantage of the high-level properties of the structure of the carrier.

3. Statistical attack: In mathematics, the study of statistics makes it possible to determine whether some
Phenomenon occurs at random within a data set.

E. Steganography vs. Cryptography: In steganography message is hidden within other carrier (cover image), so no chance of naked eye detection though in cryptography message is converted through the encryption key and generated message is easy to identify that something is coded.

The capacity to embed message within cover image is differs as different technologies are used usually low hiding capacity with the use of steganography .Whereas, in cryptography encrypt capacity is much high, but as message is long it chances to be decrypt by hacker by the use of english language common phrase.

Detection of data in steganography is little bit hard as data is embedded though in cryptography detection of data depends on the technique used.

Strength of steganography technique is that it conceals the data whereas in cryptography message is hidden by altering the message by assigning key.

II. LITERATURE REVIEW

There is a prevailing myth that secrecy is good for security, and since cryptography is based on secrets, it may not be good for security in a practical sense (Schneier, 2004; Baker, 2005). The mathematics involved in good cryptography is very complex and often difficult to understand, but many software applications tend to hide the details from the user thus making cryptography a useful tool in providing network and data security (Robinson, 2008)

(Kerckhos,1883),enunciated the first principles of cryptographic engineering, in which he advises that we assume the method used to encipher data is known to the opponent, so security must lie only in the choice of key .

(Fitzmann 1996),today most of communication occurs electronically .There have been advancements utilizing digital multimedia signals as vehicles for steganographic communication These signals, which are typically audio, video or still imagery are cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as cover escrow.

(Swanson et al., 1996) utilizes an approach of perceptual masking to exploit characteristics of the human visual system (HVS) for data hiding.

(Schotti, 2008), in his book of Steganography, entitled schola steganographica, published in 1665. schotti drew extensively upon the work of Johannes Trithemius (1462-1562), a German Monk and early researcher in steganography and cryptography, steganographic research continued to develop in the fifteenth and sixteenth centuries .Bishop John Wilkins – later the master of Trinitity college, Cambridge – devised a number of steganographic processes that ranged from coding messages in sheet music and string knots to invisible inks.

III. IMPORTANCE OF PROPOSED RESEARCH WORK

The importance of the research work is to develop a technique to hide the data inside the digital image which can be difficult to detect and only receiver can detect it. Because advance security is not maintained by the password protection but it is gained by hiding the existence of the data which can only be done by steganography.

IV. DESIGN AND RESEARCH METHODOLOGY

Steganographic tool is developed by keeping in mind the demand for secure transaction over the internet.

The model is developed as information (data) is hiding within particular one image, so not easy to detect the correct data as well as it also helps for identity access management. Because we observe that there are so many mistakes with voter ID card and other government documents. Identity access management is a prime issue with e-government website because password is not that much efficient.

Figure 1 (a), is an example of Digital Image Steganography, Image (*b*) is to be embed within image (*a)* and create stegogramme (*c*), which is same as original image (a). So that it is not easy to detect that image is hided and receiver at the other end can transmit original image (message).

NAME : ABC
ADDRESS : C-FLOOR
APPARTMENT
PINCODE:123456
EMAIL : A@XYZ.COM

(a) (b) (c)

[*Fig .2 :(a) Cover/Carrier Image (b): Image to be Hide (c): Cover /Carrier Image (with Stegogramme*)]

V. CONCLUSION

We observed that image containing stegogramme is same look alike original image. Steganographic tool is developed as it is very popular technique for data hiding in today's world, it's a good practice to hide particulars information it helps in identity access management as well as security of information is achieved by it. This technique is also useful for verification of data as well by using it we can reduce the risk and secure information and achieved accuracy.

References

[1] United Nations, Department of Economic and Social Affairs (2012). "*E-Government Survey 2012*. *E-Government for the People"*. ISBN: 978-92-1- 123190-8.

[2] J. Boritz, Efrim (2011). "IS Practitioners' Views on Core Concepts of Information Integrity". *International Journal of Accounting Information Systems*. Elsevier.

[3] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker (2007). "Digital Watermarking and Steganography (Second Edition)", Morgan Kaufmann Publishers.

[4] B. Schneier (2004). The Nonsecurity of Secrecy. Communications of the ACM,47(10), 120-120. Retrieved August 2, 2008, from Academic Search Premier database.

[5] M.Baker,(2005). Keeping a Secret. Technology Review, 108(1), 82-83. Retrieved August 12, 2014, from Academic Search Premier database.

[6] S.Robinson (2008). Safe and secure: data encryption for embedded s ystems. (Coverstory). EDN Europe, 53(6), 24-33. Retrieved August 2, 2008, from Academic SearchPremier database.

[7] A. Kerckhos (1883). La Cryptographie Militaire."Journal des Sciences Militaries, vol. 9, pp. 538.

[8] B. P Fitzmann (1996). "Trials of traced traitors." Information hiding, first international work shop, Lecture notes in computer science R. Anderson, Ed. Berlin, Germany: Springer Verlag 1996, vol. 1, pp= 49-64.

[9] M. D. Swanson, B-zhu and A. H. Tewfik, (1996). "Robust Data Hiding for Images" in proc. IEEE Digital signal processing workshop, Loen, Norway,pp-37-40.

[10] P. Gasparis Schotti e Societate Jesu Schola steganographica Working Paper in International Studies Centre for International Studies Dublin City University Working Paper 6 of 2008.