IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 76-81
www.iosrjournals.org

Pros and Cons of Cryptography, Steganography and Perturbation techniques

Haripriya Rout[1], Brojo Kishore Mishra[2]
[1, 2](Departmen of Information Technologyt, C. V. Raman College of Engineering, India)

ABSTRACT : *Cryptology was as significant as weapons during the World War II and the Cold War. There were lots of studies to develop robust crypto-systems and to use them in communications. These studies have continued up to now. Today some of those crypto-systems called as "classical crypto-systems" are improved and still being used. Mostly we can secure our data in three ways first one is cryptography where content of the message is kept secret by encoding it, secondly Steganography where the message is embedded in another medium, third perturbation technique which performs some operation on actual data so that its actual meaning is not obvious/disclosed.Here we have a comparative study on cryptography, steganography and perturbation technique with pros and cons of each.*

Keywords *- Cryptography, Data Security, Encryption, Perturbation, Steganography.*

I. INTRODUCTION

Data security is critical for most businesses and even home computer users. Client information, payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Data lost due to disasters such as a flood or fire is crushing, but losing it to hackers or a malware infection can have much greater consequences.

1.1. Risk Assessment

Thorough data security begins with an overall strategy and risk assessment. This will enable you to identify the risks you are faced with and what could happen if valuable data is lost through theft, malware infection or a system crash. Other potential threats you want to identify include the following:

- Physical threats such as a fire, power outage, theft or malicious damage
- Human error such as the mistaken processing of information, unintended disposal of data or input errors
- Exploits from corporate espionage and other malicious activity

You can then identify areas of vulnerability and develop strategies for securing your data and information systems. Here are several aspects that need to be considered:

- Just who has access to what data
- Who uses the internet, email systems and how they access it
- Who will be allowed access and who will be restricted
- Whether or not to use passwords and how they will be maintained
- What type of firewalls and anti-malware solutions to put in place
- Properly training the staff and enforcing data security.

After the above analysis, you can then prioritize specific data along with your more critical systems and determine those that require additional security measures. It is also a good idea to layout a BCP (Business Continuity Plan) so that your staff is still able to work effectively if the systems happen to fail. Company risks and security implementations should be reviewed frequently to support changes such as the growth of your business and other circumstances.

1.2. Securing Data

Once you draw up a plan and assess your risks, it is time to put your data security system into action. Since data can be compromised in many ways, the best security against misuse or theft involves a combination of technical measures, physical security and a well educated staff. You should implement clearly defined polices into your infrastructure and effectively present them to the staff. Here are things that you may do:

- Protect your office or data center with alarms and monitoring systems
- Keep computers and associated components out of public view
- Enforce restrictions on internet access
- Ensure that your anti-malware solution is up to date
- Ensure that your operating system is up to date
- Fight off hacking attacks with intrusion detection technology
- Utilize a protected power supply and backup energy sources

1.3. Mobile Data Security[13]

Hand-held devices and laptop computers have become popular in the business environment. However, mobile computers are at a much greater risk of data loss through damage and theft. For this reason, different safeguards need to implement in addition to the security measures listed above.

- Regularly backup data on removable media and safely store multiple copies
- Activate password protection whenever the device is left alone
- Never leave the device alone and visible in a vehicle
- Protect the device from physical damage by transporting it in protective casing

Efficient data security involves numerous steps, many of which can be downright time consuming. On the other hand, I am sure you will agree that actually losing this important data could be much worse.

II. CRYPTOGRAPHY

There are three basic types of secure system by which we can protect or secure our data. Those are Cryptography, Steganography and Perturbation technique. Let us discuss one by one with pros and cons of each one.

Cryptography is the science of writing in secret code and is an ancient art[14] .Cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into plaintext.

Although it seems like common sense to use data encryption in business and other entities for security, many organizations are opposed to encrypting data because of some of the obstacles involved with doing so. Like everything else, data encryption has its pros and cons and businesses must look at all of the considerations to make an informed decision about encryption.

1.4. Data Encryption Pros

- Separation: Data encryption allows the data to remain separate from the device security where it is stored. Security is included with the encryption which permits administrators to store and transmit data via unsecured means.
- No Data Breaches: Data encryption circumvents the potential complications that accompany data breaches which provide ensured protection of intellectual property and other similar types of data.
- Encryption Is On The Data: Because the encryption is on the data itself, the data is secure regardless of how it is transmitted. An exception to the rule can be transmission tools such as email because sometimes a typical email account does not provide the necessary security.
- Encryption Equals Confidentiality: A lot of organizations are required to meet specific confidentiality requirements and other associated regulations. Encrypting data means that it can only be read by the recipient who has the key to opening the data.

1.5. Data Encryption Cons

- Encryption Keys: Without a doubt, data encryption is a monumental task for an IT specialist. The more data encryption keys there are the more difficult IT administrative tasks for maintaining all of the keys can be. If you lose the key to the encryption, you have lost the data associated with it.

- Expense: Data encryption can prove to be quite costly because the systems that maintain data encryption must have capacity and upgrades to perform such tasks. Without capable systems, the reduction of systems operations can be significantly compromised.
- Unrealistic Requirements: If an organization does not understand some of the restraints imposed by data encryption technology, it is easy to set unrealistic standards and requirement which could jeopardize data encryption security.
- Compatibility: Data encryption technology can be tricky when you are layering it with existing programs and applications. This can negatively impact routine operations within the system.

III. STEGANOGRAPHY

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 [7] and a communication is happening [8, 17]. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography[12] can be used to carry out hidden exchanges.

The main goal of steganography is to communicate securely in a completely undetectable manner [9] and to avoid drawing suspicion to the transmission of a hidden data [10]. 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 [11].

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996. There has been a rapid growth of interest in steganography for two main reasons [16]:

- The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.
- Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message. Basically, the model for steganography is shown on Figure 1 [1]. Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as stego-key, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [9]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include [10]:

- Least significant bit insertion (LSB)
- Masking and filtering
- Transform techniques

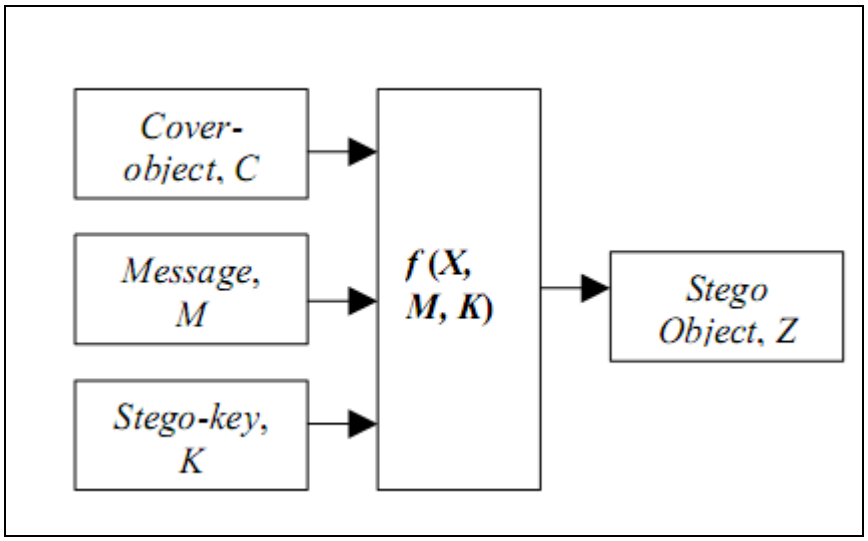

Figure 1: Basic Steganography Model [1]

1.6. Steganography Pros:

- One-Way Hashing :- Used to ensure that a third party has not tampered with a sent message. This is accomplished by creating a hash of the message using a fixed character length for every item in the message, when the original items are in fact of variable character length. The hash is encrypted and sent with the message. When the recipient receives the message it is decoded. If the hash from the decoded message does not match the hash from the encrypted message, both the sender and recipient of the message know that it has been tampered with[5].
- Attaching Text to an Image: - Explanatory notes are attached to an image. In the medical profession this could be used when one medical office sends an image to another medical office. If the sending medical office needs to include explanatory notes of what the receiving medical office should be focusing on, this could be accomplished with steganography [6].
- Hiding Information: - Steganography can also be used to protect identities and valuable data from theft, unauthorized viewing, or potential sabotage by concealing the message within a unsuspicious image.

1.7. Steganography cons:

Unfortunately most uses of steganography and research around the topic of steganography center around the illegitimate purposes. The three biggest areas of illegitimate steganography evolve around terrorism, pornography and data theft. During the research for this website the illegitimate uses of steganography were also found to be on a global scale, involved national security or were done on an academic basis in order to better understand the potential danger of steganography if created by individuals with ill-intentions.

1.8. Steganography vs. Cryptography

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 [6]. 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 contras, 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 ciphertext, 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 [4]. 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 [1]. Table 1 shows that both technologies have counter advantages and disadvantages [19].

Steganography	Cryptography
Unknown message passing	Known message passing
Little known technology	Common technology
Technology still being developed for certain formats	Most algorithms known to government departments
Once detected message is known	Strong algorithm are currently resistant to brute force attack Large expensive computing power required for cracking Technology increase reduces strength

TABLE 1 - Advantages and disadvantages comparison

Unfortunately most uses of steganography and research around the topic of steganography center around the illegitimate purposes. The three biggest areas of illegitimate steganography evolve around terrorism, pornography and data theft. During the research for this website the illegitimate uses of steganography were also found to be on a global scale, involved national security or were done on an academic basis in order to better understand the potential danger of steganography if created by individuals with ill-intentions.

IV. PERTURBATION

Perturbation is a technique by which after perturbation, the resulting data look very different from original data and the distribution of data values is also very different from original data values. It is not possible to accurately estimate the individual data values from record[18].

Data perturbation is a data security technique that adds 'noise' to databases to allow individual record confidentiality. This technique allows users to ascertain key summary information about the data while preventing a security breach. Data perturbation involves adding random noise to confidential, numerical attributes, thereby protecting the original data. Even while altering the original data, these methods allow users the ability to access important aggregate statistics (such as means, correlations and covariances, etc.) from the entire database, thus 'protecting' individual records. For instance, in the case of sales data, an employee may not be able to access what a particular individual purchased from a store on a given day, but that employee could determine the total sales volume for the store on the same day.

Four bias types have been proposed which assess the effectiveness of such a technique. However, these biases deal with simple aggregate concepts (averages, etc.) found in the database. In e-commerce applications, organizations are interested in applying data mining approaches to databases to discover additional knowledge about customers.

This study is interested in a particular form of data privacy/security whereby individual, confidential attribute values are not made available to legitimate users, but aggregate 'relationships' of the database are (hopefully) made accessible. The rationale of these data perturbation techniques is that 'users' do not need to know individual identities of customers (data), only an understanding of aggregate relationships of the customers (data)[15].

- Bias occurs in a data perturbation method when a query generated using perturbed data produces a result significantly different than the same query would using the original data. Four types of biases were identified in (Muralidhar et al., 1999) termed Type A, Type B, Type C, and Type D.

- Type A bias occurs when the perturbation of a given attribute causes summary measures of that individual attribute to change due to a change in variance.
- Type B bias is identified as a bias that occurs when perturbation changes the relationships between confidential attributes.
- Type C bias occurs when perturbation changes the relationship between confidential and non-confidential attributes.
- Type D bias deals with the distribution of the data in a database. When the underlying distribution of a given database is not multivariate normal, and/or the added noise term is not multivariate normal, the form of the resulting perturbed database cannot always be determined.

Databases are ubiquitous and of immense importance to e-commerce applications. The information and knowledge that can be generated from them are absolutely essential; helping organizations to match and customize their products and services to potential customers. Organizations store large amounts of data, and some (most?) may be considered confidential. Thus, security of the data is a concern. This concern applies not just to those who are trying to access the data illegally, but to those who have legitimate access to the data.

1.9. Perturbation Pros:

- Perturbation technique is generally used for privacy preserving in data mining.
- Can be used is genetic study and analysis.
- Low computational expense, even with high dimensional state space

1.10. Perturbation Cons:

- accuracy decreases substantially for state values far from the steady state
- Higher complexity

V. CONCLUSION

Since there are many points both positive and negative to consider, strategic planning for data encryption within an organization is the key. Without detailed planning, data encryption can easily become complex for the IT administrator to manage and complicated for the end users.

REFERENCES

[1]. Muhalim Mohamed Amin et al., "Information hiding using Steganography", 2003.
[2]. C. Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.
[3]. D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-Jun 2001.
[4]. E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, Image Capture Systems Conference, PICS '99, Ed., Apr. 1999, pp. 274--278.
[5]. F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in proceeding of IEEE, pp. 1062-1078, July 1999.
[6]. Webopedia Online. Copyright 2009 WebMediaBrands Inc. Deborah Radcliff. QuickStudy: Steganography: Hidden Data.
[7]. M. Ramkumar & A.N. Akansu. "Some Design Issues For Robust Data hiding Systems", <http://citeseer.nj.nec.com/404009.html>
[8]. N.F. Johnson, S. Jajodia, "Staganalysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 1998.
[9]. N.F. Johnson & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", in Proceeding for the Second Information Hiding Workshop, Portland Oregon, USA, April 1998, pp. 273-289.
[10]. N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34, 1998.
[11]. N. Provos, P. Honeyman, "Detecting Steganography Content on the Internet". CITI Technical Report 01-11, 2001.
[12]. Muhalim Mohamed Amin et al., "Information hiding using Steganography", 2003.
[13]. Peter Tarasewich et al., "WIRELESS/MOBILE E-OMMERCE:TECHNOLOGIES,APPLICATIONS,AND ISSUES".
[14]. T. P.Wasnik et al., "CRYPTOGRAPHY AS AN INSTRUMENT TO NETWORK SECURITY", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.
[15]. Rakesh Agrawal et al., "Privacy-Preserving Data Mining".
[16]. R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Area in Communications, pp. 474-481, May 1998.
[17]. R.Popa,"An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.
[18]. Rick L. Wilson et al., "The Impact of Data Perturbation Techniques on Data Mining", Decision Science Institute Meeting Proceeding 2002.
[19]. S. Tanako, K. Tanaka and T. Sugimura, "Data Hiding via Steganographic Image Transformation", IEICE Trans. Fundamentals, vol. E83-A, pp. 311-319, February, 2000.