The method of file security through Cryptography and Steganography

– **Anukool Bajpai**
Principal, SIMS, GGSIP University, Delhi
anukoolbajpai@gmail.com

Today technology changes so fast and our lives are totally dependent on computer and networks. There is a huge number of files on the network for communication over the network. These files are stored on server and this introduces security threats also. Many Organizations such as Banking, University and Medical store their sensitive data for day-to-day operation of their organization. So the security is the most important factor for handling such interactive transactions. File security is the one type of mechanism that is used to secure and authenticate the file.

There are various techniques used to secure the file. The files which reside in the system or which are in the way or the networks must be secure from any type of attack by the intruders. Now a day's cryptography is widely used in various areas. Cryptography is about communication in the presence of an adversary. It encompasses many problems (encryption, authentication, key distribution to name a few). The field of cryptography provides a theoreticalfoundation based on which we may understand what exactly these problems are, how to evaluate protocols that claim to solve them, and how to build protocols in whose security we can have confidence. We introduce thebasic issues by discussing the problem of encryption. Steganography is a technique that used to hide datawithin an image file. It is used encrypt the file and then decrypt that file by Steganography. In this paper we will describe some of the ongoing techniques in this area, as well as describe some of the new challenges and theways in which they are being met.

Introduction

Steganography is a technique that used to hide data within an image file. It is used encrypt the file and then decrypt that file by Steganography. There are various techniques used to secure the file. The files which reside in the system or which are in the way or the networks must be secure from any type of attack by the intruders. Now a day's cryptography is widely used in various areas. Cryptography is about communication in the presence of an adversary. It encompasses many problems (encryption, authentication, key distribution to name a few).In this paper we commence the techniques of file security and also explain the key features of the cryptography and Steganography techniques. The purpose of cryptography is to render information incomprehensible to all but the intendedreceiver. The sender enciphers a message into unintelligible form, and the receiver deciphersit into intelligible form. The word "cryptology" is derived from the Greek ***kryptos*** (hidden) and***logos*** (word) (*The American Heritage College Dictionary*, 1987). [1]

Cryptography is "The process of designing systems to realize secure communications over non-secure channels".A secure storage system should protect the privacyand the integrity of the stored data. In distributed storagesystems, data exists in two different forms, leading alsoto different exposures to unauthorized access. [2]

Steganography isabout hiding the message so that intermediatepersons cannot see the message.Data privacy issues can arise from a wide range ofsources such as healthcare records, criminal justiceinvestigations and measures, financial institutionsand transactions, biological traits, residence andgeographic records and ethnicity. Data security or dataprivacy has become increasingly important as moreand more systems are connected to the Internet. Thereare information privacy laws that cover the protectionof data or information on private individualsfrom intentional or unintentional disclosure or misuse. Thus,hiding the data in a kind of form such as within animage is vital in order to make sure that security orprivacy of the important data is protected.In this paper we will describe some of the ongoing techniques in this area, as well as describe some of the new challenges and the ways in which they are being met. [3]

File Security

File Security Methods

i. **Password Protection:** It now common practice for users of computer systems to be required to enter a user ID and a password in order to gain access to the systems. Passwords may be required to gain access at various levels from the system itself to individual applications. Within Applications users may be limited toaccessing particular modules and within these Modules to particular data fields. Furthermore users may be restricted to reading data onlywhereas others can amend data.

ii. **Communication Security:** Computers that can be accessed via telephone lines are vulnerable to hackers who have discovered IDs and passwords. Security, in this situation, can be enhanced by getting the host computer to dial back the computer that is attempting to log on.

iii. **Data Encryption**: When data is transmitted over a network and, in particular, the Internet it is generally sent in plain text and, as such, may be read by other users using specialized software. This is a particular problem when confidential information such as passwords or credit card details is being transmitted. This is dealt with by encrypting the data so that it becomes unintelligible to all except those who possess the necessary key to decode (decrypt) the data.

iv. **Access Rights:** The privileges or permissions determine specific access rights, such as whether a user can read from, write to, or execute a file.

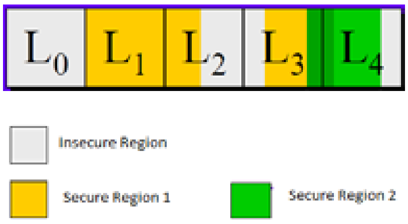
v. **Biometric Security Methods:** Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Computer science, biometrics to be specific, is used as a form of identification and access control. It is also used to identify individuals in groups that are undersurveillance.

vi. **Periodic Backups:** The most common technique of ensuring that data is not lost is to make regular periodic backups of all important files. For example, all data and applications on the CLASS fileserver are backed up every night onto tape. The tapes are kept in a safe in another Location.

Intra-File Security Technique

We present Intra File Security (IFS), an end-to-end file system encryption technology that provides the ability to encrypt independent file extents. It provides flexibility in encryption region size. A single file may contain one or more isolated or overlapping secure regions. It provides transparent to the user. It supports strong encryption.

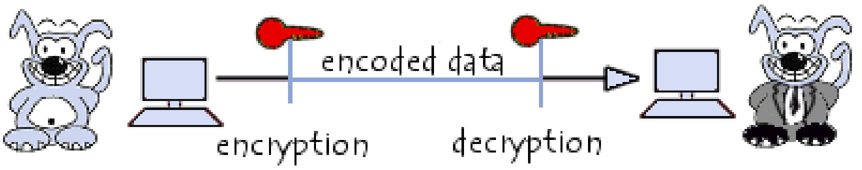
Example of an Intra File Security



Secure Segment: A Single encrypted portion of a file.

Secure Region: A set of secure segments encrypted with the same key.Other types of techniques that are used for Encryption and Decryption.

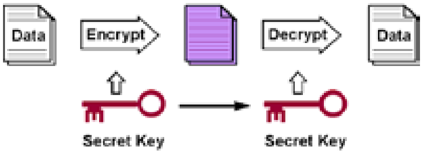
Cryptography



Cryptography word comes from Greek that is hidden secret or hiding details. It is used to study of techniques for secure communication in the presence of third parties.It about constructing and analyzing protocols. It's related to various aspects in information security such as data confidentiality, data integrity, data encryption and authentication.Modern cryptography is used in mathematics, computer science, and electrical engineering. Cryptography applications are include ATM cards, computer passwords, and electronic commerce.Cryptography is widely used in modern era.Its convert of information from a readable state to unreadable state. An encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same.

New Cryptography is based on math theory and computer science practice; its algorithms are designed around computational hardness assumptions. It is hard to break in practice by any adversary. That is possible to break such a system but it is infeasible to do so by any known practical means. This scheme computationally secure and theoretical advances (Integer factorization algorithms) and faster computing technology require these solutions to be continually adapted. This information-theoretically secures schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Secret-Key Cryptography



Secret key cryptography also called private-key encryption or Symmetric key encryption. Itis using same key for encryption and decryption.Encryption applying an operation or an algorithm to the data to be encrypted using the private key to make them unintelligible. Exclusive OR techniques are used in slightest algorithm.

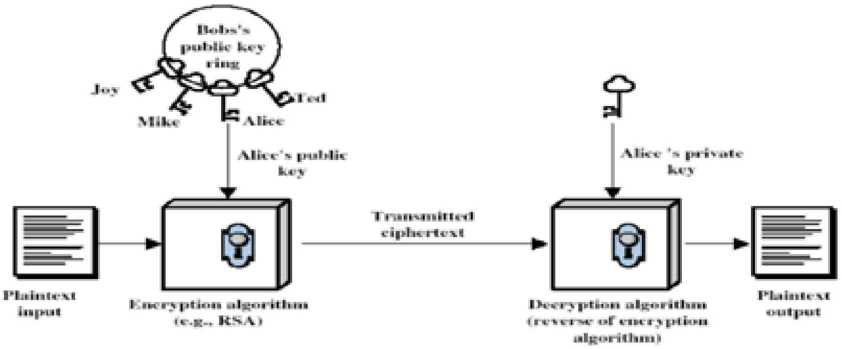
In mid 1940 the Claude Shannon proved that to be completely secure, private-key systems need to use keys that are at least as long as the message to be encrypted. Moreover, symmetric encryption requires that a secure channel be used to exchange the key.

The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). The problem of key distribution therefore arises:

Moreover, a user wanting to communicate with several people while ensuring separate confidentiality levels has to use as many private keys as there are people. For a group of N people using a secret-key cryptosystem, it is necessary to distribute a number of keys equal to N * (N-1) / 2.

In the 1920s, Gilbert Vernam and Joseph Mauborgne developed the One-Time Pad method (sometimes called "One-Time Password" and abbreviated OTP), based on a randomly generated private key that is used only once and is then destroyed. During the same period, the Kremlin and the White House were connected by the famous red telephone, that is, a telephone where calls were encrypted thanks to a private key according to the one-time pad method. The private key was exchanged thanks to the diplomatic bag (playing the role of secure channel).

Public-Key Cryptography



Public Key Systems are much slower than Symmetric Key Systems. It's 100 to 1000 times slower than DES and 10,000 times slower than AES. It's generally used in conjunction with a symmetric system for bulk encryption. PKS are based on "hard" problems such as factoring large numbers, discrete logarithms, and elliptic curves. Only a handful of public key systems perform both encryption and signatures.

RSA Algorithm

Encipher

- Choose two large prime numbers p, q
  - Let n = p*q; then f(n) = (p–1)(q–1)
  - Choose e<n such that e is relatively prime to f (n).
  - Compute d such that e*d mod f(n) = 1
- Public key: (e, n); private key: d
- Encipher message 'm' : c = me mod n
- Decipher: m = cd mod n
- Given public key (e,n) and cipher text c = me mod n , find m
- n = p*q , both unknown, both primes
  - But suppose you could factor n quickly, and discover p and q
  - The RSA algorithm for computing d (the private portion of (e, n)) is "Computed such that e*d mod f (n) = 1 "andwas executed using the same known set of inputs:n, p, q, and e.
- So by factoring n into p and q we can compute d, and thus use the RSA decryption formula to compute mC = F(m, e) = me mod n (C is cipher text)

Decipher

- F(F(m, e), d) (given C, this is the decipher step)
  - (me mod n) d mod n (symbol substitution)
  - me*d mod n (rules of modular arithmetic)

e*d mod f(n) = 1 (byconstruction of d)

k* f(n) + 1 = e*d (k exists by definitionof mod function)

- (m1 mod n * m k*f (n) mod n) mod n (by substitution)

By Euler's theorem Xf (n) mod n = 1

- m mod n
- m

Steganography

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, a form of security through obscurity. The word Steganography is comes on Greek means "concealed writing" from the Greek words stegano means "covered or protected", and graphy meaning "writing". First use of the term was in 1499 by Johannes Trithemius in his Steganography, a treatise on cryptography and Steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of Steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. [1] Therefore, whereas cryptography protects the contents of a message, Steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include Steganography coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for Steganography transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

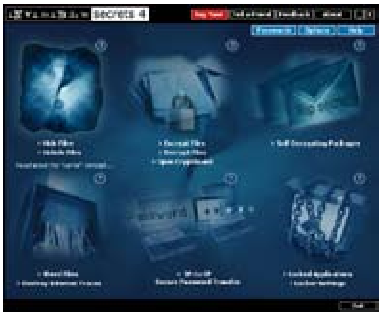
Encrypto-stego Technique or Steganography Technique

This technique is used to file encryption. Invisible Secrets 4 is used to Steganography or Encrypto-stego. Invisible Secrets 4(IS4) not only encrypts your data and files for safe keeping or for secure transfer the file across the network; it is also used to hides them in places that on the surface appear totally innocent, such as picture, sound, webpages, word file. These types of files are a perfect disguise for sensitive information. Every person such as wife, boss, or a hacker would realize that your important papers or letters are stored in your last holiday pictures, or that you use your personal web page to exchange messages or secret documents. With IS4 - File encryption software you may encrypt and hide files directly from Windows Explorer, and then automatically transfer them by e-mail or via the Internet. [3]

It features strong file encryption algorithms (including RC4), a password management solution that stores all your passwords securely and helps you create secure passwords, a shredder that helps you destroy beyond recovery files, folders and internet traces, a locker that allows you to password protect certain applications, the ability to create self-decrypting packages and mail them to your friends or business partners, a tool that allows you to transfer a password securely over the internet, and a crypt board to help you use the program from Windows Explorer. IS4 - File encryption software is shell integrated and offers a wizard that guides you through all the necessary steps needed to protect your data. IS4 used different type of encryption algorithm.

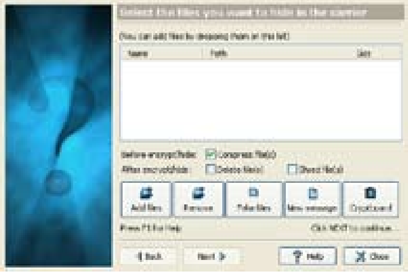
AES-Rijndael, Two fish, RC4, Cast 128, Gost, Diamond 2, Sapphire II and Blowfish.

Step1:



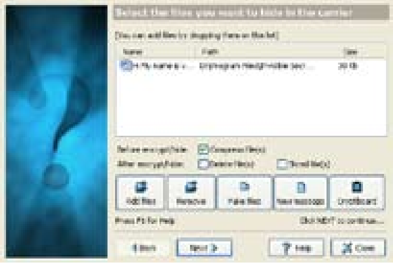
Install the IS4

Step 2:



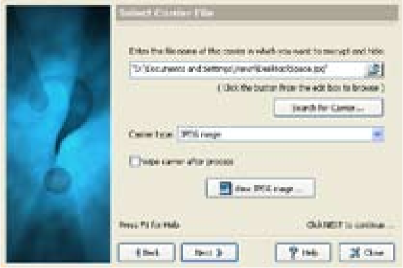
Select the add file Button

Step 3:



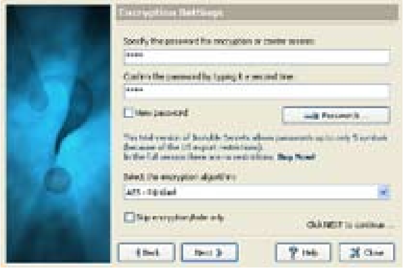
Select the Any Word File or Message File

Step 4:



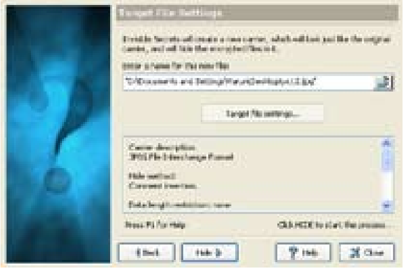
Click next and select space.jpg from Which you want to be hidingexplorer

Step 5:



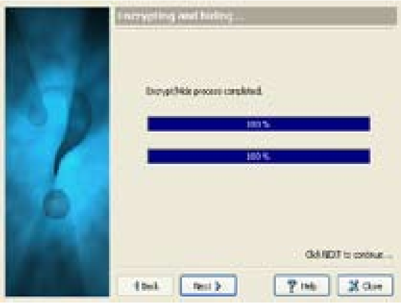
Now give the secret key and select the encryption Algorithm.

Step 6:



Now give the new name of the jpg.

Step 7:



Now Conversion is finished.

Algorithmthrough IS4 by All Algorithms Techniques -:

Algorithm for embedding data Input image.

Begin

Input: Image, Secret Message (Html, XMl, Doc Format etc), Secret Key (Pwd)
Written Secret Message into Word file;
Attach Word file to Image file by IS4;
Convert word File to Binary Codes;
Convert Secret Key into Binary Codes;
Set Bits per Unit to Zero;
Encode Message to Binary Codes;
Add by 2 units for BitsPerUnit;
Output: Convert Image;

Input Image space.jpg
without Word File

End

Algorithm for extracting data from Output image

```
Begin
Input: Output Image, Secret Key (Pwd);
Compare Secret Key;
Calculate BitsPerUnit;
Decode All_Binary_Codes;
Shift by 2 unit for BitsPerUnit;
Convert Binary Codes to Word File;
ExtractWord File;
Output: Secret Message;
```

Output Image spage.jpg
with Word File
End

Conclusions

ThispaperisproposedforCryptography and Steganographyalgorithm. System named IS4 (Invisible Secret 4) has been developed for using the proposed algorithm. That System used all 8 techniques for Algorithm. Some images are testing by this system. That Image is automatic encrypting by this System. This system encrypted various sizes of data to be hidden. With theproposed algorithm, we found that the stego image that is space.jpg. We also tested our stego images usingPSNR value. Based on the PSNR value of each images, thesteno image has a higher PSNR value. So that this Steganography algorithm is very efficient to hidethe data inside the image. IS4 SIS can be used by various users who want to hidethe data inside the image without revealing the data toother parties. IS4 maintains privacy, confidentialityand accuracy of the data.

The appropriateness of Steganography as a tool to hideextremely sensitive information has been discussed by using this methodology distribution the concept of hybridizationand a multilevel of protection of data is achieved. ThisSuggests that an image containing encrypted data can betransmitted to anybody any where across the world in acomplete secured form. Downloading such image andusing it for many a times will not permit any criminalperson to share the hidden information. Industries likeMusic, film, publishing and association like ministry andmilitary will definitely be highly benefited by the use ofsuch techniques. We can conclude here by saying thatgrouping of both Steganography and cryptography can afford us a double layer of protection.

References

[1] Research Book "Cryptography and Security Services Mechanisms and Applications "darksiderg.

[2] William Stallings, Cryptography and Network security: Principles andpractice (Second Edition), Pearson Education Asia, Sixth Indian Reprint 2002.

[3] M. Sitaram Prasad "A Novel Information Hiding Technique for Security by Using Image Steganography" 2005 JAIIT.

[4] Artz, D., "Digital Steganography: HidingData within Data", IEEE Internet Computing Journal, June 2001.

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

[6] Arvind Kumar, Km. Pooja, "Steganography - A Data Hiding Technique" International Journal of computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010.

[7] Steganography Algorithm to Hide Secret Message in side an Image RosziatiIbrahim and Teoh Suk Kuan Faculty of ComputerScience and Information Technology, University Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia Received: November 25, 2010 / Accepted: January 10, 2011 / Published: February 25, 2011.

[8] P.Y. Chen, W.E. Wu, A modified side match Schemefor imageSteganography, International Journal of AppliedScience & Engineering 7 (2009) 53-60.

[9] R. Ibrahim and T.S. Kuan, Steganography Imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings ofthe World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.

[10]"Designing an Embedded Algorithm for Data Hiding usingStenographic Techniqueby File HybridizationG. Sahoo1 and R.K.Tiwari Department of Computer Science and Engineering. B.I.T., Mesra, Ranchi Jan 2008.

Dr. Anukool Bajpai: BCA, MCA, Ph.D. (Computer Science), started his career as Assistant Professor in Computer Science in 2008 at COMM-IT Career Academy (Affiliated to GGSIP University, Delhi) New Delhi-110017. Before joining GGSIP University, he has been visiting faculty in Shri. Aurbindo College (University of Delhi) for 2 years. He has contributed research and seminar papers on various topics of Computer Science. He has organized Seminars/FDP programmes apart from participation in academic meetings of the University. He was placed as Associate Professor in August 2015 with additional charge of Officiating Principal, COMM-IT Career Academy, GGSIPU.

Dr. Bajpai is Principal, Sirifort Institute of Management Studies (Affiliated to GGSIP University, Delhi) since February 2018.

anukoolbajpai@gmail.com