Oriental Journal of Computer Science & Technology Vol. **4**(1), 189-193 (2011)

Enhancing Data Security by using Crypto-Steganography in Image

AJAY GADICHA[1], V.T. INGOLE[2] and AMIT MANIKRAO[3]

[1]Department of Information Technology, PRMIT, Badnera (India).
[2]Principal PRMTI, Badnera
[3]Department of Information Technology PRMIT (India).

(Received: December 13, 2010; Accepted: January 10, 2011)

ABSTRACT

In this paper, actually we will present a technique of secure data transmission through hiding of data in image file by replacing it's one of the LSB bit. The watermarked bit embedded into image sample to increases the robustness against noise hence by combining cryptography and steganography we will increases the security of data.

Key words: Cryptography ,Digital Watermarking, Steganoraphy

INTRODUCTION

Security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information.

Related Work

Services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The strategies and methodologies of computer security often differ from most other computer technologies. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

Basics of Cryptography

Cryptography is the process of converting the important data and information into a cipher text form and then convert it again to the decipherable form when it reaches its authorize user. The process of encryption and decryption is the main mechanism which is working and guiding the flow of data. Cryptography has two modes known as public key and secret key. Key is usually defined as the secret information which needs to be transferred over the network. The use of secret key is sometimes known as symmetric key and that of an asymmetric key is known as public key. The working of the secret key is really uncomplicated. The original information is transformed to the encrypted content using the

secret key, then with the help of another secret key it is transformed again into readable form. The working of the public key is a little different. In asymmetric transformation the private or secret key is used to transform the original data into ciphered form, then at the other end the public key is used to convert the data into decrypted data again. The public key provides slow data transformation and it is suitable to be used for converting small amount of data. Cryptography is used to secure the confidential information.

It is mechanism which is used to hide the secret information, provide authentication to users prevents the undetected amendment and prevent the unauthorized use of network by the intruder

There are numerous methods used to hide information inside of image.

The most common methods are

LSB (Least Significant Byte)
Finger Printing & Watermarking
Masking and Filtering
Substitution - Altering/Replacing the LSB

When files are created there are usually some bytes in the file that aren't really needed, or at least aren't that important. These areas of the file can be replaced with the information that is to be hidden, without significantly altering the file or damaging it. This allows a person to hide information in the file and make sure that no human could detect the change in the file. The LSB method works best in Picture files that have a high resolution and use many different colors, and with Image files that have many different formats and that are of resolution. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside The file, the file can become noticeably distorted[12].Usually 24-bit or 8-bit files are used to store digital images. The former one provides more space for information hiding; however, it can be quite large. The colored representations of the pixels are derived from three primary colors: red, green and blue. 24-bit images use 3 bytes for each pixel, where each primary color is represented by 1 byte. Using 24-bit images each pixel can represent 16,777,216 color values. We can use the lower two bits of these color channels to hide data[14]. Then the maximum color change in a pixel could be of 64-color values, but this causes so little change that is undetectable for the human vision system. This simple method is known as Least Significant Bit insertion[15]. Using this method it is possible to embed significant amount of information with no visible degradation of the cover image.

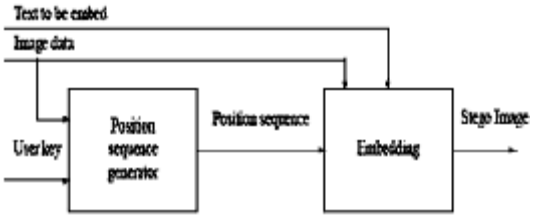


Fig. 1: Shows the process

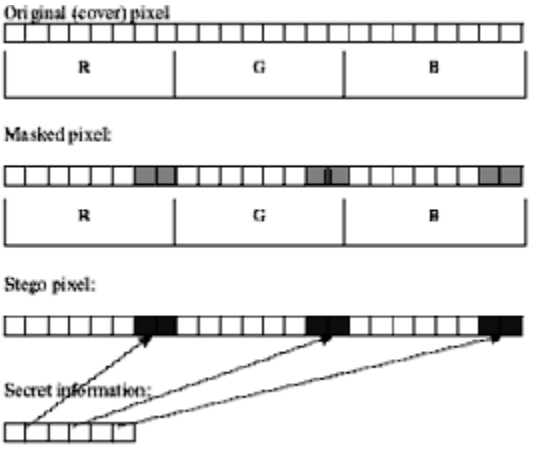


Fig. 2: Information hiding technique in bitmap image

Several versions of LSB insertion exist. It is possible to use a random number generator initialized with a stego-key and its output is combined with the input data, and this is embedded to a cover image [13]. For example in the presence of an active warden it is not enough to embed a message in a known place (or in a known sequence of bits) because the warden is able to modify these bits, even if he can't decide whether there is a secret message or not, or he can't read it because it is encrypted. The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithm itself, instead

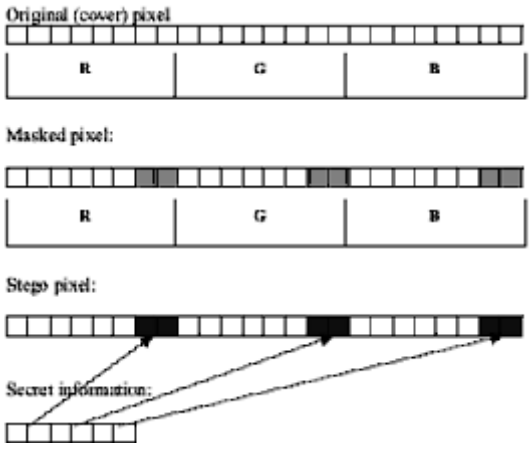
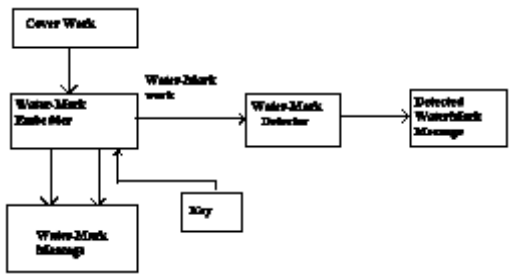


Fig. 3: Information hiding in bitmap image

Fingerprinting and Watermarking
"Information hiding technique"

Several versions of LSB Insertion exist. It is possible to use a random number generator initialized with a stego-key and its output is combined with the input data, and this is embedded to a cover image[13]. For example in the presence of an active warden it is not enough to embed a message in a known place (or in a known sequence of bits) because the warden is able to modify these bits, even if he can't decide whether there is a secret message or not, or he can't read it because it is encrypted. The usage of a stego-key is important, because the security of a protection system should not be based on the secrecy of the algorithm itself, instead Now a days steganography is more and more important in publishingand broadcasting industries, where the embedding of copyright marks or serial numbers is needed in digitalfilms, photos and other multimedia products. Some steganographic applications are able to scan the Internet, and to detect a copy of aspecific image,or the modified image is published – so an illegal usage of a copyrighted image can be detected.



Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Proposed System
Analysis/Design

The Image stegnography is the area of INFORMATION SECURITY in which data will be hidden inside a image file. Image file is a simple file format that provides a maximum capacity to hide a data than any other image file format. The current dissertation work will be combination of Cryptography & stegnography technologies. This proposed work could be implemented technically using some suitable web development programming tools (c#. net).

Cryptography

The key idea of the proposed Cryptography technology that plays a vital role to encrypting a data before inserting into an image file. Here I will use RSAalgorithm that encrypt a secret message or data.

RSA Algorithm

The RSA algorithm scheme is a block cipher in which the plain text and Cipher text are integers between 0 & n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. That is , n is Less that 2^{1024} .the scheme was developed by Rivest, Shamir & Adleman makes use of an Expression with exponentials. Plain text is encrypted in block with each blockhaving a binary value less than some number n. that is block size must be less than or equal to log2 (n);In general Block size is 'i' bits where $2^i < n < 2^{i+1}$

The RSA algorithm which will be stated as follows :

1. Pick P , Q
2. Calculate n = P *Q
3. Calculate $\Phi(n) = (P-1)(Q-1)$
4. Select integer e;where gcd
   $(\Phi(n), e) = 1; 1 < e < \Phi(n)$
5. Calculate d ; $d = e^{-1} \pmod{\Phi(n)}$

Encryption and decryption are of the following form for some plaintext block M and cipher text For Encryption I will proposed a plain-text as M & for decryption I will proposed a Cipher text as C. Most widely used encryption scheme to encrypt a data before insert into image file. **Encryption**
Plain text:M < n
Cipher text:$C = M^e \bmod n$

Stegnography

Steganography is a type of hidden communication that literally means "covered writing" (from the Greek words stegano or "covered" and graphos or "to write"). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties The process of finding these distortions is called Statistical Steganalysis. There are many forms of steganography including audio, video and image media. These forms of steganography often are used in conjunction with cryptography, so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and *then* decrypt it. The following formula provides a very generic description of the pieces of the steganographic process:

Cover Medium + Hidden Data + Stego Key = Stego Medium

Here example of encoding of replacing LSB of the any data stream :
10010101 00001101 11001001
1010110 00001111 11001010
10011111 00010000 11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed):
10010101 00001100 11001001
10010111 00001110 11001011
10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011

Conclusion & future work

Here in the proposed dissertation work we need to provide the input as a image file (in. Jpeg, .png,.bitmap format) the secret message, which may be available in any of the file formats(.txt, .doc, .xls, .pdf, etc). This image file will embed the secret message inside it. This message will be inserted by substituting the bit of the LSB in the stream of 16 bits of the image wave file in the time domain.

Here we will using the concept of a key file that actually selects the image bit streams which may be watermarked with the secret message bits. After the replacement the output of the proposed work will be a stego- object, which will contain the image file as the actual output file (in .jpeg,.png,.bitmap format). This image file contains the inputted image file which has the secret message hidden inside it. We need to separate the watermarked bit information from this stego-object to obtain the secret message, which is hidden in the image file, by virtue of this we will get our hidden message on the remote or destination side.

The goal of Crypto-stegnography is to hide the messages inside other harmless messages (here a image file) in way that doesn't allow any intruder to even detect that there is a second secret message present inside it. By using this proposed algorithm we can hide our file of any format (.txt, .doc,..xls, .pdf, etc) in an Image file. We can than send the Image via email attachment or post in on the website & any one with \ knowledge that it contains secrete information & who is in possession of the encryption password, will be able to open the file, extracts the secrete information & decrypt it.

REFERENCES

1. Neil F. Johnson, "Information Hiding: Steganography & Digital watermarking", 1995 [online], Available: http://www.jjtc.com/ Steganogr aphy/
2. "stegoarchive", *stegoarchive.com,*1997 [online],
3. S. Lyu, H. Farid, "Steganalysis using color wavelet statistics and one-class support vector machines", *in: SPIE Symposium on Electronics Imaging* (2004).
4. I. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", *IEEE Trans. Image Process.* **6**(12): 1673-1687 (1997).
5. Neil F. Johnson and Sushil Jajodia, "Steganography: Seeing the Unseen" *IEEE Computer*, February 1998. [online],Available:http://www.jjtc.co m/pub/ r2026a.htm