ISSN:0975-9646
Ravi Kumar. B et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1453-1456

Data Security and Authentication Using Steganography

Ravi Kumar. B [#1], Murti. P.R.K.*[2]

[1,2] *Department of Computer and Information Sciences, University of Hyderabad, (P.O) Central University, Gachibowli, Hyderabad 500046, India.*

***Abstract*—Steganography is the art of *covered*, or *hidden*, *writing*. The purpose of *steganography* is covert communication to hide the existence of a message from a third party. This proposed system deals with implementing security-using *Steganography*. In this technology, the end user identifies an image which is going to act as the carrier of data. The data file is encrypted and authenticated. This message is hidden in the image. The image if hacked or interpreted by a third party user will open up in any image previewer but not displaying the data. This protects the data from being invisible and hence be secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the image.**

***Keywords*— Steganography, Security, authentication**.

I. INTRODUCTION

The art of writing in cipher, or in characters which are not intelligible except to persons who have the key is cryptography. *Steganography* is the art of *covered*, or *hidden*, *writing.* The purpose of steganography is *covert communication* to hide a message from a third party. This differs from *cryptography*, the art of **Steganography** *secret writing*, which is intended to make a message unreadable by a third party but does not hide the very existence of the secret communication. While steganography is separate and distinct from cryptography. Both have been used throughout recorded history as means to protect information, there are many analogies between the two and, in fact, some authors categorize steganography as a form of cryptography since *hidden* communication certainly is a form of *secret* writing [1]. Steganography hides the covert message but not the fact that two parties are communicating with each other. The embedded data is the message that one wishes to send secretly. The stego process generally involves placing a *hidden message* within some transport medium, called the *carrier*. The secret message is embedded within the carrier to form the *stego medium*. The use of a *stego key* may be employed for encryption of the hidden message and/or for randomization within the stego scheme[19]. Classical steganography system depend on keeping the encoding system secret, but modern steganography is detectable only if secret information is known, e.g. a secret key. The actual process of embedding information in another file usually involves two classes of files –message files and cover files. The message file is the information that is hidden or embedded during the steganographic process. Depending on what a user is hiding, the message file can be any type of information source – audio, graphic, text, or even malicious files. The only restriction on a message file is that it must fit within the cover file. The cover file is the medium that contains the message file after the steganographic process is applied. Again, the intent of steganography is to maintain the initial visible quality of the cover file after the message file is hidden. Therefore, the file should not draw undue attention to itself or compromise any features and characteristics generally found in other similar files of its particular type. A cover file can also be referred to as a container file or stego-file. The latter term usually only applies to the cover file after the message file has actually been embedded.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [3]. The strength of steganography can thus be amplified by combining it with cryptography.

In our method we using the technique of hiding the data with an image file, the visibility of the image, resolution or clarity is not being affected. The hidden data can be of length in size. To the hacker, only, the image is make going to be visible when previewed and not a trace of the hidden data. If the image file is opened across a text editor, then also the data is not going to be visible as the information is stored in an encryption form, which is also binary. Hence making it difficult for the enclosure to differentiate the data to the image file.

II. RELATED WORK

In today's dynamic and information rich environment, information system has become vital for any Organization to survive. With the increase in the dependence of the organization on the information system there exists an opportunity for the competitive organizations and disruptive forces to gain access to other organizations information system. This hostile environment makes information systems security issues critical to an organization. The Internet is a vast channel for the mass dissemination of information (e.g. publications and images), Images provide excellent carriers for hidden information. Many different steganographic techniques exist.

In Least-Significant Bit Encoding (LSB) a digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest steganographic techniques embed the bits of the message directly into the least-significant bit plane of the cover image in a deterministic sequence. Modulating the least-significant bit does not result in a human-perceptible difference because the amplitude of the change is small. Other techniques "process" the message with a pseudorandom noise sequence

before or during insertion into the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods [4]. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image.

Statistical technique that uses redundant pattern encoding to embed a message in an image [9]. The algorithm adds redundancy to the hidden information and then scatters it throughout the image [6]. A pseudorandom generator is used to select two areas of the image (or patches), say patch A and patch B [10]. All the pixels in patch A is lightened while the pixels in patch B is darkened [10]. In other words the intensities of the pixels in the one patch are increased by a constant value, while the pixels of the other patch are decreased with the same constant value [5]. The contrast changes in this patch subset encodes one bit and the changes are typically small and imperceptible, while not changing the average luminosity [6]. A disadvantage of the patchwork approach is that only one bit is embedded. One can embed more bits by first dividing the image into sub-images and applying the embedding to each of them [1]. The advantage of using this technique is that the secret message is distributed over the entire image, so should one patch be destroyed, the others may still survive [6]. This however, depends on the message size, since the message can only be repeated throughout the image if it is small enough. If the message is too big, it can only be embedded once [9]. The patchwork approach is used independent of the host image and proves to be quite robust as the hidden message can survive conversion between lossy and lossless compression [1].

Recently, a great deal of research has been reported in expanding the hiding capacity and robustness of steganographic techniques by exploiting the properties of the human visual system [7, 8, 11]. The development of accurate human vision models facilitates the design and development of perceptual masking hiding systems [8]. Steganographic techniques designed to be robust to lossy image compression must insert the message into the cover in a manner that is perceptually significant. Techniques that attempt to embed information only in a perceptually insignificant manner, such as LSB embedding techniques, are vulnerable to having the embedded data distorted or quantized by lossy image compression. The masking properties of the human visual system allow perceptually significant embedding to be unnoticed by an observer under normal viewing conditions [8]. “Masking” refers to the phenomenon where a signal can be imperceptible to an observer in the presence of another signal (referred to as the masker.) The masking properties are the reason why it is difficult for one to find a randomly placed needle in a haystack; the needle can be in plain view to an observer (not obscured by any object) yet the observer will have great difficulty locating the needle. Masking (sometimes referred to as image-adaptive [8]) systems perform analysis of the image and use the information to determine appropriate regions to place the message data. Masking systems can also use the analysis to vary the strength (amplitude) of the embedded data based upon local image characteristics to maximize robustness. These systems can embed in either the spatial or a transform domain.

M.S.Sutaone, M.V. Khandare, developed an interesting application of steganography and cryptography, where a steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method. In this method, the secret data are spread out among the cover image in a seemingly random manner. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out. The advantage of this method is that it incorporates some cryptography in that diffusion is applied to the secret message [12].

Miroslav Dobsicek developed the next interesting application of steganography where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information [13].

Nameer N. EL-Emam proposed an algorithmic approach in 2007 to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse steganoalysis too [14].

G. Sahoo and R. K. Tiwari in 2008 proposed a good method. In their method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography. And due to this reason they have used a stego key for the embedding process [15].

Unfortunately, modifying the cover image changes its properties as well as its features, so eavesdroppers can detect the distortions in the resulting stego-image’s statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. So, in order to obtain more security in our prescribed method.

III. OUR PROPOSED SYSTEM

The algorithm present in the existing system was somewhat complicated. In cryptography, the meaning of data has been changed. So, it makes intention to the hacker to hack or destroy the data. In our proposed system, we implementing a new technology called steganography for data security, it not only change the meaning of data but also hides the presence of data from the hackers. The main objective of this system is hiding large amount of encrypted and authenticated data irrespective of the size, dimensions of the image and without disturbing the clarity of the image.

IV. ENCRYPTION

In the encryption process from the message all printable characters occupies 7 bits and the last bit value is 0. In the first step I am taking 8 characters at a time from the data file

and the last character 7bits are adjusted to its previous 7 characters and these 7 characters are maintained separately in another file. Like that every 8 characters are converted in to 7 characters and all these encrypted characters are maintained separately in another file (say encr1). After that by using a random function we generate a 4 bit polynomial. Take 4 characters from the encrypted file and by using this polynomial perform modulo- 2 division operation on these 4 characters then we will get a remainder of 3bits. In the second step of encryption these 4 characters, polynomial and the remainder are adjusted in 5 bytes. These five bytes are maintained separately in another file (say encr2). Like for every 4 characters of first encrypted file after performing modulo-2 division operation, 5 bytes are maintained in the file encr2.

A. Data embed

This method deals with identifying the (encrypted data) **cipher text** with key (encr2) and the image to embed the data before it can be transmitted. Open the given image file in the binary mode and find the size of the original image. This size is maintained in the image itself by using a special signature which is useful to retrieve the data from the image. Now add **cipher text** from the file encrc2.cmp to the image. Now the image is ready to transmit. If the image already contains some data you cannot add some more data for the same image. So before embedding data check whether the image contains data or not.

B. Data retrieve

After receiving the image through some media, the end user also opens the image in the binary mode and checks whether the image contains the special signature or not. If signature found then image contains data. Then get the original size of the image from that signature. Now except original data of the image extract data from the image up to the special signature. This is encrypted data (cipher text). This data is maintained in a file say decypt2..For this data check authentication whether data is corrupted or not and then decrypt the data to get the original message. Take five characters from the retrieved data file (decypt2.) and detect the key from the fifth character and by using this key perform modulo 2 division on these five characters. If the remainder is zero then there is no corruption in the data otherwise data is corrupted. If the data is not corrupted then remove key and remainder from the five characters and arrange the bits in 4 bytes to get the encrypted data. These 4 bytes are maintained separately in a special file say dect1. Like that for every 5 bytes from decypt1. after removing key and remainder the 4bytes are maintained in the file dect1.cmp.This is the encrypted file without key.

C. Decryption

Take 7 bytes from the encrypted file decypt1. and decrypt these bytes in such a way that take last bit from these 7 bytes and arrange them in a new byte. Make the last bit value of these 7 bytes as well as the new byte as 0. Now maintain these 8 bytes in special file say **data1.** This is the decrypted data. Like that for every 7 bytes from the encrypted file form 8 bytes and maintain these bytes in the file **data1**. This file contains the original data

V. SAMPLE TEST RESULTS

A. Encoding: Sample – 1 (image pc1.jpeg)

The system deals with security of data during transmission. Commonly used technology is cryptography. This proposed system deals with implementing security-using steganography

Plain text (175 bytes)

Thå óùóåí dåáì wéth óãõòétù f
äatá uòinç ôánsíióóïn® Cïíïnìy õóä ôåcèîlogy
éscòypôïçaphù. Ôéó ðrïðseä óùóåí
dåáì wéôh éðleíeîônç såãõiôù-uóég óôeçáography

Encrypted data (156 bytes)

y+B£O/ŸÏŸ□+!lK½g
MC§M□—¯›}Ë§LK! 3K-
§O;sO•Kw¥□›Okš}sw□Ÿ□oz{Ïcw}O'Ÿ©K/¥
K{gwE□IË={Ï“™O?□£□OËC*ƒ*□N¥t{—
…žK+Ÿ‡~OÏ™!Io/□□g+"□§K½O‡ME{/k+c□;w§
uO+™□Ï£O¬□O›-o□§□>K□;.{*ƒ*
“:IËF

Encrypted data with key(195 bytes)

Fig.1 Actual image (pc1.jpeg) 160 × 120

B .Decoding

Retrieved data from the image pc1.jpeg

Fig.2 Stego image (pc1.jpeg) 160 × 120

y+B£O/ŸÏŸ□+!lK½g
MC§M□—¯›}Ë§LK! 3K-
§O;sO•Kw¥□›Okš}sw□Ÿ□oz{Ïcw}O'Ÿ©K/¥
K{gwE□IË={Ï‘™O?□£□OËC*f*□N¥t{—
…žK+Ÿ‡~OÏ™!Io/□□g+"□§K½O‡ME{/k+c□;
w§uO+™□Ï£O¬□O›-o□§□>K□;.{*f*
“.ËE

Retrieved data from stego image(195 bytes)

Thå óùóåí dåái wéth óãõòétù f
äatá uòinç ôánsíióóïn® Cïíïnìy õóä ôåcèîlogy
éscòypôïçaphù. Ôéó ðrïðseä óùóåí
dåái wéôh éðleíeîônç såãõiôù-uóég óôeçáography

Authenticated data (encrypted data) (156 bytes)

The system deals with security of data during transmission. Commonly used technology is cryptography. This proposed system deals with implementing security-using steganography

Decrypted data (175 bytes)

C. Results analysis

We have tested our method for different sets of images as well as messages. For each and every normal jpeg and the bmp images the proposed method is working fine. The analysis for different data is shown in the below table1 and table2.

TABLE 1

Image Size (bytes) IS	Data size (bytes)	After encryption Size (bytes)	Encrypted data with key (bytes) ES	Stego image size (bytes) IS+ES+10	Data retrieved from stegoimage (After decryption) (bytes)
4,608	1	4	5	4,623	4
4,608	2	4	5	4,623	4
4,608	3	4	5	4,623	4
4,608	4	4	5	4,623	4

TABLE 2

Image Size (bytes) IS	Data size (bytes)	After encryption Size(bytes)	Encrypted data with key(bytes) ES	Stego image size (bytes) IS+ES+10	Data Retrieved from stegoimage (After decryption) (bytes)
4,608	1	4	5	4,623	4
4,608	2	4	5	4,623	4
4,608	3	4	5	4,623	4
4,608	4	4	5	4,623	4

VI. SUMMARY

The system deals with secure transmission of data. This system deals with implementing security using steganography. ie . hiding large amount of information in an image without disturbing the image clarity and its pixels. The main objective of this system is hiding large amount of encrypted and authenticated data irrespective of the size, dimensions of the image and without disturbing the clarity of the image. In this chapter we have describe the methodology for the entire process. That is how to encrypt, decrypt, authentication, and inserting message into image, identify the message from the stego image and retrieve the message from the stego image.

VII. CONCLUSIONS

In this system the designed tool deals with providing easy and secure information. The data is encrypted with key and embedded with an Image which is ready to send through communication channels. It is going to be reliable and secure. At the receiving end, the tool checks the availability of data and authenticates the data. It retrieves data from the stego image and decrypts it. This package contains two sessions. The first sessions deals with Embedding, Retrieving and Authentication of data. The second sessions provide the utilities for encryption and decryption of data.

REFERENCES

[1] F. A. P. Petitcolas, , R. J. Anderson, and M. G. Kuhn. "Information Hiding-A Survey." *Proceedings of the IEEE*, special issue on protection of multimedia content, 87(7):1062-1078, July 1999.

[2] R. J. Anderson, and F. Petitcolas. "On the Limits of Steganography." University of Cambridge, Computer Laboratory: Cambridge, UK. September 1997. Published in *IEEE Journal on Special Areas in Communications,* v 16 no 4: 463-473. (May 98). http://www.cl.cam.ac.uk/~fapp2/papers/jsac98-limsteg/.

[3] H. Wang, & S.Wang, “Cyber warfare: Steganography vs. Steganalysis”, *Communications of the ACM*, 47:10, October 2004.

[4] R. Chandramouli, , M. Kharrazi, & N. Memon, “Image steganography and steganalysis: Concepts and Practice”, *Proceedings of the 2nd International Workshop on Digital Watermarking*, October 2003

[5] L.M. Marvel, Boncelet Jr., C.G. & C. Retter, “Spread Spectrum Steganography”, *IEEE Transactions on image processing*, *8:08*, 1999

[6]. N. Johnson and S. Jajodia, “Steganalysis of images created using current steganography software,” *Lecture Notes in Computer Science*, Vol. 1525, pp. 273-289, 1998.

[7] M. Swanson, M. Kobayashi, and A. Tewfik, “Multimedia data embedding and watermarking technologies,” *Proceedings of the IEEE*, Vol. 86, No. 6, pp. 1064-1087, June 1998.

[8] R. Wolfgang, C. Podilchuk and E. Delp, “Perceptual watermarks for images and video,” to appear in the *Proceedings of the IEEE*, May, 1999. (A copy of this paper is availavle at: http://www.ece.purdue.edu/~ace).

[9] N.F. Johnson, & S. Jajodia, “Exploring Steganography: Seeing the Unseen”, *Computer Journal*, February 1998

[10] W. Bender, D. Gruhl, N. Morimoto, & A. Lu, “Techniques for data hiding”, *IBM Systems Journal*, Vol 35, 1996

[11] I. Cox and M. Miller, “A review of watermarking and the importance of perceptual modeling,” *Proceedings of the SPIE/IST&T Conference on Human Vision and ElectronicImaging II* , SPIE Vol. 3016, San Jose, CA, pp. 92-99, February1997.

[12] Sutaone, M.S., Khandare, M.V, “Image based steganography using LSB insertion technique”, IEEE WMMN, pp. 146-151, January 2008.

[13] M. Dobsicek, “Extended steganographic system”, 8th International Student Conference on Electrical Engineering, FEE CTU 2004, Poster 04.

[14] Nameer N. EL-Emam, “Hiding a large amount of data with high security using steganography algorithm”,Journal of Computer Science, Page(s): 223 – 232, April 2007.

[15] G. Sahoo, R. K. Tiwari, “Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File ybridization”, IJCSNS, Vol. 8, No. 1, pp. 228-233, January 2008.