Message Security over Image Communication

[1]Dinesh Goyal, [2]Vishal Srivastava,
dinesh13dg@gmail.com
vishal0882@gmail.com
Arya College of Engg. & IT, Jaipur, India,

ABSTRACT

Previous work of us was to generate a secure Steganographic System with a password authentication, which is good enough for the host machine. But when the Steganographed image is communicated over the channel the security is quite low and interpretation of Steganography and the message is quite possible.

In this paper an authentication system for Steganographed image is proposed in which a authentication watermark is used for the Steganographed image while being transmitted over the communication channel. They key distribution for the secure communication is generated using Kerberos.

Keywords

Steganography, Kerberos, RDA Algorithm

1. INTRODUCTION

Steganography comes from the Greek words Steganos(covered) & Graptos(writing). Thus Steganography is a process that hides private or sensitive information (file). Inside something that appears to be nothing out of the usual.

In other words Steganography is a process that hide a file (original info), inside another file (carrier file) i.e. picture, video, or audio file. When information or a file is hidden inside a carrier file, the data is usually encrypted. Steganography is often confused with Cryptography because the two are similar in the way that both are used to protect the information. But in Steganography the information or the file is not modified, and is just embedded into the cover file while in Cryptography the original message is modified using a key to attain the security.

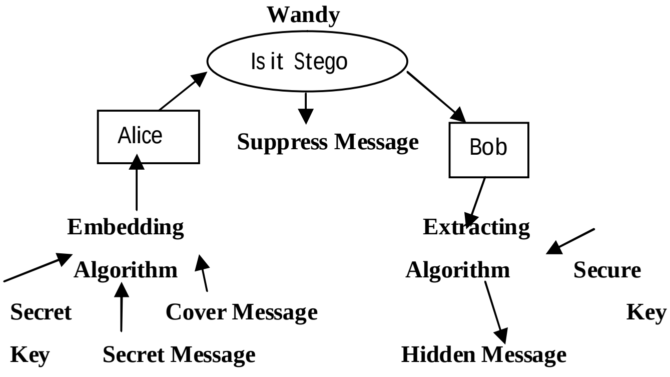


Fig 1 General Model of Steganography[3]

Here Alice & Bob are two persons who wish to make a secure communication avoiding a eavesdropper (Wandy). In order to do so, Alice embeds Secret Message M into Cover Object C, and obtains a Stego Object S. The Stego Object S is then sent through the public channel. The Wandy is free to examine all Message exchanged between Alice & Bob. [11]

These are the following definitions for Steganography:

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-object: refers to the object which is carrying a hidden message. So given a cover object, and a messages the goal of the steganographer is to produce a stego object which would carry the message.

Steganalysis: The process of detecting hidden information inside of a file.

Redundant Bits: Pieces of information inside a file which can be overwritten or altered without damaging the file.

Payload – The information which is to be concealed.

2. TYPES OF STEGANOGRAPHY

There are two basic types of Steganography, which are:

1. Linguistic
2. Technical

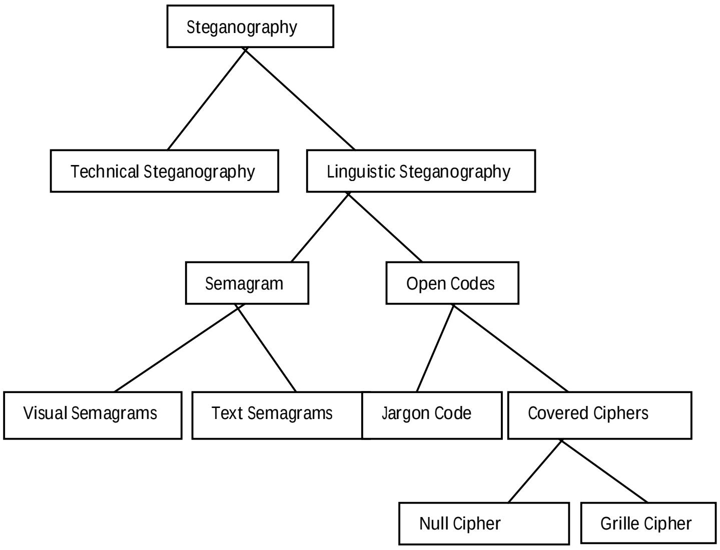


Fig. 2 Classifications of Steganography Techniques (Adapted from Bauer 2002)[15]

2.1 LINGUISTIC STEGANOGRAPHY

Linguistic Steganography can be described quite simply as any form of Steganography that uses language in the cover. The goal of the NICETEXT is to provide a program that can transform cipher text into the text that looks like natural language while still providing a cover for the original cipher text. An added benefit of this type of program is that it can be applied to many different languages.

a. Open Codes

In the case of open codes, the openly readable text is mostly well constructed. It can contain certain words or sentences, certain letters can be in certain places in the text, or words can be hidden in vertical or reversed.

Types of open Codes:

- Masking
- Null Ciphers
- Cues
- Music
- Largon Code
- Newspaper Code
- Grilles

b. Text Semagrams

Text Semagrams work with graphical modifications of the text. They concern details that are tiny but nonetheless visible.

- Type Spacing and Offsetting
- Tiny Spaces
- Old Typewriter Effect
- Real Semagrams

2.2 TECHNICAL STEGANOGRAPHY

Technical Steganography is a little broader in scope because it does not necessarily deal with the written word even though it communicates information. Technical Steganography is the method of Steganography where a tool, device, or method is used to conceal the message. [10]

- **Invisible ink**

It is a special ink that is colorless and invisible until treated by a chemical heat or special light. Because invisible ink does not have to be used to write words it can safely be considered a form of technical Steganography.

- **Microdots**

The microdot is a form of micro photography that allows for sheets of printed material to be reduced to a dot that is no larger than ½ millimeter across. In 1946 J. Edger, coated that the microdots was “the enemy’s master piece of espionage”, and indeed it has been just that. The microdot has taken a new form in the modern world and is being used to uniquely identify automobiles and other motor crafts. There is even a potential for a microdot to be attached to a strand of DNA.

- **Computer based methods**

With the advancements in computer technology throughout the 1990s, this is the newest of the Steganography methods and can be very effective in its native environment. There are many computer based methods including substitution of bits, addition of bits and others.

3. TECHNIQUES OF STEGANOGRAPHY

There are many approaches to hiding the embedded file. The embedded file bits can be inserted in any order, concentrated in specific areas that might be less detectable, dispersed throughout the cover file.

1. Substitution Techniques:

Substitute redundant parts of a cover with a secret message. In this method it chooses a subset of cover elements and substitute least significant bit(s) of each element by message bit(s), also in this method Message may be encrypted or compressed before hiding in some cases pseudorandom number generator may be used to spread the secret message[5].

For example, the following string of bytes represents part of a cover, a picture:

10000100 10000110 10001001 10001101

01111001 01100101 01001010 00100110

These bits make up a color value in a picture, a shade of red or blue etc. The last bit of the binary digit considered as the least significant bit, the change in LSB’s value has little effect on the information the byte is representing.

We introduce hidden message; which is the number of a locker in a bus terminal, locker number 213. 213 represented as binary number is 11010101

Now, using the least significant bit method, the 213 will be blended into our cover. We will do this one byte at a time:

10000100: The 0 is replaced by a 1, the first bit of our message.

10000110: The 0 is replaced by a 1, the second bit of our message.

10001001: The 1 is replaced by a 0, the third bit of our message.

10001101: The 1 is left alone because it corresponds to the 1 in our message.

01111001: The 1 is replaced by a 0, the fifth bit of our message.

01100101: The 1 is left alone because it corresponds to the 1 in our message.

01001010: The 0 is left alone because it corresponds to the 0 in our message.

00100110: The 0 is replaced by a 1, the eighth bit of our message.

Here only five bits have been altered, and our message has been embedded. Now, while this example deals with only 8 bytes of data, imagine the amount in a cover image that is 500Kilobytes or 1 megabyte. Within all those 1s and 0s are a lot if least significant bits can be changed with little or no noticeable difference to the cover image.

The LSB technique is commonly used in Steganography applications because the algorithm is quick and easy to use; LSB also works well with gray scale as well as color images.

2. Transform Domain Techniques:

Transform domain techniques hide message data in the “transform space” of a signal. This technique splits the cover image into 8 X 8 blocks. Each block is used to encode one message bit; these blocks are chosen in a pseudorandom manner. The relative size of two pre defined DCT coefficients is modulated using the message bit. The two coefficients are chosen from middle frequencies (trade off between robustness and imperceptibility. For Example, the Discrete Cosine Transform (DCT) is the keystone for JPEG compression and it can be exploited for information hiding.

3. Spread Spectrum Technique:

In this technique; the message is spread over a wide frequency bandwidth.

Direct Sequence

In direct sequence spectrum, the stream of information to be transmitted is divided into small pieces. Each of the pieces is allocated to a frequency channel of the spectrum. The data signal, at the point of transmission is combined with a higher data- rate bit sequence that divides the data according to a predetermined spread ration. Redundant data rate bit sequence code helps the signal resist interference and enables the original data to be recovered if any of the data bits are damaged during the transmission.

Frequency Hopping

This technique divides a broad slice of the bandwidth spectrum into many possible broadcast frequencies. In general frequency hopping devices use less power and are cheaper, but the performance of direct sequence spread spectrum systems is usually better and more reliable.

4. Statistical Techniques:

In this Technique we encode information by changing several statistical properties of a cover. The cover is split into blocks. Each block is used to hide one message bit. If the message bit is “1” then the cover block is modified, otherwise the cover block is not modified.

5. Distortion Techniques:

In this we store information by signal distortion. This method of Steganography creates a change in a cover object to hide information. The secret message is recovered when the algorithm compares the changed, distorted cover with the original.

6. Cover Generation Techniques:

Encode information in the way a cover is generated Cover generation methods are probably the most unique of the six types. Typically a cover object as chosen to hide a message in but that is not the case here. A cover generation method actually creates a cover for the sole purpose of hiding information. Spam mimic is an excellent example of a cover generation method.

4. STEGNALYSIS

The art of detecting Steganography is referred to as Steganalysis**.** To put it simply Steganalysis involves detecting the use of Steganography inside of a file. Steganalysis does not deal with trying to decrypt the hidden information inside of a file, just discovering it.

Two major tools in Steganalysis, information theory and statistical analysis, reveal in clear terms the tremendous potential for hidden information. Though the first goal of Steganalysis is detection, there can be additional goals such as disabling, extraction, and confusion. While detection, disabling, and extraction are self-explanatory, confusion involves replacing the intended embedded file (Katzenbeisser, 2000).

Steganalysis techniques can be classified in a similar way as cryptanalysis methods, largely based on how much prior information is known (Curran and Bailey 2003; Johnson and Jajodia 1998B).

Steganography-only attack: The Steganography medium is the only item available for analysis.

Known-carrier attack: The carrier and Steganography media are both available for analysis.

Known-message attack: The hidden message is known.

Chosen-Steganography attack: The Steganography medium and algorithm are both known.

Chosen-message attack: A known message and Steganography algorithm are used to create Steganography media for future analysis and comparison.

Known-Steganography attack: The carrier and Steganography medium, as well as the Steganography algorithm, are known.

5. DIGITAL WATERMARKING

Digital watermarking is the art and science of embedding copyright information in the original files. The information embedded is called ‘watermarks ‘. Digital watermarks are difficult to remove without noticeably degrading the content and are a covert means in situation where copyright fails to provide robustness.

Digital watermark is a signal which added to a document to authenticate it and to prove the ownership. A commonly encountered digital watermark is the logo most television channels display on the top of the television screen. Not only does it advertise the channel but also provides the legal benefit of having a source signature persist during video recording.

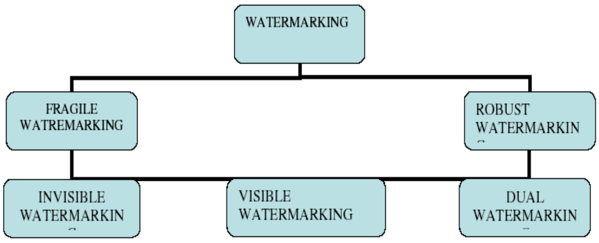
The characteristics of watermarking system largely depend on its application scenario. For instant copy write protection application require that the watermark is robust against most common data manipulation, i.e. its presents can still be detected after nondestructive transformation of host document. Two approaches for watermarking data authentication are possible:

1. Fragile watermarking

2. Robust watermarking

Fragile watermarking refers to the case where watermark inserted within the data is lost or altered as soon as host data undergoes any modification. Watermark loss or alternation is taken as evidence that data has been tampered with, whereas the information contained within data used to demonstrate data origin In case of robust watermarking a summary of the candidate frame or video sequence is computed and is inserted within the video sequence. Information about the data origin is also with the summary. To prove data integrity the information conveyed by the watermark is recovered and compared with the actual content of the sequence. Their mismatch is taken as an evidence of data tampering. The capability to localize the manipulation will depend on the summary of which is embedded in to the image.

5.1 Types of Watermarking



6. PROPOSED WORK

In the newly proposed model for Steganography there are basic three layers of security for the text message are being used which have either existed in earlier work but wore quite week in terms of security or were not existing:

1. **Authentication:** Authentication is done using email-id, by watermarking and RSA algorithm.
2. **Cryptography:** In this layer another layer of security is introduced, even though this layer of security has been existent in earlier work too but the basic drawback with them was to every time sharing a key with each transaction. Instead of that in this proposed model Vigenere Cipher model has been modified with ECB model algorithm which does not require every time key transaction.
3. **Steganography:** This is the upper most layer, which now have two more layers inside that is Authentication & Cryptography to increase the security of the text message.
4. **Key Distribution:** The key required for watermarking is generated using Kerberos.

The proposed works for a simple text file being embedded inside a simple bmp image file using LSB technique. The proposed model works in this manner.

The proposed works for a simple text file being embedded inside a simple bmp image file using LSB technique.

6.1 Process for Authentication

User A uses his email-id, which is encrypted using RSA algorithm which uses the private key of user A. This encrypted message is converted to the respective ASCII code and which in turn finally embedded as a visible watermarking into the Steganographed image.The receiver B on the other hand detects the encrypted watermark from the watermarked Steganographed image. This file yield two arts –one is encrypted Steganographed image file and second one is encrypted watermarked message. Here now the ASCII code of the message is converted back to the respective character code then again RSA algorithm is applied on the message with the public key of the user A. This leads to the production of the respective sender's email-id which shall be similar to the email-id of the senders of course shall be decoded with the sender's public key.

6.2 Process for Cryptography

In this model Vigenere Cipher Model and ECB encoding model are combined where instead of using a static key pattern (used in Original Vigenere Cipher model) we are using a dynamic key pattern by shifting the key matrix n number of times for m rounds.

In this model the plain text is modified into the cipher text by adding some value in each round and then the obtained value is added 32 X 32(1024) times with different key values. After every round of 1024 modification key pattern is changed by matrix shifting and again the same process is repeated. The key matrix is generated using the Vigenere table technique.

In the proposed model the encryption work is performed by:

CI = (P I + K I) mod 256

And decryption is performed

PI = (C I - K I) mod 256

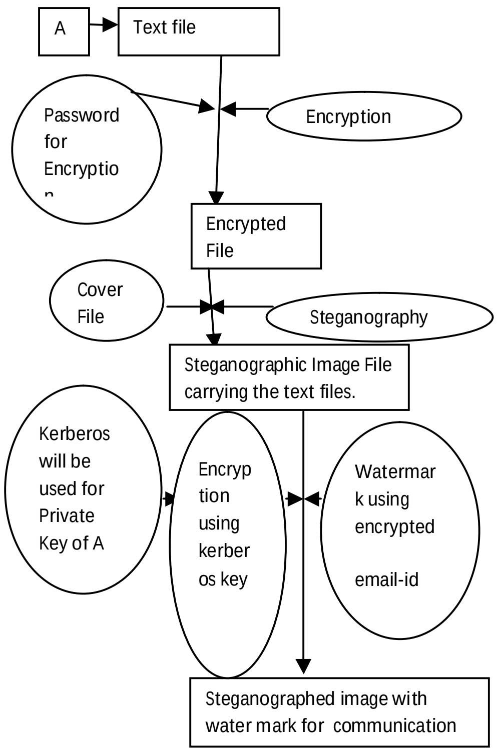
This model gives birth to a symmetric key algorithm and is not easily available for cracking. The proposed algorithm works for 1024 bytes of data and can be extended into multiple folds of 1024 bytes for a big size of data.

6.3 Process for Steganography

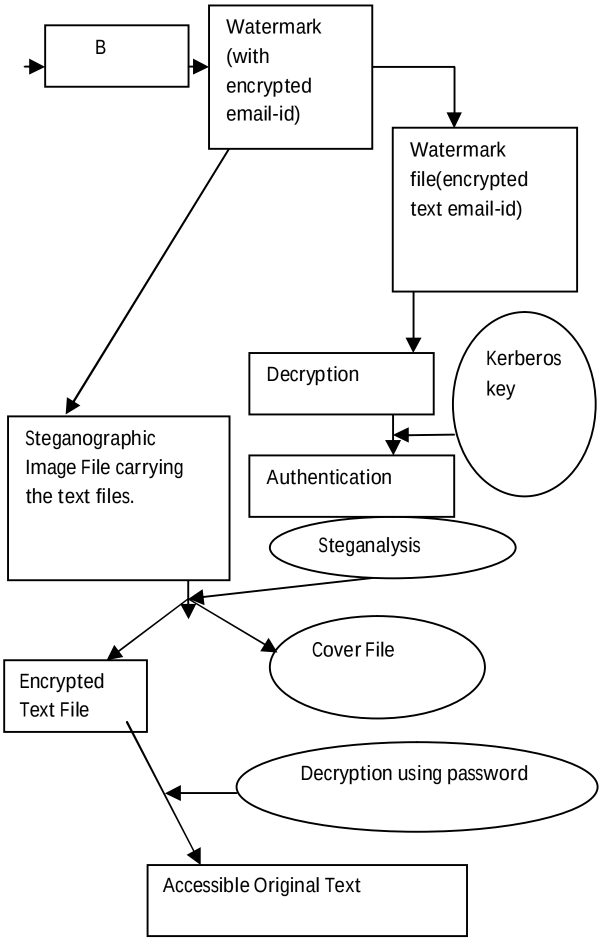
In this model Steganography is performed using image file as a cover and text file as a secret file. The text file is first encrypted using RDA algorithm & then using LSB technique it is embedded into the cover file. The same process is followed in reverse order on the receiver end.

7. THE COMPLETE DIAGRAM

7.1Embedding Process


A
Text file
Password for Encryptio n
Encryption
Encrypted File
Cover File
Steganography
Steganographic Image File carrying the text files.
Kerberos will be used for Private Key of A
Encryp tion using kerber os key
Watermar k using encrypted email-id
Steganographed image with water mark for communication

7.2 Extraction Process


B
Watermark (with encrypted email-id)
Watermark file(encrypted text email-id)
Decryption
Kerberos key
Authentication
Steganographic Image File carrying the text files.
Steganalysis
Cover File
Encrypted Text File
Decryption using password
Accessible Original Text

8. CONCLUSION

As discussed in the above paper Steganography has a great history and has been used in different ways in day to day life to the core technical world.

Symmetric key Cryptography has been in use for last few yeas but the basic drawback of the same was that the transaction of keys every time a message is communicated across the users, this makes the system quite vulnerable and thus the level of security though it is 2-tier is not that reliable. In this paper a tool has been explored which is used for Steganography and at the same time uses the symmetric key algorithm for the encryption of the message before the message is being embedded into the cover file(image) using LSB technique.

In this paper the watermark with Kerberos is used for the authentication purpose in which asymmetric key cryptography is used to modify the watermark.

9. REFERENCES

1. Katzenbeisser, S., Petitcolas, F.A.P., Information hiding techniques for Steganography and digital watermarking, Artech House Publishers, 2000.

2. Gnanaguruparan, M., “Recursive secret sharing in visual cryptography”, MS thesis, Louisiana State University.

3. Shoemaker, C., “Hidden bits: A survey of techniques for digital watermarking”, Independent study, EER 290, spring 2002.

4. Johnson, N.F., Jajodia, S., and Duric, Z., Information hiding: Steganography and watermarking attacks and countermeasures, Kluwer academic Publishers, 2000.

5. Wang, Y., Doherty, J.F., and Van Dyck, R.E., “A watermarking algorithm for fingerprinting Intelligence images”, Conference on Information Science and Systems, The John Hopkins University, March 21-23, 2001.

6. Kutter, M., and Hartung, F., Introduction to watermarking techniques – Information technology for steganography and digital watermarking, Artec House, 2000.

7. I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “A secure, robust watermark for multimedia,” in Information Hiding: First Int. Workshop Proc. (R. Anderson, ed.), vol. 1174 of Lecture Notes in Computer Science, pp. 185–206, Springer-Verlag, 1996.

8. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol. 35, no. 3/4, pp. 313–336, 1996.

9. Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. Attacks on copyright marking systems. In *Second workshop on information hiding*, pages 218-238, 1998.

10. Brassil, J. Low, S. Maxemchu, N., and O’Gorman, L., “Electronic marking and identification techniques to discourage document copying”. Proceedings of IEEE INFOCOM’94, 1994 3, pp.1278-1287

11. Matt L. Miller, Ingemar J. Cox, Jean-Paul M.G. Linnartz, Ton Kalker, A review of watermarking principles“. Published in “Digital Signal Processing in Multimedia Systems”, Ed. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 461-485, (1999)

12. http://www.digimarc.com

13.http://watermarkingportal.ipsi.fraunhofer.de/

14.Mustak e. Yalcin and Joos Vandewalle “fragile watermarking and unkeyed hash function implementation for image authentication on cnn-um”.

15. Dinesh Goyal, S.Bhargava “Authenticated Crypto Steganographic System”.

16. **http://www.watermarkingworld.org**

17. **http://www.research.ibm.com/image_apps**

18. **http://www.securitydocs.com/library/3461**

19. **http://www.dlib.org/dlib/june01/iannella/**