Vol III Issue VI July 2013
Impact Factor : 0.2105
ISSN No : 2230-7850

Monthly Multidisciplinary
Research Journal

Indian Streams Research Journal

IMPACT FACTOR : 0.2105

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Indian Streams Research Journal
ISSN 2230-7850
Volume-3, Issue-6, July-2013

Steganography – A Scientific approach to Hide Data within data to provide data security

M.Vijaya Kumar
HEAD OF THE DEPARTMENT, Department of Computer Engineering
Department of Technical Education, Govt of Andhra Pradesh, INDIA.

Abstract: Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art of inconspicuously hiding data within data. The main goal of steganography is to hide information well. In other words Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files . The aim is to conceal the very existence of the embedded data .In today's world the art of sending & displaying the hidden information especially in public places, has received more attention and faced many challenges. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography.

It is well known that encryption provides secure channels for communicating entities. However, due to lack of covertness on these channels, an unauthorized user can easily identify encrypted streams through statistical tests and capture them for further cryptanalysis. In cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Most steganography jobs have been carried out on images, video clips ,texts, music and sounds.

Therefore, different methods have been proposed so far for hiding information in different cover media. This method can be used for displaying a secret message in public domains which are accessed by any body.

Keyword: Stego file, private marking system, billboard display, Digital image steganography; spatial domain; frequency domain; adaptive steganography, security.

INTRODUCTION:

1.1 Ancient Steganography

The word steganography is originally derived from Greek words which mean "Covered Writing". Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text.

1.2 Nomenclature

The term "cover image" will be used throughout this paper to describe the image designated to carry the embedded bits. We will be referring to an image with embedded data, called herein payload, as "stego-image". Further "steganalysis" or "attacks" refer to different image processing and statistical analysis approaches that aim to break or attack steganography algorithms.

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used.The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. Nowadays, using a combination of steganography and the other methods, information security has improved considerably. Steganography can also be used in copyright, preventing e-document forging etc applications.

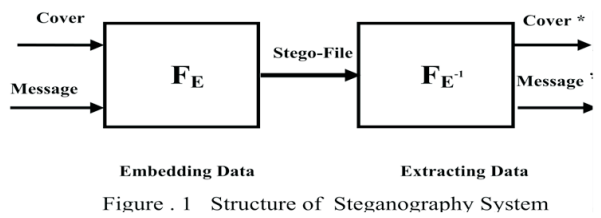


Figure . 1 Structure of Steganography System

Having produced the stego object, it will then be sent off via some communications channel, such as email, to the intended recipient for decoding. The recipient must decode the stego object in order for them to view the secret information. The decoding process is simply the reverse of the encoding process. It is the extraction of secret data from a stego object. In the decoding process, the stego object is fed in to the system. The public or private key that can decode the original key that is used inside the encoding process is also needed so that the secret information can be decoded. After the decoding process is completed, the secret information embedded in the stego object can then be extracted and viewed.

In steganography the Image can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words. Three techniques steganography, watermarking and cryptography are

interlinked, The first two are quite difficult to tease apart especially for those coming from different disciplines.

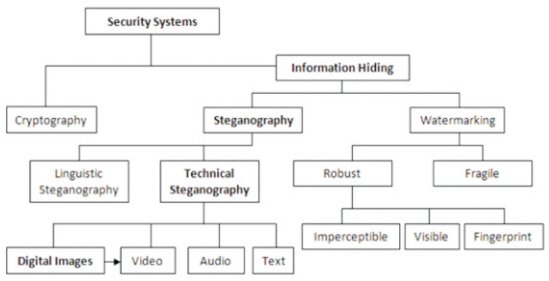


Fig. 1. The different embodiment disciplines of information hiding. The arrow indicates an extension and bold face indicates the focus of this study.

Table 1. Comparison of steganography, watermarking and encryption.

Criterion/Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload	watermark	plain text
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	blind	usually informative (i.e., original cover or watermark is needed for recovery)	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	robustness	robustness
Type of attacks	steganalysis	image processing	cryptanalysis
Visibility	never	sometimes (see Fig. 2)	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

The main goal of this method is to hide information on the output image of the instrument (such as image displayed by an electronic advertising billboard). This method can be used for announcing a secret message in a public place. In general, this method is a kind of steganography, but it is done in real time on the output of a device such as electronic billboard. Following are the steps involved in embedding the secret information within a cover media.

a) Send the normal data that has to be displayed to the display board.
b) Using a suitable Steganography algorithm hide the secret data within the normal data before sending it to the display board. This method can be used for announcing a secret message in public place. It can be extended to other means such as electronic advertising board around sports stadium.

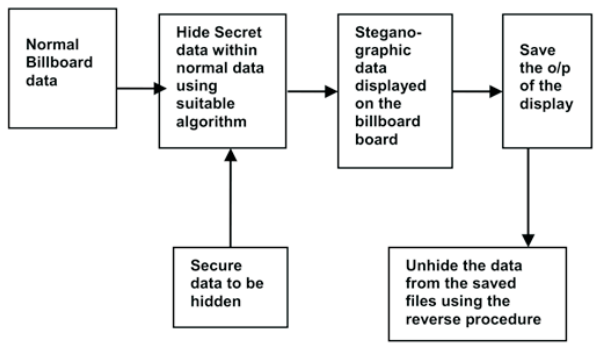
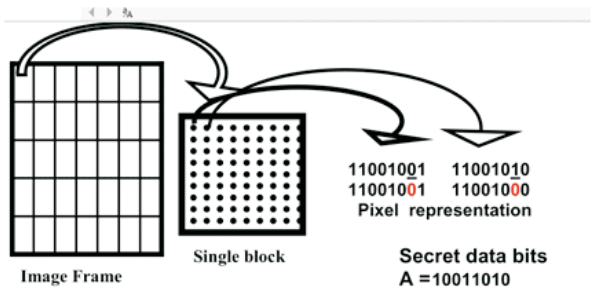


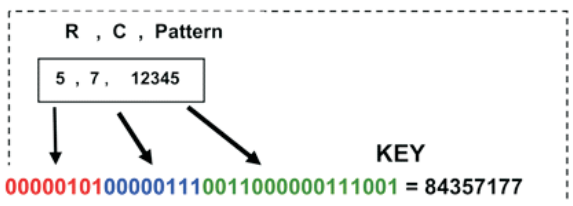
Figure 2 Block diagram of the proposed idea

Description of the algorithm for embedding the secret message:

Algorithm for embedding the secret message is as follows:

a) Read the image from the source.
b) Divide the image into [R x C] smaller blocks .Where R &C are the first & second bytes of the key respectively
c)Each smaller block is a combination of many pixels of different values.
d) The LSBs of the pixel are changed depending on the pattern bits and the secret message bits.
e)The pattern bits are considered in sequence form its MSB.
f)If the pattern bit is 0, then the first LSB of the pixel is changed [i.e if data bit is 1 and pixel bit is 0 then pixel bit is changed to1 or else it is retained as it is.]





g) If the pattern bit is 1, then the second LSB of the pixel is changed accordingly.
h) A single bit of the secret message is distributed through out the block. This is done to have enough information so that correct information can be retrived after decoding
i)Similarly the other bits are inserted in the remaining blocks.
j)If the length of the secret message is large , then it can be divided and stored in two or three frames.

k) To extract the information, operations contrary to the ones carried out in embedding are performed. The key plays a very important in embedding the message. Larger the key size, the more difficult to suspect the secrecy.

The figure above shows how the key is generated. The first 8 bits in red colour represent the no. of rows R & the next 8 bits in blue color represents the no. of columns C. The 16 bits in green followed by row and column represent the pattern bits. Each whole block of the cover image includes only one bit of the secret data. This is done so that more amounts of data is available During retrieval.

2.STEGANOGRAPHY APPLICATIONS

Steganography is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [1], and also checksum embedding [15]. Petitcolas [16] demonstrated some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient's information in the image could be a useful safety measure and helps in solving such problems. Steganography would provide an ultimate guarantee of authentication that no other security tool may ensure data hiding.

5. Fujitsu exploitation of steganography: (a) a sketch representing the concept and (b) the idea deployed into a mobil

CONCLUSIONS AND SUMMARY

This paper presented a background discussion steganofraphy, its methodology and applicationons. stganography deployed in digital imaging. The emerging techniques such as DCT, DWT and Adaptive steganograsphy are not too prone to attacks, especially when the hidden message is small. This is because they alter coefficients in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. There are different ways to reduce the bits needed to encode a hidden message. Apparent methods can be compression or correlated steganography.

Steganography methods usually struggle with achieving a high embedding rate. As an alternative channel to images, video files have many excellent features for information hiding such as large capacity and good imperceptibility. The challenge, however, is to be able to embed into a group of images which are highly inter-correlated and often manipulated in a compressed form.

As steganography becomes more widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should becom

For a system to be considered robust it should have the following properties:

a) The quality of the media should not noticeably degrade upon addition of a secret data.
b) Secret data should be undetectable without secret knowledge, typically the key.
c) If multiple data are present they should not interfere with each other.
d) The secret data should survive attacks that don't degrade the perceived quality of the work.

This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties. Both steganography and cryptography can be oven into this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network .In addition, the proposed procedure is simple and easy to implement. Also, the developed system has many practical, personal and militaristic applications for both point-to-point and point-to-multi-point communications

REFERENCES

I] Mohammad Shirali-Shahreza , “A new method for real time steganography”, ICSP 2006 Proceedings of IEEE .
II] Yuk Ying Chung, fang Fei Xu , “Development of video watermarking for MPEG2 video” City university of Hong Kong ,IEEE 2006.
III] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", Signal Processing : Image Communication 20, 2005, pp. 624–642.
IV]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett,“Steganography and digital watermarking” School of Computer Science, The University of Birmingham. 2003.
www.cs.unibo.it/people/phdstudents/scacciag/home_files/teach/datahide.pdf.
V] Ravi shah , Abhinav Agraval & subramaniam Ganesham, “Frequency domain real time digital image watermarking “ Oakland university.
VI] C. Lu, J. Chen, H. M. Liao, and K. Fan, "Real-Time MPEG2 Video Watermarking in the VLC Domain", Proc.of 16th International Conference on Pattern Recognition, Vol. 2, 11-15 August 2002, pp. 552-555.

ISSN 2230-7850
Volume-3, Issue-6, July-2013

VII] J. Haitsma and T. Kalker, "A Watermarking Scheme for Digital Cinema",Proceedings of the IEEE International Conference on Image Processing, Vol. 2, 2001, pp. 487–489.
VIII] Christoph Busch ,Wolfgang Funk & Stephen Wolthusen ,"DigitalWatermarking from concepts to Real - Time Video applications", IEEE Computer graphics and applications 1999.
IX] Chen Ming ,Zhang Ru, Niu Xinxin,Yang Yixian, "Analysis of current steganography tools: Classification & features" ,Information security center,Beijing University.China.
X] S. Katzenbeisser, F.A.P. Petitcolas (Ed.), Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, ISBN 1-58053-035-4, 2000. Proceedings of 2001 International Conference on ImageProcessing, Thessaloniki, Greece, 2001, pp. 542–545.