International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 22, 2017 ISSN: 2348-6600
Reference ID: IJCS-262 PAGE NO: 1673-1677
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

A PRAGMATIC STUDY OF STEGANOGRAPHY- AN ART OF HIDING DATA

STEGANOGRAPHY- AN ART OF HIDING DATA

Dr. C.BHUVANESWARI
Assistant professor & Head, Department of computer science,
Thiruvalluvar University College of arts and science,
Thiruvennainallur
Bhuvana.csdept@gmail.com

S.DAISY FATIMA MARY
Lecturer, Department of computer science,
Thiruvalluvar University College of arts and science,
Thiruvennainallur
daisyfatima_mca@yahoo.co.in

Abstract – The art of sending and displaying the hidden information has especially received more attention and faced many challenges. Steganography deals with hiding the available communicated data in such a way that it remains confidential. Usually the data covered is achieved by the means of image, text, communication, voice or multimedia military communication, content for copyright, authentication and many other purposes. This paper deals with the complete overview of the steganography its requirements, various methods of the steganography, its classifications and the various techniques used in the study. Finally the applications of the steganography are discussed in this work

Index Terms - Authentication, Copyright, Communication, Information, Multimedia.

I. INTRODUCTION (HEADING 1)

Steganography is a study of invisible communication and it is art of hiding communication that embeds hidden content in unremarkable cover media that can be viewed by the sender and intended recipient only. The greek word steganography is means "concealed writing" steganos meaning "covered or protected", graphei meaning "writing" which was first used by Johannes Trithemius in 1499.

The steganography has higher level of confidentiality, integrity, non removability than encryption and digital signatures.

II. LITERATURE REVIEW

The method of steganography is among the methods that have received attention in recent

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 22, 2017 ISSN: 2348-6600
Reference ID: IJCS-262 PAGE NO: 1673-1677
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

years. [1]There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly [2]. LSB matching revisited image steganography and edge adaptive scheme are proposed which can select the embedding regions according to the size of secret message For large embedding rates, smooth edge regions are used while for lower embedding rate, sharper regions are used.[3]Supervised learning is an effective and universal approach to cope with the twin difficulties of unknown image statistics and unknown steganographic codes. [4]

III. TYPES OF STEGANOGRAPHY

Steganography can be split into two types, these are Fragile and Robust.

a) Fragile : This steganography involves embedding information into a file which is destroyed if the file is modified.

b) Robust: Robust marking aims to embed information into a file which cannot easily be destroyed.

There are two main types of robust marking.

➢ Fingerprinting: involves hiding a unique identifier, fingerprints are used to identify people who violate the license agreement watermarks help with prosecuting those who have an illegal copy

➢ Watermarks are typically hidden to prevent their detection and removal, visible watermarks can be used and often take the form of a visual pattern overlaid on an image.

- Digital watermarking: Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove.
- Visible Watermarking: The information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the media.
- Invisible Watermarking: The information is added as digital data to audio, picture or video, but it cannot be perceived as such.

A. STEGANOGRAPHIC TECHNIQUES

a)Binary File Techniques

This method is very simple but is not resistant to attacks. If the attacker has many different versions of the marked files then he may detect the watermark and hence be able to remove it.

b) Text Techniques

The key is that the documents altered in a way that it is not visible to the human eye yet it is possible to decode it by computer.

c) Line Shift Coding Protocol

In line shift coding, we simply shift various lines inside the document up or down by a small fraction (such as 1/300th of an inch) according to the codebook. The shifted lines are undetectable by humans because it is only a small fraction but is detectable when the computer measures the distances between each of the lines.

d) Word Shift Coding Protocol

The word shift coding protocol is based on the same principle as the line shift coding protocol. It shift words left or right that is the justification of the document.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 22, 2017 ISSN: 2348-6600
Reference ID: IJCS-262 PAGE NO: 1673-1677
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

e) Feature Coding Protocol

The document is passed through a parser where it examines the document and it automatically builds a codebook specific to that document.

f)White Space Manipulation

One way of hiding data in text is to use white space. This is done by adding a certain amount of white space to the end of lines. The amount of white space corresponds to a certain bit value.

g)Text Content

It is possible to change sentences to store information, keep the original meaning and seems to be inconspicuous text.

IV. TYPES OF STEGANOGRAPHY

A. STEGANOGRAPHIC METHODS

- Image Hiding – Least Significant Bit Hiding (LSB):

  This method works by using the least significant bits of each pixel in one image to hide the information in the most significant bits of another. Consider the JPEG image for an example,

  1. First load up both the host image and the image that need to hide.
  2. Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates.
  3. A new image is formed by combining the pixels from both images.

  Example, to use 4 bits to hide the secret image, there will be four bits left for the host image.

  Host Pixel: 10110001 , Secret Pixel: 00111111 , New Image Pixel: 10110011

  4. To get the original image back, scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

  Host Pixel: 10110011 , Bits used: 4 , New Image: 00110000.

Fig: Least significant bit hiding

- Direct Cosine Transformation:

  The DCT algorithm is one of the main components of the JPEG compression technique. This works as follows :

  1. First the image is split up into 8 x 8 squares.
  2. Next each of these squares is transformed via a DCT, which outputs a multi dimensional array of 63 coefficients.
  3. A quantizer rounds each of these coefficients, which essentially is the compression stage as this is where data is lost.
  4. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 22, 2017 ISSN: 2348-6600
Reference ID: IJCS-262 PAGE NO: 1673-1677
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

5. An array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar.
6. Decompression is done via an inverse DCT.

- Wavelet Transformation :
  Wavelet transformations on the other hand are far better at high compression levels and thus increase the level of robustness of the information that is hidden, something which is essential in an area like watermarking. This technique works by taking many wavelets to encode a whole image.
- Sound:
  Encode data as a binary sequence which sounds like noise but which can be recognized by a receiver with the correct key.
- Video:
  For video, a combination of sound and image techniques can be used.

B.STEGANOGRAPHIC PROTOCOLS:

There are basically three types of steganographic protocols used. They are:

Pure Steganography is defined as a stenographic system that does not require the exchange of a cipher such as a stego-key. This method is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message.

Secret Key Steganography is defined as a stegnographic system that requires the exchange of a secret key (stego-key) prior to communication. It takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message.

Public Key Steganography is defined as a steganographic system that uses a public key and a private key to secure the communication between the parties wanting to communicate secretly. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology.

C.APPLICATIONS OF STEGANOGRAPHY

Steganography is applicable to, but not limited to, the following areas.

1. Confidential communication and secret data storing
2. Protection of data alteration
3. Access control system for digital content distribution
4. Media Database system

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
  It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source.
- Steganography can also be used to implement watermarking.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 22, 2017 ISSN: 2348-6600
Reference ID: IJCS-262 PAGE NO: 1673-1677
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges.
- The transportation of sensitive data is another key use of steganography.

V. CONCLUSION

This work presents the complete overview of the steganography, the classification its types, different kinds of steganography methods are discussed in detail with appropriate examples. The stegenography being the emerged field lot of the research work is going on in the field of transferring the data from one place to another. With the advent and the expansion of the techniques in this field a lot of achievements can be made to transfer the data securely in all the fields..

REFERENCES

[1] Mohammad Shirali-Shahreza , "A new method for real time steganography", Proceedings of IEEE, ICSP 2006 .

[2]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "Steganography and digital watermarking" School of Computer Science, The University of Birmingham. 2003.

[3] J.C.Judge, F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn" Steganography: past, present, future Informatics", SANS Institute publication, 2001.

[4] Jan Kodovsky and J. Fridrich, Influence of embedding strategies on security of steganographic methods in the jpeg domain, Proc. of IST/SPIE Electronic Imaging: Security, Forensics, Steganography Contents X, vol. 6819, pp. 1-13, 2008.

[5] M.H. Shirali-Shahreza and M. Shirali-Shahreza. Text steganography in chat. In Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Interne the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.

[6] Chen Ming ,Zhang Ru, Niu Xinxin,Yang Yixian, "Analysis of current steganography tools: Classification & features" ,Information security center, Beijing University.China,2014 .

[7] 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 Image Processing, Thessaloniki, Greece, 2001, pp. 542–545.