P: ISSN NO.: 2394-0344 RNI No.UPBIL/2016/67980 VOL-3* ISSUE-12* (Part-2) March- 2019
E: ISSN NO.: 2455-0817 *Remarking An Analisation*

A Data Security Approach Based on Steganography

Sumeet Kaur
Research Scholar,
Dept. of Comp. Engg.,
IKGPTU,
Kapurthala, India

Savina Bansal
Professor,
Dept. of E.C.
GZSCET,
Bathinda, Punjab, India

Rakesh Kumar Bansal
Professor,
Dept. of E.C.
GZSCET,
Bathinda, Punjab,India

Abstract

Information is wealth of any organization and to protect this wealth, information security has become top priority for any organizations. Whatever we choose for the security purpose, the burning issue remains the degree of security. With the advent and growth of internet and e-commerce, information is more prone to theft and misuse during transmission and there arises the need to protect the information. Steganography can be used to transmit the information in such a way that the presence of secret information cannot be detected. For security purpose steganography can be used as beneficial tool that has gained immense importance in present scenario. The main problem with steganography methods is the requirement of special data embedding methods of high capacity, transparency & robustness. Steganography has vast no of applications in different areas like authentication, financial transactions, credit cards codes, personal IDs, digital content copyrights, safe circulation of secret data, TV broadcasting, medical field etc. Steganalysis deals with breaking steganography and detecting the hidden contents. With the requirement of sophisticated steganography techniques for security, purpose there is also need to understand and develop powerful steganalysis techniques. This paper focuses on steganography and steganalysis concepts and gives overview of commonly used techniques. This paper also highlights various issues & challenges that steganography is facing currently, which may provide directions for future research.

Keywords: Steganography, Information, Security, Steganalysis.

Introduction

Steganography is an art and science of hiding a secret message in a cover medium in such a way that only receiver knows about its existence therefore Steganography is also known as 'Covered Writing' [13]. This can be achieved by concealing the existence of information within seemingly harmless carrier or cover object.

Digital media is main source of flow of information now a day. With the development of internet, digital media can be conveniently transmitted over internet and with access of internets to everyone; it became possible and easier to copy and to distribute the digital information illegally [14]. Digital media can be used to transmit secret and confidential data for personal, business or legal purposes. To keep secrecy of data has become an important issue and steganography techniques offer a very reliable solution for such problems. Steganography techniques tend to hide the very presence of the message itself from an observer thus there is no knowledge of the existence of the message in the first place. Goal of steganography is different from cryptography. Sending encrypted information will arouse suspicion whereas Steganography will not do so. Steganography involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. Most basic method of steganography is to utilize the existence of redundant information in a communication process. Images, audio and video files contain such redundancies. Purpose of using steganography is to achieve security and privacy by masking the very presence of communication [21]. Thus steganography provides an ultimate reliability and authenticity that no other security tool can provide [16]. Steganography is being used from ancient times, Simmons stated the

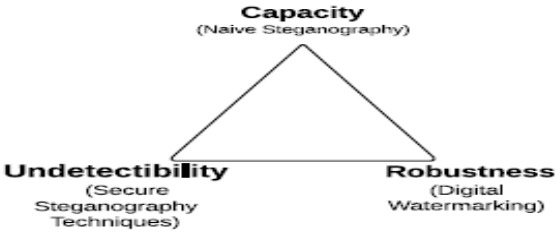
problem in terms of communication in a prison that is also commonly known to as **'Prison's Problem'** [6]. In 1985, cocept of modern Steganography came with the development of personal computers. Where Digital Steganography came into existence with the development of internet.

Each steganographic communication system makes the use of an embedding algorithm and stego key to embed the secret message into cover object, which is slightly modified to get stego object. Extraction process is used to extract secret message back from stego object by use of reverse embedding algorithm and stego key [20]. When Data hiding is parameterized by a key; it is difficult for a third party to detect or remove hidden message without knowledge of this key. Here steganography is similar to Kerckhoff's Principle in cryptography [1], which states that a cryptographic system of security should depend solely on the encryption key. For steganography to remain undetected, the unmodified cover medium must be kept secret, if it is exposed, a comparison between the cover and stego media can immediately expose the changes.

Requirements for a Steganography Algorithm

Steganography algorithm should have characteristics of robustness, capacity and undetectibility. It is difficult to have all the characteristics at fullest and generally, there is trade-off between these characteristics.

Fig 1: Showing tradeoff between Capacity, Invisibility and Robustness [28]



Capacity

The amount of data that can be hidden in cover medium without significantly changing the cover medium and can be retrieved latter successfully.

Undetectibility

It means embedded message should not be visible to human eye. Human being should be unable to distinguish between cover and stego object.

Robustness

Robustness refers to the degree of difficulty to a steganalyst to determine whether the image contains a hidden message. A stego system is said to be robust if it can bear any attack and remain intact if it undergoes transformation such as scaling, rotation, filtering and loosy compression etc.

Security

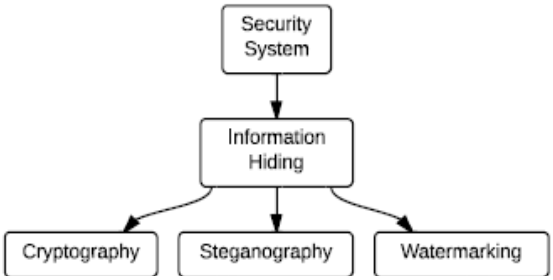
An embedding algorithm is said to be secure if the embedded information could not be removed by the attacker after detection. It depends on the total information about the embedded algorithm and secret key. A good implementation of steganography is that in which stego object can be subjected to many attacks that each proves inconclusive.

If we embed less information in a cover image then there will be lesser probability of introducing detectable artifacts by embedding process [22]. The primary goal of steganography techniques has been to maximize embedding rate and minimizing the detectability of the resulting stego images against steganalysis techniques [15].

2.1 Various Data Hiding Techniques

Data hiding has become increasingly important for various applications like confidential transmission, video surveillance; military and medical applications [18], the knowledge of data hiding can be used either in ethical or unethical ways. Data hiding algorithms cannot easily be categorized either in steganography or watermarking categories as there is no transparent boundary between these two and mostly the classification relies on application of the algorithm.

Fig 2: Various Data Hiding Disciplines



Cryptography, Steganography & Watermarking

Three techniques that are interlinked and related to security are steganography, watermarking and cryptography. Techniques for concealing meta-information about a message, such as its existence, duration, sender and receivers are collectively known as traffic security. Steganography is often considered to be a proper subset of this discipline rather than being its co-extensive [2].

Steganography vs. Cryptography

The purpose of cryptography and steganography is to make secret communication. Steganography is about concealing their very existence. Cryptography scrambles a message so that it cannot be understood. If steganography and Cryptography are used in combined form, then it becomes even more secure. The rigorous study of secure cryptography was initiated by Shannon [5], who introduced an information-theoretic definition of security.

Steganography vs. Watermarking

Steganography is similar to watermarking but have a different purpose and different applications. Steganography aims at concealing the existence of a message with high data capacity, watermarking mainly focuses on the robustness of embedded message rather than capacity or concealment. Since increasing capacity and robustness at the same time is not possible. Watermarking can be used for copyright protection and tracking legitimate use of a particular software or media file and also provide a way of tracking the owners of these materials [23].

Although it is not easy to classify different steganography methods, acc to R. Chandramouli it is big challenge and question that- "Can the current and

future steganography algorithms be categorized into distinct classes of mathematical techniques?"[19], because each method makes use of a different approach.

2.2 Steganography Types

Pure steganography

Pure steganography system requires only knowledge of embedding scheme. There is no exchange of key between communicating parties to start the process. It is one of simplest system because security of system depends entirely on its secrecy but pure steganography does not provide any security if attacker knows embedding algorithm in some way.

Private/ secret key steganography

A secret key Steganography system is similar to a symmetric Cryptography. Here sender embeds the secret message into the cover using a secret key. Here secret key is exchanged and used by receiver to extract secret message. Strength of system depends upon secrecy of key because anyone who doesn't know the secret key would not be able to obtain evidence of the encoded information.

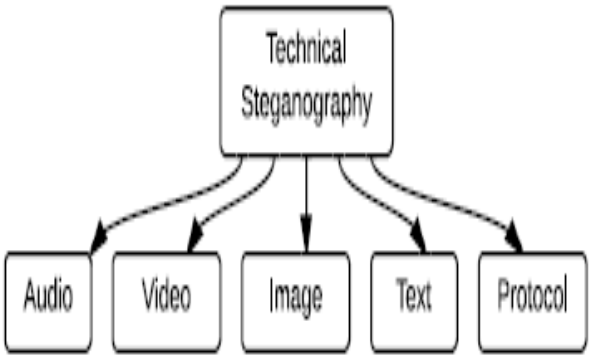
Public Steganography

It requires two keys, one of them is private (secret) and other is public. Public key is used to perform embedding process and available publically where secret key is used to extract message.

2.3 Steganography and type of Cover Objects

We can use different types of cover objects like text, image, audio and video to hide secret data.

Fig 3: Different Types of Cover Objects Used For Steganography



Text Steganography

It is one of the earliest and most difficult types of steganography. It is a method of using written natural language to conceal a secret message. Text steganography is most challenging due to the presence of lesser redundancy in text documents as compared to the images and audio files [9].

Image Steganography

In this secret message is embedded into an image. Image steganography is the most popular. Secret message is hidden into an image as noise, which is nearly impossible to differentiate by human eyes. Data hiding in still images imposes certain challenges to cope up with human visual systems (HVS)]. Further still image are subjected to various operations like ranging from simple to nonlinear transformation such as cropping, blurring, filtering and lossy compression etc. Data hiding method should be resistant to these types of transformations [10]. Images are most popular and widely used medium for steganography

Audio Steganography

Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range. Embedding secret messages in digital sound is generally more difficult than embedding messages in other media, Sensitivity to additive random noise is also acute [10]. Methods that are commonly used for audio Steganography are: LSB coding, parity coding, phase coding, spread spectrum, and echo hiding.

Video Steganography

It pertains to hide information in video files which are generally collection of sound and images. Steganography methods which are applicable to sound and images are also applicable to video files. Advantage of this method is that large amount of data can be hidden inside video with smaller amount of distortion because of continuous flow of information and that might go unobserved by observer [23].

Protocol Steganography

It pertains to hiding information in unused or optional fields of network control protocols used in transmission over a network [7]. In the layers of the OSI network model there exist covert channels where steganography can be used [8]. Information can also be hidden in the header of a TCP/IP packet in some fields that are either optional or are never used. Advantage of hiding information in header is that some fields are rarely read by humans and serve as ideal place for hiding but disadvantage is that when firewalls may be configured for safety purpose to filter out packet where reserved fields contain unusual information then hidden information may lose [12].

Image steganography is more commonly used. Here we have considered some commonly used techniques for image steganography.

2.4 Image Steganography Techniques

Spatial Domain Techniques

Spatial domain techniques embed message in the intensity of the original image pixels directly. Spatial domain techniques include bit-wise methods that apply bit insertion & noise manipulation. There are various approaches to embed data in spatial domain. Most Commonly used approaches under spatial domain for hiding secret message are least significant bit approaches.

Transform Domain Techniques

Transform domain techniques first convert image from spatial domain to frequency domain then message is embedded. These techniques hide data in mathematical functions that are often used in compression algorithms. Secret data will be embedded into transform coefficients which are transformed first into frequency domain by various frequency domain methods like discrete cosine transformation (DCT), discrete wavelet transforms (DWT), or Discrete Fourier transforms (DFT [9].

DCT

Most commonly used transformation domain technique is DCT (Discrete Cosine transformation). It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into

high, middle and low frequency components. Embedding in DCT domain is simply done by altering the DCT coefficients. DCT transformation and compression using quantization and run-length coding on raw images can be used to obtain secure stego images. DCT is a lossy compression transform because its cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into final results. Variances between original data values and restored data values depend on the method used to calculate DCT [25]

Embedding Methods

Some of commonly used embedding algorithms for image steganography are considered here:

Least Significant Bit Method (LSB)

It replaces least significant bits of cover object with message to be embedded. It is most popular and simple technique when dealing with images. It has low computational complexity and high embedding capacity [24]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB. Although it is very simple technique but it is susceptible to lossy compression and image manipulation such as scaling, rotation, cropping etc, and addition of noise or lossy compression to the stego-image will destroy the message. It works best when the image file is larger than the message file and if the image is grayscale and with gradual changes in shades.

Spread Spectrum

This technique is based on spread spectrum communication that is spreading the bandwidth of a narrowband signal. In spread spectrum steganography secret message is embedded in noise then combined with cover image to generate stego image and power of embedded signal is much lower than cover image and stego image is not perceptible to HVS [26][27].

Masking

This technique masks secret data over original data by changing the luminance of particular areas. It embeds the message within significant bits of the cover image. Unlike LSB; masking is not susceptible to lossy techniques because image manipulation does not affect the secret message because masking adds redundancy to the hidden information. This makes the masking technique more suitable than LSB with lossy JPEG images. It may also help to protect against some image processing operations such as cropping and rotating.

Statistical

Here hiding and extracting the data are based on certain statistical properties of cover. It uses existence of “1bit” steganography and modifies cover in such way that if a“1” is transferred by changing certain statistical properties of cover otherwise cover remains unchanged [30].

Distortion

Here secret message is embedded by distortion of cover and measuring deviation between original cover and stegos at decoding stage. Distortion techniques are less secure and are not used in various applications because original cover object may available to steganalyst for comparison. Text based steganography techniques generally use distortion type for embedding [30]

Cover Generation Methods

As the name indicates here secret message is encoded in such a way that a cover is generated [30].

2.5 Different type of Image file formats and Steganography

While working with steganography, it is very important to understand the compression and type of compression used in cover object. Image compression is a good solution to use large image to hide secret information and then transmit it over the internet. Most commonly used image format on internet are Graphic Interchange Format (GIF), Joint Photographic Expert Group (JPEG), and to lesser extent – the Portable Network Graphics (PNG). Most of the steganography techniques exploit these image formats and some of the techniques are also based on Bitmap format (BMP) [16]. Uncompressed formats (GIF &BMP) are more convenient for data hiding algorithms, because their size is more than any other format on the internet. Majority of image data hiding techniques use uncompressed formats because potentially they have much visual redundancy and are able to accommodate higher volume of secret data. Most common format found on the Internet is GIF files. Neil F. Johnson and Sushil Jajodia observed that steganographic systems for palette-based images leave easily detected distortions [4]. Many steganography experts recommend using images featuring 256 shades of gray. Gray-scale images are preferred because the shades change very gradually from byte to byte, and lesser the value changes between palette entries, the better we can hide information [25]. While gray-scale images may render the best results for steganography, images with subtle color variations are also highly effective. EZ Stego is one of the most popular data hiding schemes for palette-based images.

Earlier it was believed that steganography could not be used with JPEG images due to loosy compression and their compression algorithm does not support a direct LSB embedding into spatial domain [16], but now, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and not affected by visual attacks [3]. JPEG image use DCT to achieve compression. Jsteg was the first steganographic algorithm for JPEG images developed in 1993 by D Upham. Major JPEG Steganographic methods are: JP Hide/ Jsteg, F5, Outguess, YASS etc.

3.1 Steganalysis and Its Significance

Steganalysis is the science and art of attacking Steganography. Purpose of Steganalysis is to detect steganography by deciding whether an observed object is pure cover or stego object [33]. Modern steganography’s goal is to keep the presence of hidden message undetectable, but steganographic

systems leave behind certain detectable points in the cover medium. Even if secret content is not revealed, the existence of it is modifying the cover medium changes its statistical Properties, so attacker can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis [5]

Steganographer can create Steganalysis merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques e.g. image filtering, rotating, cropping, translating, etc. More deliberately steganalysis can check the stego image structure and measures its statistical properties e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, and direction). Apart from many other advantages higher order statistics, if taken into account before embedding, can improve the signal-to-noise ratio when dealing with Gaussian additive noise. In order to develop a good steganography algorithm, one should have knowledge about the different steganalysis techniques. By identifying the tools used to hide secret message, we can use the tools to extract the hidden secret message [29].

3.2 Classification of Steganalysis Techniques

Steganoanalysis methods can be classified based on type of attacks (i.e. Active and Passive attacks)

Active Steganoanalysis

Active steganoanalysis first detects the presence of hidden secret message and once the message is detected then purpose of is to extract the secret message.

Passive Steganoanalysis

Here main purpose of steganoanalysis is just detecting whether secret information is present or not. If message is present then purpose is not extracting it. [31]

Steganoanalysis methods can also be classified based upon whether steganoanalysis algorithm is specific or general

Targeted Steganalysis

A targeted steganoanalysis is works on specific type of embedding algorithm and sometimes limited on specific image format. They are generally designed by studying specific characteristics of given embedding algorithm and image statistics that change after embedding. They are specific to one embedding algorithm not general one and hence these are more accurate.

Blind Steganalysis or Universal Steganalysis

A blind steganoanalysis technique is more general and works on all embedding algorithms. Blind steganalysis algorithm finds difference in statistical properties of pure and stego images by learning process and it is done by training the machine on large database. These algorithms are less accurate [32].

Steganoanalysis methods can be classified depending upon the type of technique used for steganoanalysis

Visual Steganoanalysis

Visual syteganoanalysis is based on comparing and analyzing original and cover object to inspect any difference or degradation that exist in color, quality or any other type of change that exist between original and stego image. It is one of simple type of technique but not effective because original image is generally is not available for comparison purpose.

Statistical Steganoanalysis

Steganography process generally changes the statistical properties of cover object which steganoanalyst may detect and process of attempting to detect change in statistical properties between cover and stego object are known to as statistical steganoanalysis [32]. One of the simplest statistical attacks is Chi-Squared test. This test makes it possible to compare statistical properties of suspected image with theoretical expected properties of its carrier to determine the likelihood that suspected image was stego programme. Chi-Squared test was used in steganography terms by Westfield and Andreas Pfitzmann [3].

There are various other steganalysis tools and techniques are also available based on different concepts and mathematical techniques like RS, gradient energy-flipping rate detection and histogram difference etc to check difference between cover object and stego object.

4.1 Metrices

Quality of a steganography algorithm can be evaluated with the help of various quality measuring parameters and some of commonly used parameters are considered here:

PSNR

Peak Signal to noise ratio is a measure used in to check the quality of stego images. It is often expressed on a logarithmic scale in decibels (dB), higher the values of PSNR more the quality of stego image. PSNR value falling below 30dB indicates a fairly low quality [16].

RMS

Root mean square error for stego image can be calculated and checked and smaller the value better is the embedding algorithm.

Histogram

To check any change in statistical properties of stego image after performing embedding we can compare histogram of original cover image and stego image.

Different metrics respond differently to different distortions Like mean square error responds more to additive noise spectral phase or mean square HVS-weighted error are more sensitive to blur gradient measure reacts more to distortions concentrated around edges and textures.

Other important performance evaluation measures for image steganography algorithm are capacity, bit error rate, entropy etc.

4.2 Factors Affecting the Strength of Steganographic Algorithm

Choice of cover object is an important factor for the security of a steganography algorithm. Some images are much better than others when used as a cover object. Cover objects with larger no of changeable coefficients will lead to smaller no of artifacts and hence lesser detectability is there as

result of embedding. Images with fewer numbers of colors, details, with computer arts and semantic contents should be avoided. Best choice can be uncompressed scans of photographs or images obtained with a digital camera and a high number of colors [15].

4.3 Challenges and Issues with Steganography

Steganography algorithms are facing different types of challenges and some of them are considered here:

1. Data hiding in still images poses various challenges like they provide less redundancy and Imperceptibility as compare to audio and video files [10][16].
2. Steganography algorithms generally struggle for providing high data rate and Imperceptibility. If a technique provides high payload capacity then it may be less robust and vice versa. Requirements for higher capacity and secure communication are often contradictory [10]. Depending upon the specific application this trade off needs to be sought out and at the same time there is also need to produce high quality stego algorithm by achieving high value of PSNR.
3. Other challenge is to embed into group images which are highly inter-correlated and often manipulated in compressed form [16] [17].
4. Steganographic techniques are very sensitive to various modification in cover medium like Image processing techniques (smoothing, filtering, image transformations etc), compression techniques, removing and filtering digital noise techniques because these techniques lead to removal or modifications of secret embed information too.
5. While designing a secure steganographic algorithm there is need to pay special attention to the presence of active and malicious attacks. Hidden message must be secure both from perceptual and statistical attacks.
6. Steganography has various useful applications but like other technologies it can also be miscued by criminals and terrorists for ill purposes. So there is need to understand all steganography as well as steganoanalysis concepts and practices

Conclusion

Steganography had been used widely in historical times and also being used currently for its various applications. It is an ongoing research area. The focus of this research paper is to understand image steganography, related concepts, commonly used embedding techniques for image steganography and also about steganalysis. There are different methods for hiding data, with their own pros and cons respectively. If a technique provides high payload capacity, it may be less robust and vice versa. Steganography can be used for secure and secret communication where cryptography methods are either not available or not allowed. For all the major image file formats (BMP, GIFF, TIFF, JPEG etc) uncompressed formats ((BMP, GIFF, TIFF) based on lossless compression are more convenient for data hiding algorithms and provides high data capacity. Lossless compression of images with great deal of colors variation work best as a cover image to embed a message, but on other hand working with JPEG images and using transform domain we can achieve more secure embedding because it cannot be detected visually. The technical challenges of data hiding are finding any “holes” to fill with data in a host signal, that cannot be statistically and perceptually attacked, and further embedded data is not removed by lossy signal compression.

Steganalysis is also gaining importance with the advent and growth of steganography. Steganography can be beneficial tool for privacy but one has to cautiously select a suitable cover medium with required file format, compression and particular embedding algorithm according to need of the application. Further one also has to decide about which characteristics have to be compromised in order to ensure high performance of other desirable characteristics.

End notes

1. *Kerckhoffs, “La Cryptographie Militaire (Military Cryptography),” J. Sciences Militaires (J. Military Science, in French), Feb. 1883.*
2. *R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography,” J. Selected Areas in Comm., vol. 16, no. 4, 1998 pp. 474–481.*

A. *Westfield and A. Pfitzmann, “Attacks on Steganographic Systems,” Proc. Information Hiding—3rd Int’l Workshop, Springer Verlag, 1999, pp. 61–76.*

3. *N.F. Johnson and S. Jajodia, “Steganalysis of Images Created Using Current Steganographic Software,” Proc. 2nd Int’l Workshop in Information Hiding, Springer-Verlag, 1998, pp. 273–289.*
4. *C.E. Shannon.’ Communication theory of secrecy systems’. In: Bell System Technical Journal, 28, (1949), Pages 656-715.*
5. *G.J. Simmons. The Prisoner's Problem and the Subliminal Channel. In: Proceedings of CRYPTO '83. 1984.*
6. *Ahsan, K. & Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.*
7. *Handel, T. & Sandford, M., “Hiding data in the OSI network model”, Proceedings of the 1st International Workshop on Information Hiding, June 1996*
8. *Lee, Y.K. & Chen, L.H., “High capacity image steganographic model”, Visual Image Signal Processing, 147:03, June 2000*
9. *Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, No. 3-4, pp 313-316, 1996.*
10. *Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001*
11. *Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001*
12. *P.salee , “Model–based Steganography”, in: proceeding of the 2nd International workshop on digital water marking, Seoul , Korea, October 20-22 2003 , LNCS , vol.2939, pp. 254-260.*
13. *Summrina Kanwal Wajid, M. Arfan Jaffar, Wajid Rasul, Anwar M. Mirza, 2009 International Conference on Machine Learning and Computing ,*

IPCSIT vol.3 (2011) IACSIT Press, Singapore , pp 385-391.

14. *M. Kharrazi, H.T. Sencar and N. Memon , "Cover Selection for Steganographic Embedding", IEEE International Conference on Image processing, 8-11 oct 2006, Atlanta USA, pp 117-120*
15. *Abbas chedad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Signal Processing, Vol 90, Issue 3, March 2010, page 727-752.*
16. *Z. Zhao, N. Yu, and X. Li, "A novel video watermarking scheme in compression domain based on fast motion estimation", in proceedings of IEEE International Conference on Communication Technology, 2003, pp. 1878-1882.*
17. *P. Amat, W. Puech, S. Druon, J.P. Pedeboy, " Lossless 3D Steganography based on MST and Connectivity modification", Signal Processing: Image communication 25(2010) Elsevier, pp 400-412.*
18. *Chandramouli, R. Mathematical approach to steganalysis. In: Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 14-25.*
19. *Fridrich, J. and Goljan, M. Practical steganalysis of digital images: State of the art. In: Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, 2002, pp. 1-13.*
20. *Fridrich, J. and Du, R. Secure steganographic methods for palette images. In: Proceedings of the 3rd Information Hiding Workshop, Lecture Notes in Computer Science, vol. 1768. Dresden, Germany, September 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 47-60*
21. *Jessica Fridrich, Miroslav Goljan, and Rui Du, "Detecting LSB Steganography in Color and Gray-Scale Images", IEEE Multimedia and Security, 2001, pp 22-28*
22. *Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at: ttp://www.krenn.nl/univ/cry/steg/article.pdf*
23. *R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.*
24. *Neil F. Johnson Sushil Jajodia, George Mason University, "Exploring Steganography: Seeing the Unseen Steganography", February 1998, IEEE, pp 26-34.*
25. *T. Morkel, J.h.p. eloff, M.S. Olivier "An overview of image Steganography" information and computer security architecture (icsa) research group.*
26. *Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE transactions on image processing, 8:08, 1999*
27. *J. Fridrich. "Applications of data hiding in digital images." Tutorial for the ISPACS'98 Conference, 1998.*
28. *Steganography, Stegananysis and Cryptanalysis by Michael T.Rago, Defcon 12, Aug 1, 2004.*
29. *Neil F. Johnson and Stefan C. Katzen Beisser, "Information hiding techniques for steganography and digital watermarking", pp 67-71.*
30. *Yeh-Shun Chen and Ran-Zan Wang, " Steganalysis of Reversible Contrast Mapping Watermarking", IEEE Signal Processing Letters, VOL. 16, NO. 2, Feb 2009, pp 125-128.*
31. *Siwei Lyu, Hany Farid, "Steganalysis Using Hiher-Order Image Statistics", IEEE Transitions On Information Forensics And Security, Vol 1, No. 1, March 2006. Pp 111-119.*
32. *Ismail Avcibas, Nasir Memonb, Biilent Sankur "Image Steganalysis With Binary Similarity Measures", IEEE ICIP 2002, pp III 645-648*
33. *Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001*