Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (2): 53-66, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.53.66

Steganography-Time to Time: A Review

Rengarajan Amirtharajan and J.B.B. Rayappan
Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Corresponding Author: Rengarajan Amirtharajan, Department of Electronics and Communication Engineering, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

ABSTRACT

It is time to wrap up the old stories of covert communication. As time goes by, we are updating in each and everything in what we do, want and utilize. Communication and technology are not exceptions. Although they go hand in hand, Internet aficionados often end up with security issues in the former directly or indirectly in touch with the latter. What has to be done? Increasing the security in whatever conveyed to the world online; for that emerging technologies (in our case with an ancient touch!) should be drawn into battle between the originators and mutilators! For efficient way of secret exchange of information, Cryptography and Steganography endow with a phenomenal contribution. The objective is to grant this as a study identifying the nuances of steganography in some notable grounds. This study does not fail to present the principles and attributes of steganography, traditional methods in the past, upcoming directions and also glances through detection mechanisms. Thus, this study gives the readers a good overview about Steganography.

Key words: Data security, data hiding, information hiding, steganography, steganalysis

INTRODUCTION

Information Security is a subfield of computing which stands for defending information from illicit entrée, scrutiny, amendment, commotion etc. (Schneier, 2007). Putting it simple it deals with the technologies to safeguard covert information from all sorts of hacking. Information Security can be broadly categorized as Network Security (Stallings, 2010a, b), Computer Security and Internet Security. Computer Security incorporates all the practices and means through which system-based paraphernalia, data and services are safeguarded from the premeditated or involuntary access of the third party. It embraces fortification not only from the above mentioned but also from impromptu actions, natural catastrophe etc.

While Network Security is a dedicated field concerning provisions and guidelines espoused by a network/system. It bureaucrat to shelter a network and the wherewithal accessed via the network from mistreat. Internet Security is a division coping with browser and application level security because this is the widely utilized medium which is also highly prone to scam. The three fundamental notions for information security are privacy, reliability and accessibility (Stallings, 2010a, b). That is, the users should be guaranteed that information is trusted to be shared, it should be shared only in the form they suppose. It should be obtainable when needed and of course it should be processed by the systems in time and in truthful conduct.

Let's roll back to know the brief history information security. It gets back to primeval times and begins with the egression of officialdom in organization and rivalry. Caesar took the pride of inventing Caesar cipher around 50 B.C. to foil his communication from being examined. Insightful information is communicated from source to destination via trusted people and is also stocked up in a protected milieu. Encoding the covert information was also in practice during the World War II (Stefan and Fabin, 2000).

The beginning of computer epoch witnessed brisk and speedy progression in providing security both in hardware and software level (Janakiraman *et al*., 2012a, b; Rajagopalan *et al*., 2012). The researches exploited mainframes to achieve the goal by rewiring and punch cards as there were no computer networks at that time. In 1960s, ARPANET project, the forerunner of internet, made the possibility of data storage and processing. Defense Department presented a study based on Security Controls known as R-609 in 1970s. Increased usage of PCS in 1980s demanded the enhanced security and GUIs to OSs drew hackers from nook and corner of the globe in 1990s. The unavailability of protection technologies leads to various forms of security theft in those days during which it was not fashionable concern.

As many techniques used from the ancient period up to recent times failed to pledge secret data communication, Cryptography (Salem *et al*., 2011; Schneier, 2007; Stallings, 2010a, b) and Steganography (Stefan and Fabin, 2000) came into light and blow the lid off. They have now become the unbeatable mode of communication of a secret from source to destination. While the former deals with text or numbers alone, the latter spreads its wings to all multimedia files (Cheddad *et al*., 2010; Zaidan *et al*., 2010). Cryptography initially eased the problem of one to one communication whereas Steganography endeavors peer to peer communication in a more sophisticated way.

The underlying principle in steganography is that the cloak-and-dagger information is communicated from the source to destination in disguise (Amirtharajan and Rayappan, 2012a-d; Alanazi *et al*., 2010). That is generally the receiver gets the desired message undercover. How it is so? The key elements involved for an indispensable steganographic scheme are the payload (Hmood *et al*., 2010b), cover, key, saving the best for last, the algorithm (Stefan and Fabin, 2000). Payload is what the private information to be conveyed, cover is the medium in which payload is entrenched, key, as it says, is the crucial index involved in the operation and finally the algorithm is the course of action we adopt to attain the goal. The simple classification in steganography is given in Fig. 1.

Simple yet most needed mottos of steganography will be the message should not be visible to any one (imperceptibility). Even to the receiver, when he/she does have a look at it, it should be

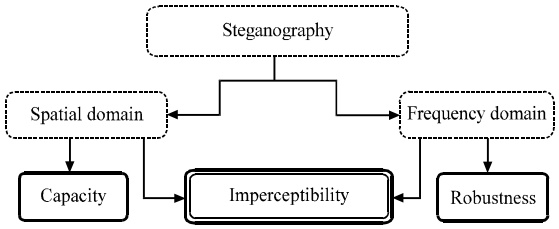

Fig. 1: Simple classification in types of steganograph

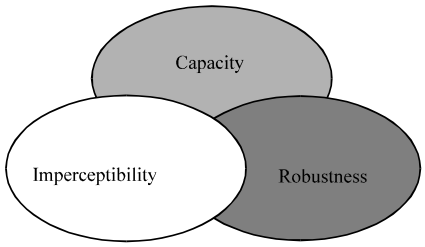

Fig. 2: Basic requirements of steganographic methods

incubus for everyone trying to retrieve (robustness) it. The technique should be put into service effortlessly, more of secret data should be able to infix and convey (capacity) (Amirtharajan and Balaguru, 2009, 2010; Amirtharajan *et al*., 2011; Hmood *et al*., 2010a; Qi *et al*., 2010; Thien and Lin, 2003). The basic requirements is given in Fig. 2.

The following sections throw a light in knowing the details of steganography. The history and current trends behind the routine, utilities of one, methodologies in practice, ways to crack a steganographic scheme (steganalysis) are discussed (Fridrich *et al*., 2001; Qin *et al*., 2009, 2010; Xia *et al*., 2009).

PAST

Greeks were more successful in conveying secret messages. Though their measures did not fall into the category of prompt cryptography, they were the initiatives for the later discovered. They also did not fail to use steganography; in fact the word is coined from the Greek language meant for hidden writing. For evidence, the archives date back to 440 B.C. They also conveyed the secret with the help of wax in woods! The messenger's body is tattooed with secret and sent over to the destination (Kahn, 1983).

In olden days, secret message is communicated to the recipient by placing a grille having holes in script of not detrimental text. This revealed the covert content within the holes. Invisible ink was used by Romans as a key to privacy using which the secret is written and becomes quickly invisible. The measures to later make visible the invisible are also noteworthy. It was a successful key to espionage. It was useful in stamping, marking properties, product identification and many more. Invisible ink is developed by means of heat, UV rays, chemical reaction etc. that could stand for its purpose (Petitcolas *et al*., 1999; Cheddad *et al*., 2010).

Another prominent means of steganography is usage of dots and microdots. England was known for this practice. Unlike Greeks, British used newspapers rather than harmless text to hide the message. This seemed safer with almost zero percentage for detection as no one reading the newspaper would think that there was actually something hidden. All they could see is splash of ink. Not only did they use papers but also tapes, frames, unreadable signs, in fact whatever they got. People used Morse code and postal stamps for writing covert data.

Ancient emperors used null ciphers; books 'Polygraphie' was written on methods and practices of cryptography and 'Steganographia' dealt with steganography; Americans used code talkers later in world war to communicate. Furthermore the recent prisoners' problem explained by Simmons gives a clear picture about the basis of steganography and given in Fig. 3.

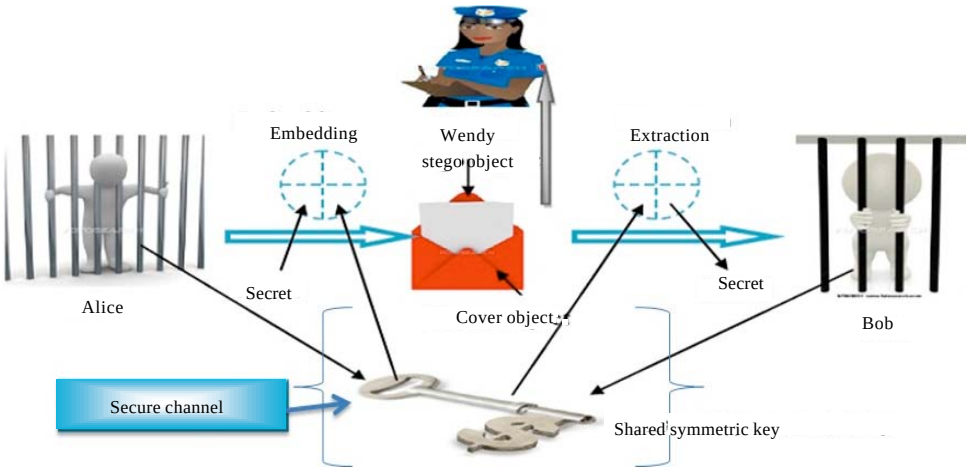

Fig. 3: Simmons prisoners' problem

PRESENT

Steganography can be stated as an extended version of cryptography i.e., it is security all the way through anonymity! Present day steganography aims at only one thing 'security in all means'! (Pfitzmann, 1996) Well, privacy is what we anticipate in internet communication. As internet has become necessity rather than luxury these days, the more information we access and share via internet, the more risky the process is. Steganography and its branches, used in their digitized version have reached out to the researchers to exploit the two as means of secrecy. Digital techniques may be categorized into spatial (Amirtharajan and Balaguru, 2009, 2010; Amirtharajan *et al*., 2011; Amirtharajan and Rayappan, 2012a, c; Aura, 1996) and transform domains (Amirtharajan and Rayappan, 2012d; Amirtharajan *et al*., 2012; Thanikaiselvan *et al*., 2011a), distortion based, masking, filtering based which under variant conditions yield projected results. The specialty in this new phase of steganography is that it suits all types of multimedia files (Bender *et al*., 1996). The concept can be molded according to the application and need (Bender *et al*., 2000).

This ecstatic mechanism has given numerous measures for instance watermarking (Zeki *et al*., 2011; Zhang *et al*., 2010), fingerprinting to hide a secret in a carrier file. Many algorithms (Thanikaiselvan *et al*., 2011a, b) and new methods like Least Significant Bits (LSB), Optimal Pixel Adjustment Process (OPAP) (Chan and Cheng, 2004; Zanganeh and Ibrahim, 2011), Pixel Indicator (PI) (Gutub, 2010; Amirtharajan *et al*., 2011; Janakiraman *et al*., 2012b; Padmaa *et al*., 2011) have been developed to enrich a scheme for practical implementation. Moreover, steganography exploits various disciplines of mathematics and engineering which gives a different color to the scheme. To name a few, matrix, set theory, information theory, calculus, OFDM, CDMA and many more (Hong *et al*., 2009; Kumar *et al*., 2011; Thenmozhi *et al*., 2012). The basic classification in information security is given in Fig. 4.

Some of the applications of steganography are when organizations use it to protect the intellectual property, to prevent piracy, digital watermarks for films, producing photo tiles, forensic science, authentication of documents, ethical issues etc. Nowadays steganography is used along

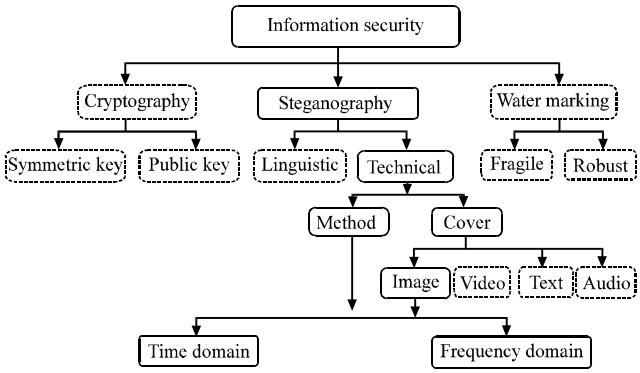

Fig. 4: Various sub-disciplines of information security

with cryptography to give better results. New forms of steganography are also being discovered. There were no measures for evaluating a particular method in olden days. But now as technology has seen a phenomenal evolution performance measures are applicable to steg algorithms too. Thus, it is done via the image metrics MSE and PSNR. If a method is proposed nowadays, with the results it has given, it is tested against attacks, compared with the existing ones and then is accepted or modified.

FUTURE

Steganography bids interesting revelation for information hiding commercially. Since steganographic schemes have proved their purposes beyond imagination, their new phases are now being uncovered for hiding data without a glitch. No wonder this has become one of the prime fields of research and works are going on around the planet to implement the notion more effectively. Also it is noteworthy to mention here is the fact that equal importance is given to steganalysis as well. Up-to-the-minute strategies of reprobates are unearthed by the researchers which have in return turned as another research field. Though steganography is a good stuff to hide data, getting all its prospects in a single scheme is really tough and the choice and the classification is shown in Fig. 5.

The future of this discipline may directed towards applying steganography mechanism in every explicit application so that rather than in general it can be exploited for a specific purpose like telemedicine (Alanazi *et al*., 2010; Zaidan *et al*., 2011). Another criterion may be tagging a digital file where steganographic schemes may contribute even more. Already existing schemes can be improvised and made resistant to attacks of geometrical nature and compound embedding is also a good line of protection. Even there is possibility of reversible embedding, where, reversibility will retrieve the cover object (Hong *et al*., 2009; Zhao and Luo, 2012). Even though steganography remains a paradox, protecting cerebral business properties with its help is highly indispensable. Apart from researchers, Governmental and Nongovernmental organizations, industrialists, business men can come forward to widen the area of steganographic research to improvise it and can think of measures for practical implementation and to create awareness. Effective combination of steganography with other disciplines like spread spectrum of study is another area of focus (Marvel *et al*., 1999; Thenmozhi *et al*., 2012).

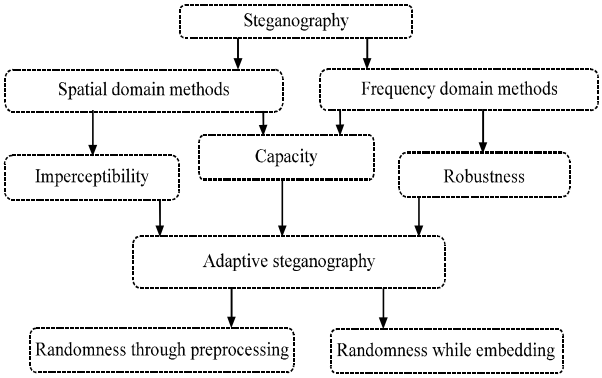

Fig. 5: Adaptive steganography and its classification

STEGANOGRAPHIC TECHNIQUES

Engender of many techniques in steganography (Rabah, 2004) which gives the path to take it to a more secured level as in Fig. 6. Mainly in steganography, one can lock the data in text (Al-Azawi and Fadhil, 2010; Shirali-Shahreza and Shirali-Shahreza, 2008; Xiang *et al*., 2011), video (Al-Azawi and Fadhil, 2010), audio (Zhu *et al*., 2011) and in image (Luo *et al*., 2008, 2011; Mohammad *et al*., 2011; Padmaa *et al*., 2011; Provos and Honeyman, 2003). The following section discusses about how safe these techniques are?

Text steganography: Hiding secret message in text (Yang *et al*., 2011) is a very taxing task. Replacing secret message requires more redundant data but it is not so in text files. But its smaller memory occupation and simpler communication attracts the steg people to use this efficiently. Three basic categories of text steganography is format-based, random and statistical generation and linguistic method. Physical text formatting is used in format based methods to conceal the data. For example, inclusion of spaces, planned misspellings scattered all over the text and font resizing.

The second one is random and statistical generation which makes use of the character and word sequences to hide the data. In character sequences just entrench the data randomly, in word sequences, by making use of the statistical properties of word length and letter frequency, generate the words which will have the identical statistical properties of the actual words. Third method uses the linguistic structure and properties of text to hide the information.

In text steganography, different steganographic approaches are hiding by selection, HTML documents, Line and Word shifting, hiding using white space, Semantic based hiding, Abbreviation based hiding. Hiding by selection, the name implies that by selecting the character in the cover text is the easiest way to bury the data. HTML tags are case insensitive, so it is simple to embed in HTML documents, this is one of the method in text steganography. Next popular method is line and word shifting, by shifting the line vertically and word horizontally by spacing of fixed inches gives the secret information to the receiver.

White spaces in text also behave as a carrier to send the secret data, two spaces implies 1 is hidden and one space mean 0 is hidden, so based on the White spaces the receiver reveal the data. In semantic based hiding, synonyms of words are used for hiding. Next one is Abbreviation based hiding, create the lexical dictionary with corresponding abbreviation and then replace the carrier text with this abbreviation. American and British spellings for the same words produce the text

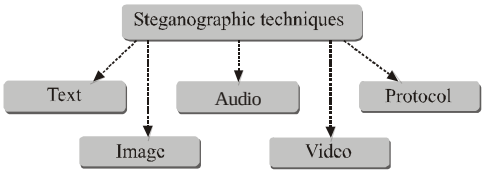

Fig. 6: Steganographic techniques and its classification

steg. For example, "Center" is designated by 1 while "Centre" is designated by 0. To consider the above methods as base, many advanced methods are created with better embedding capacity and imperceptibility in text steganography.

Image steganography: Image steganography is the most accepted and widely used steganographic means in which hush-hush information is transmitted from the sender to the receiver through an innocuous interface. Since there are plentiful images on hand, one can do wonders in secret communication which is already rocking the world and no doubt it is going to rule the upcoming years. Images of different formats with varying characteristics are exercised which gives distinguished and anticipated results. Commonly gray and color images are used to achieve secrecy during transmission. Thousands of techniques are currently in practice to achieve the same which alters the color symbolizing pixels' arithmetic value and intensity.

Image steganographic techniques are broadly classified into spatial and transform domain, distortion, masking techniques and filtering techniques. One of the most employed mechanisms in spatial domain other than PVD and matrix based embedding, is LSB. It is established in the pixels of the cover either in sequential or in random fashion. It does not produce perceptible modification to the image thus making it escapes human eye attack. The benefit of LSB is that it can hide more secret bits but at the same time it needs enhanced robustness.

Common way of masking or filtering images is by watermarking where rather than embedding in noise level, crucial areas only submit themselves to manipulation. Its main aim is to provide copyright protection and is more connected to images and survives attacks attributable to lossy compression. Watermarking is more robust than LSB and can be categorized as fragile, fingerprinting and visible. Of this fingerprinting is a helping hand in forensics, authentication, copy and copyright control etc., DWT (Chen and Lin, 2006), DFT and DCT (Provos and Honeyman, 2003) are the eminent transform domain techniques. Distortion techniques are nothing but they are out and out cover images and their characteristics based and one should have a thorough knowledge about these prior to retrieval. The cover images used in image steganography may have the formats of mp3, jpeg, wav, bmp etc. Out of these jpeg offers maximum compression ratio and image quality. So they are widely used as covers in current trends of image steganography.

Audio steganography: The process of hiding the information in a digitized audio and making it unnoticeable to the human ear is called audio steganography (Zhu *et al*., 2011). This subfield of steganography has emerged recently due to the abundance of audio files. In support of exemplar, channel can be preferred by making a perceptible sound imperceptible in the company of other sound. Since we have a sharp and vibrant hearing capacity, encoding secret information in audio is one of the exigent process. At the same time, we have a ban of inability to set apart strident and quiet sounds which is, without doubt, is a key for encoding secrets. The two crucial constraints for encoding technique are the broadcasting means of the audio and its digital layout. The main

attributes of audio steganography are sampling rate, amplification, adding noise, quantization, encoding and decoding, filtering, transcoding.

The audio steganographic domains may be broadly classified as Codec, Temporal and Transform. Codec domain platforms are bit stream hiding and modifying code book. Temporal domain embraces the disciplines Silence intervals, echo hiding and LSB. Distinguished Transform domain principles are Wavelet, Tone insertion, magnitude spectrum, cepstral domain techniques etc., of all these prominent encoding techniques employed are spread spectrum, LSB and parity coding, phase coding. LSB coding is the common method of substituting secret bits in the place of that of the cover. Phase coding is characterize by embedding the secret as phase shifts in the cover's spectrum leading to muffled coding described by SNR. Spread spectrum technique comprises of DSSS and FHSS. The secret message can also be infixed into a cover audio by means of echo which process is known as Echo Hiding. Three crucial bounds for doing so are namely decay rate, offset and amplitude. Generally, they are positioned below the humans' audible range so that they cannot identify the echo.

Even though audio steganography is an effective way of hiding data, it suffers from some notable criticism. To name a few, selected audio files (mostly wav) only can be encoded; up to 500 characters of message is only allowed; the increase in amount of data to be embedded causes increased intricacy; short of estimable interface; more time consumption for computation; one cannot know the frequency discrepancies etc.

Video steganography: Since video is the combination of image and audio, their steganographic techniques are pertinent to video as well (Al-Frajat *et al*., 2010). Instead of images and audio separately, a video containing secret information is sent from the source to destination. Payload in video steganography can be a text, audio or image. This application is developed for embedding secrets in an inoffensive medium. Unlike others, key is optional here in video. Bob communicates the encrypted video to Alice through an open channel where she retrieves the secret using the algorithm and key. Video steganography, more-attention-needed discipline, carries files in a more stout and secure manner, incorporating features of cryptography and steganography.

Since DCT changes the images in a video to a negligible extent, it is mostly employed in video Steganography. That is, it does so by rounding the images' value. Thus a change in a pixel color goes unnoticed. To make the attack harder, secret can be embedded in then and there manner rather than sequentially. For a perfect video steganographic routine, extraction should be lossless, the quality of sound and that of the picture should be high and the video should be absolutely distortion less.

Two correlations of video file come from the fact that every frame in a sequence has inter pixel spatial correlation and a video's anecdotal feature leading to temporal correlation. Some huge benefits of video steganography are distortions go unnoticed since video is nothing but incessant course of data or information and ability to hide more data contrasting audio steganography. Also since it is highly complex to embed data in a video, this resists attacks to a great extent.

Protocol steganography: The phenomenon by which the secret information is rooted inside network protocols is called protocol steganography (Fraczek *et al*., 2012). Thus steganography has come up with one more form to have private communication. There subsists some stealthy channels in OSI model used in almost all systems where in steganography comes into play. For example, TCP/IP's header in some places where they are not at all employed or discretionary can be used to

hide data or by manipulating the packet length also the goal is achieved. It covers the major properties of a successful steganography methodology whilst continuing the blatant transmission.

The two common approaches associated with protocol steganography are typical embedding and phylogenic retrieval. The former is the customary embedding strategies whereas the latter comprises of functions engendered inherently which reduces the buried data by making the most of payload. In spite of rigorous experiments, statistical tests, linguistic verification, protocol steganography has emerged as a secure and robust means of communication.

STEGANOGRAPHY DETECTION-STEGANALYSIS

As per the proverb "Nothing ventured nothing gained", we should take some risk to detect hide information over a media, There are lot of steganographic techniques to hide information; similarly there are lot of techniques to analyze it. Different steps are followed for different techniques as follows.

Text steganalysis: Text steganography can be broken down into three basic categories-format-based (Xiang *et al.*, 2007), random and statistical generations and linguistic method. Text steganography methods encrypt the information in such a way that other than receiver and sender, no one can find that there is some hidden information. Public key and private key are used to encrypt the information (Meng *et al.*, 2008).

Abnormal patterns, evolution algorithm and computer astuteness stand out in uncovering the probability of hidden information. Small shifts in word and line spacing over text may be somewhat difficult to find out to the normal observer. Still, appended spaces and "invisible" characters can be freely judged by opening the file using ordinary word processing software (Cheng *et al.,* 2005). Mainly if source of the keys or method of encryption gets revealed then secrecy of the information won't exist.

Image steganalysis: Since image steganography has caught millions' attention, the reverse technique, image steganalysis is also being the subject of interest; not only literally but also the techniques used in steganography like PVD, OPAP, LSB etc. (Dumitrescu *et al.*, 2003; Fridrich *et al.*, 2001). Blind analysis applied in images offer good and improved end results (Goljan *et al.*, 2006; Lie and Lin, 2005). Mostly this type of approaches is based on hypothesis test between stego and reference images. Many techniques like ANOVA, IQM etc., provide a helping hand in this type of work (Avcibas *et al.*, 2003). Steganalysis over image is based on image format, the various image formats are gif, bmp, jpeg with experiments on histograms and statistical studies etc. (Fridrich and Goljan, 2002).

In gif: Basically palette image steganalysis is used for gif images; it has 8 bits per pixel. The color of pixel is referenced with the help of palette table. LSB embedding over gif image alters the 24 bit RGB value of the pixel results, changing palette color of the pixel (Ker, 2005). When palette color changes strength of the stego-image will diminish. While fulfilling statistical steganalysis, gif image measures the alteration over the palette color.

In bmp: Raw image steganalysis is used for bmp image, it has lossless LSB plane. While embedding over lossless LSB plane results in casting over two gray scale values. Statistical analysis over bmp image shows the length of the hidden message.

In jpeg: The popular steganography systems that are available to hide message over jpeg images are as follows JSteg, JSteg-Shell, JPhide and Outguess. These three systems uses least significant bit embedding in order to hide messages, while performing statistical steganalysis over this methods, then the secret message will be revealed (Fridrich *et al*., 2003).

Audio and video steganalysis: Audio signals are high capacity data streams. Phase and echo hiding are some steganalysis technique over audio signals. The phase steganalysis scheme examines the fact that phase coding abuse in each audio segment, inducing changes in the phase difference. Statistical approaches also help in encountering disguised audio signals where designing a classifier and lineament selection play a very vital role (Ozer *et al*., 2003; Johnson *et al*., 2005). The Content-sovereign aberration measures are employed as characteristics of classifiers design (Avcibas, 2006). Experimental results show that the removal of content dependency from features enhances their discriminatory power.

Echo steganalysis scheme statistically figures out the peak frequency using short window evoking to a platform vector machine which is used to classify the audio signals with and without data. Steganalysis method for files of specific format has also been proposed earlier that gives a clear vision about wavelet coefficients and correlation (Ru *et al*., 2005). Unification of image and sound values are known as video files (Jainsky *et al*., 2007). Very few steganalysis methods are convenient for video; they are based on exploring the Temporal Correlation between Frames, Asymptotic Relative Efficiency (ARE), Mode Detection, internal dynamics (Cao *et al*., 2012). Based on effrontery flanked by hidden message and cover, aliasing upshot is revealed through mass function. This run can lucratively determine the covert information with unlike compression rates among the bits (Zhang *et al*., 2008). Adjacent frames in video are also studied where their correlation help bring out the secret message (Su *et al*., 2008).

CONCLUSION

Steganography is the science of hiding information with a long history and the capability to adapt to new levels of technology. For a confidential communication steganography plays an imperative role and it also provides secrecy as well as privacy in an organization. Various steganography techniques uses multimedia objects like text, image, audio and video to hide or cover the ambiguous information. While new steganography methods are being developed at the mean time, new methods are also rising to analyze the origin; the process of analyzing a multimedia object to check whether any secret information present in it is known as steganalysis. In this paper we discussed a lot of steganography and steganalysis methods in order to improve its intricate level of stego-object. In future more number of methods will be developed based on the steganography and steganalysis methods which we conferred in this survey paper.

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Alanazi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Amirtharajan, R. and R.J.B. Balaguru, 2009. Tri-layer stego for enhanced security-a keyless random approach. Proceedings of the IEEE International Conference on Internet Multimedia Services Architecture and Applications, December 9-11, 2009, Bangalore, India, pp: 1-6.

Amirtharajan, R. and R.J.B. Balaguru, 2010. Constructive role of SFC and RGB fusion versus destructive intrusion. Int. J. Comput. Appl., 1: 30-36.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India pp: 1-6.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Aura, T., 1996. Practical invisibility in digital communication. Inf. Hiding, 1174: 265-278.

Avcibas, I., N. Memon and B. Sankur, 2003. Steganalysis using image quality metrics. IEEE Trans. Image Process, 12: 221-229.

Avcibas, I., 2006. Audio steganalysis with content-independent distortion measures. IEEE Signal Process. Lett., 13: 92-95.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Syst. J., 35: 313-336.

Bender, W., W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, 2000. Applications for data hiding. IBM Syst. J., 39: 547-568.

Cao, Y., X. Zhao and D. Feng, 2012. Video steganalysis exploiting motion vector reversion-based features. IEEE Signal Process. Lett., 19: 35-38.

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simple LSB substitution. J. Pattern Recognit. Soc., 37: 469-474.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Chen, P.Y. and H.J. Lin, 2006. A DWT based approach for image steganography. Int. J. Applied Sci. Eng., 4: 275-290.

Cheng, J., A.C. Kot, J. Liu and H. Cao, 2005. Steganalysis of data hiding in binary text images. Proceedings of the IEEE International Symposium on Circuits and Systems, May 23-26, 2005, Korea, pp: 4405-4408.

Dumitrescu, S., X. Wu and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. IEEE Trans. Signal Process., 51: 1995-2007.

Fraczek, W., W. Mazurczyk and K. Szczypiorski, 2012. Hiding information in a stream control transmission protocol. Comput. Commun., 35: 159-169.

Fridrich, J. and M. Goljan, 2002. Practical steganalysis of digital images - state of the art. Proceedings of the SPIE, Security and Watermarking of. Multimedia Contents, April 29, 2002, USA., pp: 1-13.

Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. Multimedia IEEE, 8: 22-28.

Fridrich, J., M. Goljan, D. Hogea and D. Soukal, 2003. Quantitative steganalysis of digital images: Estimating the secret message length. Multimedia Syst., 9: 288-302.

Goljan, M., J. Fridrich and T. Holotyak, 2006. New blind steganalysis and its implications. Proc. SPIE, 6072: 1-13.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerging Technol. Web Intell., 2: 56-64.

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

Jainsky, J.S., D. Kundur and D.R. Halverson, 2007. Towards digital video steganalysis using asymptotic memoryless detection. Proceedings of the 9th ACM Multimedia and Security Workshop, September 20-21, 2007, USA., pp: 161-168.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Johnson, M.K., S. Lyu and H. Farid, 2005. Steganalysis of recorded speech. Proceedings of the SPIE International Society for Optical Engineering, March, 2005, USA., pp: 664-672.

Kahn, D., 1983. The Codebreakers: The Story of Secret Writing. Macmillan, New York.

Ker, A.D., 2005. Steganalysis of LSB matching in grayscale images. IEEE Signal Process. Lett., 12: 441-444.

Kumar, P.P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Lie, W.N. and T.C.I. Lin, 2005. A feature-based classification technique for blind image steganalysis. IEEE Trans. Multimedia, 7: 1007-1020.

Luo, G., X. Sun and L. Xiang, 2008. Multi-blogs steganographic algorithm based on directed hamiltonian path selection. Inform. Technol. J., 7: 450-457.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Marvel, L.M., C.G. Boncelet Jr. and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

Meng, Y.Y., B.J. Gao, Q. Yuan, Y. Fu-Gen and W. Cui-Fang, 2008. A novel steganalysis of data hiding in binary text images. Proceedings of the 11th IEEE Singapore International Conference on Communication Systems, November 19-21, 2008, Guangzhou, China, pp: 347-351.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

Ozer, H., I. Avcibas, B. Sankur and N.D. Memon, 2003. Steganalysis of audio based on audio quality metrics. Proceedings of the Security and Watermarking of Multimedia Contents, June 13, 2003, USA., pp: 55-66.

Pfitzmann, B., 1996. Information Hiding Terminology. Proceeding of the First Int. Workshop on Information Hiding, Vol. 1174, May 30, June 1, 1996, Lecture notes in Computer Science, Cambridge, UK, pp: 347-350.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Qi, K., D.F. Zhang and D. Xie, 2010. A high-capacity steganographic scheme for 3D point cloud models. Inform. Technol. J., 9: 412-421.

Qin, J., X. Sun, X. Xiang and Z. Xia, 2009. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

Qin, J., X. Xiang and M.X. Wang, 2010. A review on detection of LSB matching steganography. Inform. Technol. J., 9: 1725-1738.

Rabah, K., 2004. Steganography-the art of hiding data. Inform. Technol. J., 3: 245-269.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Ru, X.M., H.J. Zhang and X. Huang, 2005. Steganalysis of audio: Attacking the steghide. Proceedings of the International Conference on Machine Learning and Cybernetics, Volume 7, August 18-21, 2005, Guangzhou, China, pp: 3937-3942.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Stallings, W., 2010a. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall, USA.

Stallings, W., 2010b. Network Security Essentials: Applications and Standards. 4th Edn., Prentice Hall, USA.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Su, Y., C. Zhang, L. Wang and C. Zhang, 2008. A new video steganalysis based on mode detection. Proceedings of the International Conference on Audio, Language and Image Processing, July 7-9, Shanghai, pp: 1507-1510.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

Thien, C.C. and J.C. Lin, 2003. A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recog., 36: 2875-2881.

Xia, Z., X. Sun, J. Qin and C. Niu, 2009. Feature selection for image steganalysis using hybrid genetic algorithm. Inform. Technol. J., 8: 811-820.

Xiang, L., X. Sun, G. Luo and C. Gan, 2007a. Research on steganalysis for text steganography based on font format. Proceedings of the 3rd International Symposium on Information Assurance and Security, August 29-31, 2007b, Manchester, UK., pp: 490-495.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inform. Technol. J., 10: 992-1000.

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel document using text-rotation technique. Inform. Technol. J., 10: 889-893.

Zaidan, B.B., A.A. Zaidan and M.L.M. Kiah, 2011. Impact of data privacy and confidentiality on developing telemedicine applications: A review participates opinion and expert concerns. Int. J. Pharmacol., 7: 382-387.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zanganeh, O. and S. Ibrahim, 2011. Adaptive image steganography based on optimal embedding and robust against chi-square attack. Inform. Technol. J., 10: 1285-1294.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373.

Zhang, C., Y. Su and C. Zhang, 2008. Video steganalysis based on aliasing detection. Electron. Lett., 44: 801-803.

Zhang, Y., Z.M. Lu and D.N. Zhao, 2010. A blind image watermarking scheme using fast hadamard transform. Inform. Technol. J., 9: 1369-1375.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.