http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 11 (5): 566-576, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.566.576

Random Image Steganography and Steganalysis: Present Status and Future Directions

[1]Rengarajan Amirtharajan, [2]Jiaohua Qin and [1]John Bosco Balaguru Rayappan
[1]School of Electrical and Electronics Engineering, SASTRA University,
Thanjavur, India-61340
[2]School of Computer and Information Engineering,
Central South University of Forestry and Technology, 410004, Peoples' Republic of China

Abstract: In the current corporate scenario, data or information security is the most significant asset because loss of information will lead to financial and market loss which in-turn will be the end of business. Though, the security guards like cryptography, watermarking, steganography have armed on the electromagnetic pathway against hackers, the concern on data protection is growing in parallel with the up-to-the-minute electronic technology. In this review, the role, strength and weakness of steganography especially different random image steganography techniques in protecting the data have been analyzed and in addition how random techniques can be made smarter and effective have also been explored.

Key words: Information hiding, random image steganography, steganalysis

INTRODUCTION

Gone are the days when images were only about memories of the past. The images now speak more than that because of the advent of the field of image steganography (Cheddad *et al.*, 2010), which embeds secret information in images imperceptible to the naked human eye (Rabah, 2004; Amirtharajan and Balaguru, 2009). From time immemorial emphasis on new techniques for secret communication has been given high importance based on the levels of confidentiality required. Three interlinked techniques namely cryptography (Schneier, 2007), steganography and watermarking (Stefan and Fabin, 2000) form the base for secure communications. While, cryptography involves making the content undecipherable the other two are information hiding methods where the mere presence of information is itself hidden (Amirtharajan *et al.*, 2011).

Steganography is an art of embedding the secret information within some other file generally known as cover. The main objective of steganography is to provide a secret communication between any users such that any undesirable person cannot gain access to the information by just glancing at the cover file (Bender *et al.*, 1996). This prowess of secret communication coined as Steganography means "covered writing" in Greek. Various methods are implemented to obliterate the existence of the secret message. A bunch of such techniques include invisible ink, character arrangement, microdots and digital signatures and spread spectrum.

Steganography basically administers four main modules say, a cover file which acts as the container for the secret message, a secret message that contains the confidential data, a key for encoding the secret message and steganography algorithm for sneaking in the secret message inside the container as depicted in Fig. 1. The combination of these modules creates the stego-object which is then sent to the receiver. At the receiver's end the decoding algorithm is implemented to retrieve the original message from the stego-file (Wang and Wang, 2004).

In the recent times, digital media such as text, audio, video, protocols or image are being opted for steganography (Rabah, 2004; Bender *et al.*, 1996). The sender decides the effectuation based on their requirement. However due to the confined ability of the human visual system, image steganography is best-loved among the available methods. This is due to the presence of superfluous information in the images which can be easily interpolated. Table 1 present differences among steganography, watermarking and cryptography.

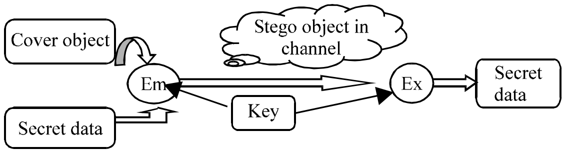

Fig. 1: Simple schematic of stego system

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering,
SASTRA University, Thanjavur, India-61340

Table 1: Different among steganography, watermarking and cryptography

Property			
Carrier, secret data, key and output	The payload is embedded in any digital media with an optional key and is called as the stego-file	The water mark is embedded in image/audio files and is called as the Watermarked-file	The information is encrypted in text or image files and output is called as the Cipher-text
Selection of cover	Any cover can be chosen	Restriction in cover selection	N/A
Objective and concern	Capacity is a major concern for the secret communication aided by steganography	Robustness is a necessary feature of copyright preservation	Robustness is essential for data protection
Detection and retrieval	The cover is not needed for recovery and full retrieval of data is possible	Data is retrieved by cross-correlation and the original cover is required for the same	Full retrieval of data without the need of the cover
Relation to cover and visibility	The information is not generally related to the cover and is never perceptible to the normal human vision	Watermarks are sometimes visible to human eye and usually becomes an attribute of the image	Due to encryption, we can easily know that there is hidden data but deciphering is difficult
Attacks	Steganalysis detects the presence of information	Image processing aids in removal /replacement of watermarks	Cryptanalysis de-ciphers the encrypted information

Table 2: Year wise publication details

Year	1997	'98	'99	2000	'01	'02	'03	'04	'05	'06	'07	'08	'09	'10	'11/12	Total No. of papers
Science direct	8	15	7	9	17	60	42	33	60	53	76	101	128	117	132/13	883
Scopus	4	17	16	20	40	54	78	155	165	215	260	325	433	600	453	2835
IEEE	2	11	9	17	29	36	55	77	75	123	168	242	317	299	157	1617
Springer	8	15	5	19	7	6	19	55	167	118	112	137	163	158	272	1261

Table 3: Total number of publication in web search

Steganography as keyword	Total No. of papers
Springer	1261
Scopus	2835
IEEE	1618
Science direct	883
DOAJ	280
Citeseer	2543
Sciverse	30225
ACM digital library	508
Google scholar	19100

Table 4: Total number of patents filed in various patent offices

Patent offices (PO)					4070				
USA PO	1604	WIPO	277	Europe PO	114	UK PO	23	Japan PO	17

While the ambit of steganography is immense, it has been mainly used for secret communication. Although, steganography and cryptography both cater to the same purpose, the advantage of former over later is that, it obliterates the existence of the secret message (Thanikaiselvan *et al*., 2011a; Padmaa *et al*., 2011; Janakiraman *et al*., 2012). It can be used to hide a systems identity by masking the TCP/IP headers. Apart from these many other task like feature tagging such as time stamp, captions etc can be embedded in an image. Steganography has also found its way in various technologies such as X-ray (containing both doctor's notes as well as the X-ray image), printers (scarcely visible tiny yellow dots indicating the printer serial number etc. (Petitcolas *et al*., 1999; Zaidan *et al*., 2011).

In order to enhance the security of the communication, the information is first encrypted and later hidden so that the attacker has to first find the blotted out information and then decrypt it (Padmaa *et al*., 2011). The flaw with cryptography alone is that the encrypted message can be easily ascertained during transit by anyone who is looking for it thus making the communication vulnerable. While aspiring for better outcome in image steganography it is important to keep three aspects in mind. The first one is the capacity of the cover image i.e., it should be able to store utmost data inside it. Second being imperceptibility should provide an unaltered image after data hiding (Zaidan *et al*., 2011). Last but not the least is robustness i.e. it should be secure against attacks. Blending these three aspects efficaciously will help in achieving the goal of image steganography.

To justify the popularity of the chosen review topic, a simple search has been conducted, to survey the number of articles, which have been published in referred and peer reviewed journals and number of Patents filed in various patent offices throughout the world with the search key word Steganography and the results are presented in Table 2-4.

Search key word: Streganography.

Web search sources: Science Direct, SCOPUS, IEEE, Springer, DOAJ, Citeseer, Sciverse, ACM Portal and Google Scholar.

Table 2-4 confirm that, year by year the number of papers published in the chosen field of study has dramatically increased. Furthermore, there are three different review/survey papers available in the existing literature for steganography (Petitcolas *et al*., 1999; Li *et al*., 2011; Chen and Shi, 2008; Cheddad *et al*., 2010), but none of the three specify anything about random image steganography. Hence, in this study, the present status and future direction has been presented.

STEGANOGRAPHY BASIC TERMINOLOGY

- Cover image is the carrier which is used to carry or preserve the embedded bits
- The image embedded with the secret data is referred to as the stego-image
- Capacity or simply Payload is amount of secret data to be embedded and sometimes expressed in Bits Per Pixel (BPP) or simply in number of bits
- Imperceptibility - literal meaning is very slight or hard to find the difference between the cover image and Stego Image
- Robustness-with standing ability even towards intentional attacks but not suitable for Steganography, because if somebody suspects, there is a covert communication, then steganography is no more undercover operation
- Steganalysis includes the attacks on the images by various image processing techniques to expose the hidden information by attackers

REVIEW ON THE STEGANOGRAPHY

Steganography, derived from Greek words meaning ‘covered writing’ has been in use over the past thousands of years (Stefan and Fabin, 2000). For example, Histaiacus tattooed a message on a slave’s shaved head and the slave was sent as messenger after his hair grew back. Another way of secret writing of the Chinese was reinvented by the Italian mathematician Jerome Cardan and included a paper mask with holes between both the sender and receiver and secret message is written by keeping the paper mask on a blank sheet. Later the blanks are filled to appear as innocuous text and this method is called as Cardan Grille. The Nazis invented several steganographic methods during the World War II using invisible ink and null ciphers and Microdots. An example can be given as follows: Apparently neutral’s protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.” is a message sent by a Nazi spy, which when decoded using the second letters reveals the secret message ‘Pershing sails from NY June 1’. Another interesting case is wherein Morse code was concealed in a drawing in the form of long grass and short grass in the year 1945. From these ancient methods, steganography has made a giant leap to the digital form as well due to the enormous improvement in computer power, internet and advancements in digital signal processing. Steganography is widely used in confidential communication purposes and a continuous evolution is guaranteed due to its applications. Any advancement in science would certainly have a disadvantage. In this case, the concern was about the usage of steganography by terrorists for secret plots, which is also called as cyber planning or digital menace (Stefan and Fabin, 2000). Steganography does not exist for still images alone. Embedding hidden messages in video (Al-Frajat *et al*., 2010) and audio files (Zhu *et al*., 2011) is also possible which makes steganalysis even tougher. The general schematic description of steganography with different cover (Video, Audio and Image) are shown in Fig. 2.

Rabah (2004) provides a brief history of steganography and discusses about how it is related to cryptography. In addition to that it also expounds the purpose, strengths, weaknesses, advantages and disadvantages of steganography. A study was conducted by Hmood *et al*. (2010a) wherein strengths and weakness for possible multimedia covers for steganography approaches were elucidated and methods to improve capacity and security were discussed. Hmood *et al*. (2010b) in their work has presented an overview of sophisticated information hiding techniques which involve image file as a cover for carrying out the processes. In a High-capacity Steganographic Scheme for 3D Point Cloud Models by Qi *et al*. (2010), Self Similarity Position Matching (SSPM) procedure was used presenting high-capacity spatial side-match steganography for 3D point cloud model. Mohammad *et al*. (2011) in their work proposed a transparent and high hiding capacity algorithm which effectively uses Block Truncation Coding (BTC) by employing a two level (one-bit) nonparametric quantizer and Human Visual System (HVS) masking characteristics ensuring high visual quality of stego image.

Hong *et al*. (2009) proposed a method to improve the stego image quality by using reversible contrast mapping data hiding scheme that uses the variance feature of the

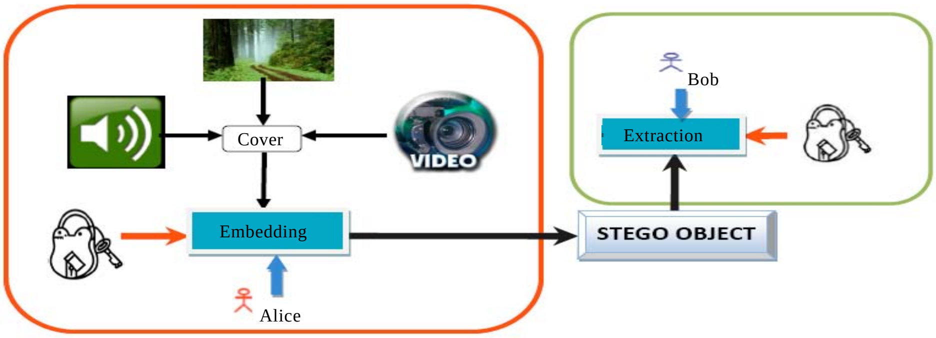

Fig. 2: General schematic description of Steganography

cover image. Luo *et al*. (2011) proposed a method that incorporates secret sharing and data hiding technique for block truncation coding for image compression. Under this method two quantization levels are hidden under in two share images to increase the level of compression. Zeki *et al*. (2011) have developed a digital watermarking model which can find out the possibility to embed maximum amount of data in an image without quality reduction. Zaidan *et al*. (2011) have done a review on the impact of data privacy and confidentiality on developing telemedicine applications in this paper. They have also done a short survey on 130 participants to support their claim. Alanazi *et al*. (2010) have proposed a handshake protocol depending on symmetric and asymmetric cryptography for patient, medical center and doctor, medical center for improving the privacy electronic medical record transmission.

Zanganeh and Ibrahim (2011) have proposed a substitution based technique which involves embedding data into uncertain and higher LSB layers which allows flexibility and also allows us to embed a large amount secret message. Padmaa *et al*. (2011) have proposed a method that combines steganography and cryptography in a unique way so as to provide enhanced level of security. Here we get two different forma of the message T1 and T2 using two distinct keys K1, K2. Amirtharajan and Balaguru (2009) have proposed a three layer method for image steganography. First layer involves pixel statistics conversion method. Second stage involves embedding the result into a gray image using moore space filling curve and finally the third stage consists of the gray image being embedded into another image using Hilbert space filling curve to produce the final colour image. Amirtharajan and Rayappan (2012) also explained a way to reduce the embedding effect and to improve the stego image quality by adapting different traversing path along with inverted pattern approach. Amirtharajan *et al*. (2010) filed a patent using kolam traversing path to improve the cryptic effect. Amirtharajan *et al*., (2011) proposes a method using Pixel Indicator along with adaptive embedding and integrity check to enhance cryptic effect. Furthermore, a detailed survey on effective way to combine OFDM+CDMA for secure communication using information hiding is available by Thenmozhi *et al*. (2011).

Al-Azawi and Fadhil (2010) proposed a text steganography technique suitable for Arabic characters, hiding information by inserting extensions character (kashida). Huffman coding was employed at its initial phase to compress text into binary format. Xiang *et al*. (2011) designed a novel steganography method that employed selecting a series of MCQ's(Multiple Choice Questions) that could generate the secret data. This technique when compared against existing linguistic steganographic techniques, seemed superior. Luo *et al*. (2008a) presented an algorithm based on the directed Hamiltonian path selection in the complete digraph mapped from multi-blogs with same article. This work was found to possess good imperceptibility and high security.

This review suggested the following, that a simple classification could be methods based on spatial (Amirtharajan and Balaguru, 2011a; Thanikaiselvan *et al*., 2011b) or transform domain techniques (Provos and Honeyman, 2003; Thanikaiselvan *et al*., 2011a) or there is a possibility to classify steganography methods based on the covers i.e., Video Steganography, Text based Steganography (Shirali-Shahreza and Shirali-Shahreza, 2008) Audio Steganography and Image Steganography. The former method could be further classified into substitution, transform, statistical, spread spectrum (Kumar *et al*., 2011) and Amirtharajan and Balaguru (2011b) and cover generation methods. Another classification on steganography is pure steganography, secret key steganography and public key steganography.

In the belles-lettres of steganography, there are three standard protocols namely pure steganography, public key steganography and secret key steganography.

Pure steganography: This system includes the pure or unadulterated working principles of steganography, wherein the prior transfer of shared/ secret key. As in the shared or secret key transfer to the other participant/recipient is not mandatory, but still the purpose can be achieved.

In the common terms, the embedding process in this mode of steganography is coined and elaborated in terms of mapping in set theory, where E be the embedding process and C be the set of all cover images and M be the set of all possible images and is defined as E: $C{\times}M \rightarrow C$ while the extraction process is denoted by D and is a mapping representing D: $C \rightarrow M$, which depicts the extraction of secret message off the cover.

It is mandatory that $|C|> = |M|$ and the embedding and extraction algorithm must be accessible to both transmitter and receiver, but to no one else.

Secret key steganography: As pure steganography relies completely on secrecy, it cannot be always banked upon when the transfer is prone to loose secrecy, although the transfer is between E (Embedding End) and D (Extraction End). This is not secure as it violates kerckhoff's principle (Provos and Honeyman, 2003), which simply states, the method of transferring must be secure even though none knows its encoding process).

With this Secret Key steganography can be implemented with three stratified objects (A cover image C, Secret Message M and a Secret key K). The sender chooses random cover image takes the secret message embeds it into the cover image deploying the secret key K along with it. And at the receiver end, if the secret key is known, the secret message can be extracted from the cover image. And as obvious, any person unaware of secret key has no scope of finding out the secret message.

Mathematically, with set notation we have, EK: $C{\times}M{\times}K \rightarrow C$ and DK: $C{\times}K \rightarrow M$ (where EK-Embedding with secret key and DK-Extraction with Secret Key K).

Public key steganography: As the name suggests the encoding key is public key, which is visible to the public database and everyone has access to it. So, the embedding process is visible to everyone. Here, the true sender will also use a secret key D, which is the apt key for decoding the secret message. So, although, the public key is known to the third person, the message cannot be decoded until and unless the third person knows the secret key D. All the three are the classification on existing steganography.

Pseudorandom permutation steganography: A little too deceiving method for the sender, as this incorporates the complete utilization of the cover image, such that every bit is not left turned. This method of employment of every bit of the image along with the secret key and in a random fashion of encoding leaves the hacker with no hint of find the subsequent encoded bits hence making it extremely tedious to poach into the data.

This random fashion of encoding can be done with multiple keys(k1, k2, k3 and so on) or by the creation of multiple element indices from (J1……… Jm).

RECENT TRENDS SUGGESTED IN RANDOM IMAGE STEGANOGRAPHY

Random image steganography, defined as an image steganography which offers cryptic effect. So far existing literature expects and suggest that well defined cryptography algorithm could be employed prior to embedding on the confidential information to offer cryptic effect. But random image steganography is to preprocess the data with well defined cryptographic algorithm then adapt any one of the possible ways to improve the complexity.

Possible ways of random image steganography:

Method 1: K bit embedding with a key 1 [0 0 0 0 1 1 0 1] in a pixel
Method 2: Key 2 [1 0 1 0 1 1 0 1] in a cover
Method 3: Using Fibonacci series 1, 2, 3, 5, 8, 13 …. If exceeds use mod length of the Cover, problem collision attacks
Method 4: Variable bit embedding on the pixel (PVD)
Method 5: Encrypt the secret then embed
Method 6: Use different encoding instead of ASCII
Method 7: Distort the cover with known value then embed
Method 8: Compress the secret data then embed
Method 9: Compress, Encrypt and Embed
Method 10: Compress+Error control codes+Encrypt then embed
Method 11: Select the pixels by Generating Pseudo random number then Embed
Method 12: Select pixels based on intensity values then variable bit embedding
Method 13: Study the statistics of the cover without affecting embed. Else Better Change the "ROUTE" for embedding

Method 1: K bit embedding with a key 1 [0 0 0 0 1 1 0 1] in a pixel: It will embed data into the pixels based on the four LSBs of the key.

- If key = [0 0 0 0 1 1 0 1] then embedding should be in the 1st (2^0), 3rd (2^2) and 4th (2^3) LSBs
- If key = [0 0 0 0 0 1 0 1] then embedding should be in the 1st(2^0) and 3rd(2^2) LSBs

Merits: Its embedding capacity, MSE and PSNR depend on the key. Randomness is introduced in this method if the keys are other than [0 0 0 0 0 0 0 1], [0 0 0 0 0 0 1 1], [0 0 0 0 0 1 1 1], [0 0 0 0 1 1 1 1] as in these cases it will be normal LSB substitution with 1, 2, 3, 4 bits, respectively.

Complexity:

- If the data is encrypted using DES it will introduce a complexity of (2^64)
- Probability of embedding 0-bits in last four LSBs is ((4c3)/16) = (1/16)
- Probability of embedding 1-bit in last four LSBs is ((4c1)/16) = (4/16)
- Probability of embedding 2-bits in last four LSBs is ((4c2)/16) = (6/16)
- Probability of embedding 3-bits in last four LSBs is ((4c3)/16) = (4/16)
- Probability of embedding 4-bits in last four LSBs is ((4c4)/16) = (1/16)
- So the final complexity of embedding 1-bit is: (2^64)*(1/16)*(1+4+6+4)

Complexity: Good when keys [0 0 0 0 0 0 0 1], [0 0 0 0 0 0 1 1], [0 0 0 0 0 1 1 1] and [0 0 0 0 1 1 1 1] are not used.

Imperceptibility: Visible to some extent if the key used is [0 0 0 0 1 1 1 1].

Suggestion: Don't embed more than 3 bits in grey and 8 bits in color image.

Method 2: Key 2 [1 0 1 0 1 1 0 1] in a cover: It will embed data into the selected pixels basing on the key.

- If key = [1 0 1 0 1 1 0 1] then embedding should be done in the pixels 1, 3, 5, 6, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding
- If key = [1 1 0 0 0 1 1 1] then embedding should be done in the pixels 1, 2, 6, 7, 8. This sequence of embedding should be repeated for a block of eight pixels for complete embedding

Merits: It has a relatively lower MSE and a relatively higher PSNR. Randomness is introduced in this method if the key is other than [1 1 1 1 1 1 1 1] as in this case it is normal raster scan LSB substitution with zero randomness.

Complexity: If the data is encrypted using DES it will introduce a complexity of (2^64).

Complexity: Good when key [1 1 1 1 1 1 1 1] is not used.

Imperceptibility: Visible to some extent if key [1 1 1 1 1 1 1] is used with 4-bit embedding in each pixel.

Method 3: Using Fibonacci series 1, 2, 3, 5, 8, 13 …. If the value exceeds, then use the mod length of the cover. The problem with this is collision attacks: In this method pixels are selected for embedding in the following way. A row is selected if it is not a Fibonacci number. Similarly, the column is also selected. Two methods are possible. In the first methodology, embedding can be done in all the row and column numbers that are a part of Fibonacci series. In the second methodology, embedding can be done in all the row and column numbers that are not a part of Fibonacci series.

In method 1 rows 1, 2, 3, 5, 8, … are selected and in a particular row again pixels 1, 2, 3, 5, 8, … will be selected for embedding.

In method 2 rows 1, 2, 3, 5, 8, … are selected and in a particular row again pixels 1, 2, 3, 5, 8, … will not be selected for embedding. All others pixels will be selected for embedding.

Merits: Method 1 gives more randomness and imperceptibility while method 2 gives more embedding capacity.

Complexity analysis: If the data is encrypted using DES it will introduce a complexity of (2^64).

For method 1: For a 256*256 image, the complexity varies with respect to size of image:

- Selecting a row which is a part of Fibonacci series can be done in (12/256) ways
- Selecting a column which is a part of Fibonacci series can be done in (12/256) ways
- 4 bits can be selected for embedding in four LSBs in 1 way
- So the final complexity of embedding 1-bit is: (2^64)*(256/12)*(256/12)*1

For method 2: For a 256*256 image, the Complexity varies with respect to size of image:

- Selecting a row which is not a part of Fibonacci series can be done in (244/256) ways
- Selecting a column which is not a part of Fibonacci series can be done in (244/256) ways
- 4 bits can be selected for embedding in four LSBs in 1 way
- So the final complexity of embedding 1-bit is: (2^64)*(256/244)*(256/244)*1

Method 4: Variable bit embedding on the pixel (PVD). This method is similar to embedding data into pixels based on the nature of image. If the image is having an edge, more bits will be embedded and if it's a smooth area then less bits are embedded.

Merits: Since, it is taking the image texture into consideration, the imperceptibility is very high. It is also complex due to the variable bit embedding.

Complexity analysis: If the data is encrypted using DES it will introduce a complexity of (2^64).

It is taking variable bit embedding and so the complexity increases. But complexity remains the same.

Imperceptibility: Is low because it takes the image texture into consideration.

Method 5: Encrypt the secret then embed: Here, simply the data is first encrypted using some encryption algorithm and then encryption is done with the encrypted data and not with the original data. Security increases because of encryption but it will also depend on the embedding algorithm. It can be combined with any of the methods above.

Method 6: Use different encoding instead of ASCII: Here encoding is changed for conversion of messages (may be text/audio/video) into bits. Normally ASCII codes are used for converting a numerical data into binary. Instead of ASCII some other encoding mechanism such as Shannon encoding, Shannon-Fano encoding, Huffmann encoding etc can be used. Some encoding algorithms give encoded data based on the probability of its occurrence in the data. This can increase the embedding capacity for the same level of distortion.

Method 7: Distort the cover with known value then embed: Here the cover image will be initially scrambled and the resultant scrambled image is used for embedding of data. After embedding process is done the image is once again de-scrambled to get the stego image. By this process we can never determine the path of embedding unless the initial key for scrambling of image is known. Thus this method increases the complexity through image encryption.

Method 8: Compress the secret data then embed: Here the secret data is compressed using some reversible compression algorithm (i.e., lossless compression is performed) and the obtained data after compression is used for embedding. The complexity lies in the embedding algorithm and the compression algorithm and the latter contributes more to complexity.

Method 9: Compress, Encrypt and Embed: t includes all the above three. Compressing the data initially, encrypting the obtained result and using this final result for embedding. This gives more complexity than the previous case.

Method 10: Compress+Error control codes+Encrypt then embed: Here, the data is initially compressed by some compression algorithm and for the resultant data, error control codes such as hamming codes, cyclic codes or convolutional codes are applied for securing the compressed data. This resultant data is then encrypted and embedded. A merit of this methodology is that even if some pixels are tampered, we will be able to retrieve back our data. Complexity will be similar to the previous methodology.

Method 11: Select the pixels by Generating Pseudo random number then Embed: In this methodology embedding is done by choosing some pseudo random number. For example the pseudo random number can be generated by taking the numbers after decimal point in pi (22/7). Here embedding can be performed by taking a block of 10 pixels at a time and processing them. Consider pi as 3.141592654. Now embedding is done in 1st pixel in first block of 10 pixels and in 4th pixel in second block of 10 pixels and in 1st pixel in 3rd block of 10 pixels and so on. This type of embedding will produce randomness and increase the complexity to a very great extent.

Method 12: Select pixels based on intensity values then variable bit embedding: In this methodology number of bits to be embedded in each pixel is decided by the pixel intensity. A threshold is set and based on this, the number of bits to be embedded in each pixel is decided. For example if the pixel intensity is greater than 75 then two bits are embedded and if it is greater than 150 three bits are embedded and if it is greater than 225 four bits are embedded or else 1 bit is embedded. Thus variable bit embedding based on the intensity value is implemented and it increases the complexity due to its variable embedding nature.

Method 13: Study the statistics of the cover without affecting embed: In this methodology embedding is done after taking image statistics into consideration. Here more number of bits are embedded in the edge areas and less number of bits are embedded in the plane areas and the imperceptibility is enhanced.

REVIEW ON THE STEGANALYSIS

With the aim of detecting the presence of secret messages (Qin *et al*., 2010), steganalysis is classified into two categories based on the way of looking out for the secret namely steganalysis fro specific embedding and universal blind steganography. The specific stegananlysis is capable of estimating the embedding ratio or even reveal the secret once the algorithm used for embedding is known. This feature is similar to that of RS, SPA, DIH and LSM algorithm which can detect the spatial LSB steganography and Pevni and Fridrich (2007) algorithms which can reliably determine the presence of secret messages embedded in the DCT domain of the image. Studies involving the theoretical analysis and practical experiments have revealed that LSB matching is more difficult than LSB replacing.

Though specific embedding steganography seems interesting and more fruitful, in reality, it is very difficult to implement since the method used for embedding is hardly known to the steganalysts. On the other hand, the Universal blind approaches are more attractive for practical applications since it detects the presence of secret message without the need of knowing the embedding algorithm. The flexibility and adaptability of the Universal blind approaches to get adjusted to new and previously unknown stego-methods gives it an edge over the specific methods which give comparatively more accurate and reliable results.

The Universal blind steganalysis technique (Luo *et al*., 2008b) is a meta-detection method which can be adjusted to detect ant steganographic method employed once it has been trained esing the cover and stego images. Two types of non-specific steganalysis techniques exist in literature. The first classifies the images as cover or stego using the original images as the training set and to extract the features and since it does not make use o of knowledge of the algorithms, it is purely a blind steganalysis technique. The second technique utilizes a combination of cover and stego images as the training set. Here, the assumption made is that special hiding techniques might have been used for embedding but details about them is not known and hence this method is also called as ‘half-blind’ detection method. This half-blind steganalysis technique is an important domain of research in blind detection researches since it has a good generalizing capability and is able to detect even new and unknown steganographic methods.

The idea of using a trained classifier to detect secret messages has been developed in the past years. Avcibas *et al.* (2003) are the first to propose the framework for classifier-based steganalysis. Subsequently, they presented a different feature set based on binary similarity measures for steganalysis and its experimental results showed that, generally, SVM (Support Vector Machines) could provide better performance than other classifiers. Farid (2002) also has investigated the problem of classifier-based steganalysis, and further validates that classifier-based scheme is an effective and universal approach to deal with the twin difficulties of unknown image statistics and steganographic algorithms. Fridrich *et al.* (2005) and other researchers also studied the technique of universal steganalysis with trained classifiers. These methods first extract an appropriate feature set that should be sensitive to steganographic modifications and then build a classifier to distinguish original images from stego ones.

Recently, researches show that the improved performance of the image steganalysis is achieved at the expense of increasing the number of the feature. A few single features for the detection of secret messages have been proposed by Liu *et al.* (2008a), point out that single feature is usually uncapable of differentiating stego and cover signals effectively. And then, they extracted two statistical properties for image steganalysis, one from the spatial domain and the other from the DCT domain. Avcibas *et al.* (2003). used ten image quality metrics as feature set and employed 18 features from binary similarity measures of the seventh and eighth bit planes in an image for classification Fridrich *et al.* (2005) extracted 23 calibrated features from DCT and spatial domain. They subsequently built the universal classifier by exploiting 81 features which were extracted from the higher-order absolute moments of residual noise in the wavelet domain, Farid (2002) extracted 72 features by image decompositions based on QMF. Lately, Fridrich *et al.* (2005) even have utilized 274 features for steganalysis. Chen and Shi (2008) adopted 324 features from the statistical moments of wavelet characteristic functions. Farid and Lyu (2003). made use of a considerably larger

432 features composed of higher-order magnitude and phase statistics.

There are other works in steganalysis, For example Xia *et al.* (2009) proposed a method wherein by studying neighborhood node degree characteristics, Least Significant Bit (LSB) matching steganography in gray images could be detected. Qin *et al.* (2009a) proposed an efficient steganalytic method that detects LSB matching steganography for the compressed and uncompressed images by constructing classifiers based on differences between the neighboring pixels (DNPs), differences between the local extrema (DLENs) and their neighbors in grayscale histogram. Qin *et al.* (2009b) presented a survey of LSB matching steganalysis methods for digital images. The study pondered over some persisting problems and made way towards aspects worth researching.

However, using too many features is undesirable in terms of classification performance due to the curse of dimension. Furthermore, performing feature selection in steganalysis offers several advantages as follows: (1) Feature selection prunes the meaningless features for the classifier. (2) Feature selection may also be used to improve the classification performance. (3) Feature selection can reduce the complexity for both features generating and classifier training. (4) The selected features can help to point out the features that are sensitive to a given steganographic scheme and consequently to bring a highlight on its weaknesses. Hence, it is necessary to reduce the feature dimension by eliminating redundant features and selecting the most relevant ones.

CONCLUSION

In this review, a brief encyclopedia of infant steganography to matured steganography has been presented. Starting with the definition, differences with other security guards like cryptography and watermarking have been highlighted. Possible ways of random image steganography is the major motivation of this review and the same has been enumerated and enunciated with practical examples. As a finishing touch to the stego implementation, the significance of steganalysis has also been highlighted.

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., D. Adharsh, V. Vignesh and R.J.B. Balaguru, 2010. PVD blend with pixel indicator-OPAP composite for high fidelity steganography. Int. J. Comput. Appl., 7: 31-37.

Amirtharajan, R. and R.J.B. Balaguru, 2011a. Covered CDMA multi-user writing on spatially divided image. Proceedings of the Wireless ViTAE Conference, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Amirtharajan, R. and R.J.B. Balaguru, 2011b. Data embedding system. WIPO Patent Application WO/2011/114196. http://v3.espacenet. com/textdoc?DB=EPODOC&IDX=WO2011114196&F=0

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 2011 IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application (IMSAA), December 12-14, 2011, Bangalore, Karnataka, India.

Amirtharajan, R. and J.B.B. Rayappan, 2012. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., (In Press).

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

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

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

Chen, C. and Y.Q. Shi, 2008. JPEG image steganalysis utilizing both intrablock and interblock correlations. Proceedings of the IEEE International Symposium on Circuits and Systems, May 18-21, 2008, IEEE Computer Society Press, Washington, USA., pp: 3029-3032.

Farid, H., 2002. Detecting hidden messages using higher-order statistical models. Proceedings of the IEEE International Conference on Image Processing, September 22-25, 2002, IEEE Computer Society Press, New York, USA., pp: 905-908.

Farid, H. and S. Lyu, 2003. Detecting hidden messages using higher-order statistics and support vector machines. Proceedings of the 5th International Information Hiding Workshop LNCS, Berlin, October 7-9, 2003, Springer-Verlag, pp: 340-354.

Fridrich, J., D. Soukal and M. Goljan, 2005. Maximum likelihood estimation of length of secret message embedded using ±K steganography in spatial domain. Proc. SPIE, 5681: 595-606.

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.

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

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.

Li, B., J. He, J. Huang and Y.Q. Shi, 2011. A survey on image steganography and steganalysis. J. Inform. Hiding Multimedia Signal Process., 2: 142-172.

Liu, Q., A.H. Sung, B. Ribeiro, M. Wei, Z. Chen and J. Xu, 2008. Image complexity and feature mining for steganalysis of least significant bit matching steganography. Inform. Sci., 178: 21-36.

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

Luo, X.Y., D.S. Wang, P. Wang and F.L. Liu, 2008b. A review on blind detection for image steganography. Signal Process., 88: 2138-2157.

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.

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

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on 2^n: 1 platform for users and embedding. Inform. Technol. J.,

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

Pevni, T. and J. Fridrich, 2007. Merging markov and DCT features for multi-class JPEG steganalysis. Proceedings of the SPIE, Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents IX, Jan. 29, SPIE, San Jose, California, pp: 301-313.

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, 2009a. Steganalysis based on difference statistics for LSB matching steganography. Inform. Technol. J., 8: 1281-1286.

Qin, J., X. Xiang, X. Sun and C. Niu, 2009b. A principal feature selection and fusion method for image steganalysis. J. Elect. Imag., 18: 1-14.

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

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

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.

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

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, 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 R.J.B. Balaguru, 2011. OFDM+CDMA+stego = secure communication: A review. Res. J. Inform. Technol., (In Press).

Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. steganalysis. Commun. ACM, 47: 76-82.

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

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.

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.

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.