IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 2, Ver. II (Mar. - Apr. 2018), PP 42-52
www.iosrjournals.org

A Survey on Different Techniques for Covert Communication Using Steganography

Tapan Kumar Hazra[1], Medha Haldar[2], Megha Mukherjee[3], Ajoy Kumar Chakraborty[4]
[1, 2, 3, 4]*Department Of Information Technology, Institute Of Engineering & Management, Y-12, Salt Lake Electronics Complex, Sector- V, Kolkata, India.*
Corresponding Author: Tapan Kumar Hazra[1]

Abstract : *With digitization, data hiding has become more important than ever. Steganography forms an undisputable tool to attain privacy during data sharing. Steganography is the art and science of hiding data within seemingly innocuous data so as to not draw suspicion. This paper provides a survey on steganography, its advantage over cryptography, the types of digital media over which steganography can be applied and the progress of steganographic methods and recent trends in steganography. Images, video, text, audio are the digital media which serve as cover-media through which secret data may be transmitted often by exchanging stego-key.*

Keywords - *cover-media, data hiding, digital media, steganographic technique, stego-key*

Date of Submission: 19-03-2018 Date of acceptance: 02-04-2018

I. Introduction

With the rapid advent of internet, the demand for data to be shared intelligently and online, there has been a subsequent desire for security in these transactions. Protection against data to be illegally shared by third party imposters and for maintaining the privacy and integrity, there has been a requirement for disguising or hiding data. While cryptography deals with protection against data removal, steganography deals with protection against data detection. Cryptography is the art of mangling data so that it cannot be deciphered and subsequent un-mangling with a key. Popularly done on text [1], cryptography is also used on other digital media like images [2-5] or techniques that can be applied in both text and images [6]. Steganography on the other hand is the attempt at hiding data within a medium such that its presence is indiscernible [7]. Some- times both cryptography and steganography are applied to form a robust secure communication system [8]. This paper concentrates on steganography and how it can be achieved [9].

II. What is Steganography

Steganography is a relatively new field in network security that protects sensitive data from cyberespionage. It is the art of concealing information in ways that the said information can be transmitted undetectably [10]. The word steganography has been derived from Greek words, 'steganos' which means covered or secret and 'grafia' which means writing. Thus etymologically steganography means 'covered writing'. Alternatively, steganography can be defined as the veritable art and science of invisible relaying of secret data by hiding it within other seemingly insipid data [11, 12].

III. History of Steganography

Since a long time, people have been hiding information by a number of methods and variations. The Golden age Greeks had first practiced Steganography by melting wax tablets and then inscribing the hidden message on the underlying wood. Wax was reapplied which gave the look of a new, unused tablet. This served their purpose of secret message communication. Later, Germans developed microdot technology. Microdots are photographs of a printed period size having the clarity of standard-sized typewritten pages where the message was neither hidden nor encrypted. It was too small to draw attention to itself and hence, helped in the transmission of large amounts of data. Steganographic technology consisted of invisible inks during early World war II. Milk, vinegar, fruit juices and urine were the common sources of invisible ink which darkened when heated. The evolving methods in this field has sparked a revolution which brings forth different ideas to convey a message secretly. A project was started in Saudi Arabia at the King Abdulaziz City of science and technology, to translate some ancient Arabic manuscripts, which are believed to have been written 1200 years ago, to English which was regarding secret writing. The Italian mathematician Jérôme Cardan reinvented a Chinese

ancient method of secret writing 500 years ago. A paper mask with holes was shared between two parties. It was placed over a blank paper and the sender wrote his hidden message through the holes. The mask was taken off and the blanks were filled so that the message appears as an innocuous text to the third party. This method is called Cardan Grille [10 - 11, 13].

IV. Steganography in Digital Media

Based on the cover media which hides the actual information, there can be five major types of steganographic techniques. They are enunciated below [14]:

Image Steganography. In this technique, image is used as the cover medium. Images are widely used because of large size and redundant data, as a result provides potential places to hide secret data. Depending on the format of the image file, different algorithms are used.

Video Steganography. Video steganography embeds the secret data into a digital video format. Generally used video formats are AVI, H.264, MPEG, MP4 etc. It provides huge cover space to hide payload data.

Audio Steganography. Audio is used as the carrier via which message is relayed. Popularly used digital audio formats include MIDI, WAVE, AVI etc. Like video, it also provides huge cover space for secret payload data.

Text Steganography. Message is hidden within the characters of a text file or within blank spaces.

V. Steganography in Image

The Image Steganography is surveyed from paper [15-17]. Digital images are considered as the most widely used cover objects for steganography where the message remains invisible to the human visual system.

5.1 Image Steganography Keywords

Cover-Image- The image carrying the hidden information.

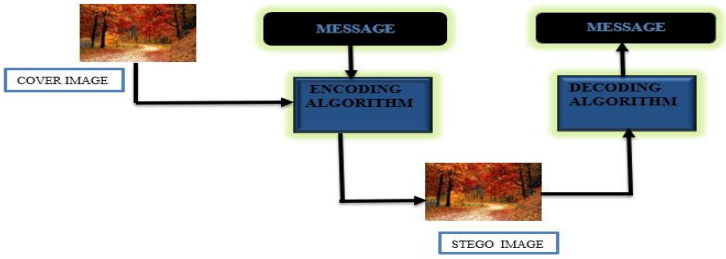
Message or payload - The actual hidden information to be conveyed.

Stego-Image - The resultant image after the hidden message is embedded.

Stego-Key - The key used for the extraction or embedding of the message.

Image steganography is a method of generating stego-image by hiding information into cover-image. This stego-image is then sent to the receiving party by a medium, where the third party is unaware that this stego-image has hidden message. The hidden message can simply be extracted with or without stego-key by the receiving end [18]. Diagram of image steganography is shown in Fig 1.

Fig. 1. Working model of Image Steganography



5.2 Steganographic Quality Measurements

High Capacity: Maximum size of hidden information that can be embedded.

Perceptual Transparency: After embedding information, perceptual quality will be degraded into stego-image [19].

Robustness: After embedding, data should stay in exact form.

Temper Resistance: It is difficult to alter the message after it's embedded.

Computation Complexity: The complexities involved in the process.

Table 1. Parameters and values for measurement

MEASURES	ADVANTAGE	DISADVANTAGE
High Capacity	Higher	Lower
Perceptual Transparency	Higher	Lower
Robustness	Higher	Lower
Temper Resistance	Higher	Lower
Computation Complexity	Lower	Higher

5.3 Techniques of Image Steganography

Following are the most used image steganography techniques are:

- Spatial domain technique
- Masking and filtering

- Transform techniques
- Distortion Techniques

5.3.1 Spatial Domain Technique

In this method, some bits of the cover image is replaced to embed the hidden message to be conveyed secretly. It is a simple technique but is less resistant to attacks like compression. Spatial domain techniques are broadly classified into:

5.3.1.1 Least significant bit (LSB) - It is one of the most common process of steganography where the least significant bits (LSB) of the cover-image are replaced with the message bits. Though, cropping and compression is involved, no obvious effect can be noticed. They are of high capacity. There are chances of hidden data being lost which makes it less robust. The message is prone to attacks.

5.3.1.2 Pixel value differencing (PVD) -The pixel-value differencing (PVD) method proposed by Wu and Tsai provides high capacity and perceptual transparency for the stego-image. The pixel-value differencing (PVD) method partitions the cover image into non overlapping blocks containing two connecting pixels and then modifies the pixel difference in each block (pair) for data embedding where a larger difference allows a greater modification. In the extraction phase, the original range table is used to segment the stego-image by the same method as used to the cover image. Chang et al. proposed using tri-way pixel value differencing for better embedding capacity and PSNR.

The other methods are:-

- Edges based data embedding method (EBE)
- Random pixel embedding method (RPE)
- Mapping pixel to hidden data method
- Labelling or connectivity method
- Pixel intensity based method
- Texture based method
- Histogram shifting methods
- GLM (Gray level modification)
- Quantization index modulation (QIM)
- Multiple-Based Notational System (MBNS)
- The Multi Bit Plane Image Steganography (MBPIS)

5.3.2 Masking and Filtering Technique

This technique hides information by embedding the message in the more significant areas than just hiding it into the noise level to ensure that changes cannot be detected. It can be applied without suffering from lossy compression as they are more integrated into the image. Since the secret information is hidden in the visible parts of the image, it is more robust than LSB technique. It has some disadvantages like this procedure is restricted to gray scale images and 24 bit color images.

5.3.3 Transform Domain Technique

Discrete Cosine Transform (DCT**),** Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are the commonly used transform techniques. This technique hides message in the transform coefficients of the cover image by tweaking the coefficients and inverting the transformation [7]. It makes the technique resistant to attacks. The result can be approximately equal to the original if the chosen coefficient and the sizes are appropriate. There are a number of suggested algorithms. Frequency domain embedding procedure has a stronger effect than time domain embedding. Today, transform domain is preferred for most of the strong steganographic systems [7, 20, 21]. Transform domain techniques hide information in the areas of the cover-image that are less exposed to manipulation. So, this serves as an advantage over LSB technique. Some of these techniques do not depend on the image format and can outrun lossless and lossy format conversions [22].

DCT based Data Hiding. In DCT, 8x8-pixel blocks of the image from spatial domain are transformed into 64 DCT coefficients where each is in the frequency domain. The hidden message is embedded in the LSB of the quantized DCT coefficients. The modification of a single DCT coefficient affects all 64 image pixels. The manipulation happens in the frequency domain, so there are indiscernible visual differences.

Advantage: DCT has the ability to minimize the block-like and the statistical properties of the JPEG files are also preserved.

Disadvantage: Only used on JPEG files. It is so as the statistical distribution is found in JPEG files. Some common DCT based steganography methods are as follows.

JSteg [23] and JPHide [24] are two classic JPEG steganographic tools based on the LSB embedding technique. JSteg performs by replacing the Least Significant Bit of quantized DCT coefficients with the secret message bits. In this way it embeds the message in the cover-image whereas JPHide changes to a process where the

second LSB-plane can also be manipulated. The quantized DCT are selected randomly by a pseudo-random number generator, which can be controlled by a key.
The JPEG file format is the most common image file format because of the small size of resultant [25].
F5 steganographic algorithm manipulated the absolute value of the quantised DCT coefficient by decreasing it by one, in case, modifications are required. The said algorithm was devised by Westfield. It encodes message bits into DCT coefficients chosen randomly and performs matrix embedding reducing the number of changes to achieve the result.

OutGuess was proposed by Neils Provos as UNIX source code in 2011. OutGuess-0.2 is the most talked about outguess. The embedding process of OutGuess is classified into two stages i.e. embedding and post embedding stage. In the former stage, the message bits are encoded in the LSB of the quantized DCT coefficients along a key-dependent walk through the image. After embedding, modifications are done and the histogram of the DCT coefficients are preserved exactly. Chi-square and its versions can't detect OutGuess [26-28].

In Yet Another Steganographic Scheme (YASS) [29], segmentation of an input image (in spatial representation) into fixed large sized blocks called big blocks (or B-blocks). Then, perform randomly selection within each B-block to find an 8 × 8 sub-block known as embedding host block (or H-block) using a key. Then via using error correction codes, secret data is embedded in the DCT coefficients of the H-blocks by QIM. After inversing DCT on the H-blocks, the image is compressed and can be used as a JPEG image.

5.3.4 DWT based Data Hiding

Wavelet-based steganography works on the idea of wavelets. The secret information is stored in the wavelet coefficients of an image. Bits are not manipulated in this case. It transforms spatial domain information to the frequency domain information. The discrete wavelet transform (DWT) method is preferred over the discrete cosine transform (DCT) method, as the resolution provided by the DWT to the image is at various levels [7, 30-35]. Wavelets are mathematical functions that divide data into frequency components so that they are ideal for image compression. They are far better at approximating data with discontinuities than JPEG formats [21].

5.3.5 Distortion Technique

In this technique, the decoding algorithm requires information of the cover-image to find the difference between the original and distorted cover-image to extract the secret message. Information is stored by signal distortion as the encoder incorporates a sequence of manipulations to the cover-image. If the stego-image and cover-image differs, then message bit is 1 else 0. The encoder preserves the statistical properties of the image while modifying the 1 value pixels [35, 36].

VI. Steganography in Audio

Audio steganography attempts to exploit the shortcomings of the Human Auditory System (HAS) by psycho-analysis and embed a secret message within a audio file in such a way that the cover audio suffers least distortion. The cipher media consists of the secret message and a stego-key which is embedded in the carrier audio via a suitable algorithm. The information disguising is done via a twofold process [10, 11]. Identification of redundant bits in a cover-file - Redundant bits are unnecessary bits which can be removed/altered without destroying the integrity of the cover-file. Embedding message in cover audio (Audio file) - To embed the secret data in the audio file, the redundant bits of the cover audio is replaced by the bits of the secret data. Some techniques are discussed below:

6.1 LSB Coding

An audio is a group of bits that hold information about the pitch, frequency etc. LSB Coding is a type of temporal audio steganographic technique which is a very simple but highly susceptible to distortion, technique which substitutes the least significant bit of the cover audio with that of message. The following are the main steps involved in LSB coding [44]:

6.1.1 The bytes of audio file are converted into bit pattern
6.1.2 All the characters of message are converted into bit pattern
6.1.3 Substitute LSB of audio with LSB from character in message.

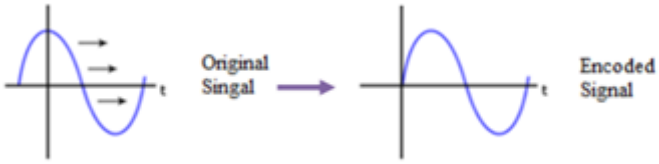
The low complexity is a major advantage while easy detection due to distortion is an obvious disadvantage.

6.2 Phase Coding

In this technique message bits are introduced as phase shift in the phase spectrum of audio signal. Its advantage w.r.t to former is its non-detectability to human ear. Phase coding follows the given procedure [44]:
An original signal is divided into smaller parts such that lengths of those parts are of the same size as the size of the secret data to be embedded. Discrete Fourier Transform (DFT) is applied to create a matrix of the phases.

Phase difference between adjacent parts are calculated. New phase matrix is created with the help of the new phase of the first segment. Reconstruction of original signal by applying inverse DFT and summing up the sound segments.

Fig. 2. Phase Shift Coding



6.3 Parity Coding

Parity coding is one of the robust audio steganographic technique. Instead of dividing the cover signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the message from a parity bit. If the parity bit of a selected sample region does not correlate to the data bit to be embedded, the process inverts the LSB of one of the samples into which signal is divided. Thus, the sender has more liberty.

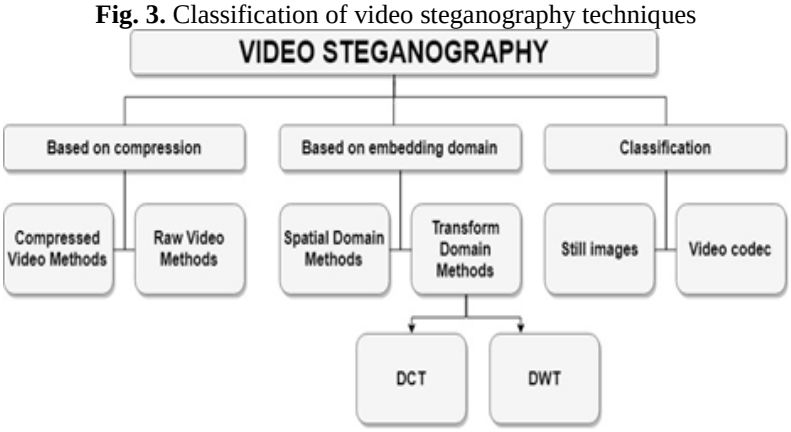
6.4 Spread Spectrum

Spread spectrum communication involves techniques in which a given signal with a narrow bandwidth is deliberately spread in the frequency domain resulting in a wideband signal like white noise. After this, the energy of the given signal in any one frequency band is low practically undetectable. Spread spectrum audio steganography uses a round-about better version of the above to encode a binary message within samples of a low-power white Gaussian noise sequence made up of real numbers. The resulting signal which contains information hidden in noise is perceived as noise and is then added with the cover audio to produce the stego-audio. Since the power of the encoded noise signal is much less than that of the cover audio, the SNR (signal to noise ratio) is low, indicating low perceptibility and low probability of detection by a listener. Subsequently, if embedded signal power is much less than the power of the audio, a listener should be unable to audibly distinguish the original audio from the stego-audio. Also, since the data is embedded using a low-rate error-correcting code, the encoding has a similar spreading effect since data bits are spread across many output bits of the error-correcting encoder [45]. This technique is robust and provide moderate data transmission rate.

VII. Steganography in Video

A video is nothing but a sequence of images. Hence, video steganography can be treated as an extension of image steganography. But as video is more dynamic as opposed to image, it is relatively easier to encode messages within video frames and the distortion is perceptible to the HVS (Human Visual System) [46]. Also, videos have more spatial and temporal redundancy and thus are excellent candidates to serve as cover media [47]. Video steganography can be achieved by various methods which can be classified as shown in Fig 3. As illustrated one basis would be of compression which fall under compressed video steganography techniques [7, 48-51] and uncompressed techniques [46]. Compressed techniques can be lossy but are useful for sending huge amounts of data. In [49] 3-D SPIHT-BPCS steganography and MotionJPEG2000-BPCS steganography was presented in which noise-like regions in a frame were substituted with secret data which theoretically did not deteriorate video quality. Raw video methods are also used to attain steganography albeit more theoretically. In [46] motion component was used to include secret data bits for increasing the ability to resist video compression. Based on the domain of embedding, there can be two methods, i.e., spatial methods [52-54] and transform methods [55-57]. Shirali-Shahreza [55] offered considering video as a sequence of images [52] or finding new formats in videos that could help analyzing the possibility of steganography [50].

Fig. 3. Classification of video steganography techniques



Off late video steganography has gained a lot of attraction from researchers. Reviewed techniques are discussed below:

7.1 Substitution based techniques

These techniques are predominantly used owing to their simplicity and embedding capacity. However, they could be lossy. Several methods under this classification include LSB substitution (Least Significant Bit), BPCS (Bit plane complexity substitution), TPVD (Tri-way Pixel Value Differencing). Eltahir et al. [53] exploited the working of the HVS to modify the traditional LSB technique. Since the eye is more sensitive to change in the blue hue, than its red or green counterparts, they made use of a 3-3-2 technique in which 3 LSBs each from red and green were used and only 2 from blue to retain the integrity of the frames. Despite using 33.3 % of each video frame for data hiding this algorithm is neither very efficient nor robust. Hu in [58] put forth an algorithm for concealing video in video using LSB which has a pre-processing step. Each frame of the secret video goes through a pre-process called non-uniform rectangular partitioning [59]. LSB attempts to replace LSB but as more significant bits are used to maintain the richness of the original secret data, the quality of the cover video reduces. Hence, BPCS and TPVD evolved. BPCS was first presented in [60] in which noise-like regions of the frame hold secret data. The information hiding capacity of true color frame is 50%. On the basis of complexity measure, α, bit planes are classified into natural informative, artificial informative and noise-like portions and then embed simple secret code blocks in the third region [60]. BPCS steganography finds application in the transform as well as the spatial domain. The idea was expanded by Noda in [50]. Another substitution-based technique is the Tri-way Pixel-Value Differencing (TPVD) which is an improvement on the PVD where data bits are hidden in the difference value of two adjacent pixels. The TPVD method embeds data in all horizontal, vertical and diagonal edges improving the hiding capacity greatly [60].

7.2 Transform domain embedding techniques

Transform domain techniques are more complex, but increase the robustness and the apparent transparency of the produced stego-objects. These techniques include some initial steps which are: transforming cover media into frequency domain and then embed the secret data in some or all the coefficients following which the modified coefficients are transformed back to the original form. These transforms are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). DFT produces round off errors and are hence not used commonly [61]. In DCT frame is divided into 8×8 blocks of pixels. From left to right, top to bottom, the DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and secret data is encoded in DCT coefficients [62]. An example of the DWT was put forth by Xu. They embedded the secret message in the motion component of the cover since it is not majorly distorted by compression and is not as sensitive to the HVS. The algorithm is explained below: The motion component is calculated on a frame-by frame basis after which it undergoes two-level wavelet decomposition. Then the data bits are encoded into low frequency coefficients based on the values of coefficients in the corresponding three high frequency sub-bands. This ensures that the message bits are embedded into large motion regions, which further maintains the integrity of the video. One major con of this technique is that it requires a huge motion component (where data is actually encoded) barring which hiding capacity is substantially reduced [52].

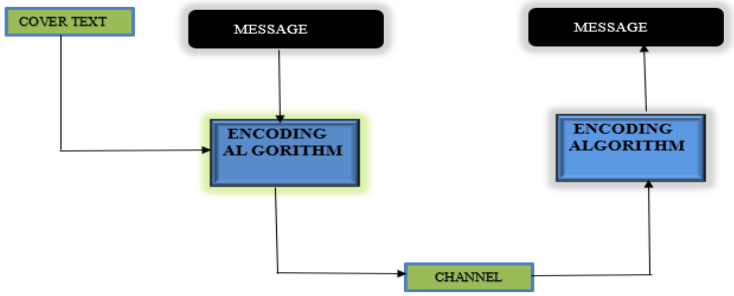
7.3 Format-based techniques

H.264/AVC is one of the newest compression standards for video. Many steganographic algorithms were designed to exploit its structure. Flash video files (.FLV) have a relatively simple structure and is compact. In [63] the format's simple structure was exploited. The secret message was embedded in the video tags. However, it is merely a naïve implementation.

VIII. Steganography in Text

Text steganography model as in Fig. 4, is a bit difficult kind to hide a message because of the lack of redundant information in a text file, while there is a lot of redundancy in a picture or a sound file [37]. In certain media objects like picture, audio etc., the structure of the document is different from what we observe whereas in text document, it is same and any changes made, renders an indiscernible manipulation in the output. Either text or text formatting is changed [38]. A hidden message will be encoded in a cover-text by using an algorithm to produce a stego-text. The stego-text will then be transmitted via a communication channel, e.g. Internet or mobile device to a receiver. The receiver uses a recovering algorithm along with a stego-key to extract the secret message [39].

Fig. 4. Working Model of Text Steganography



Text steganography can be classified into format-based, random and statistical generation, Linguistic method [40].

8.1 Format Based Method

Format Based Method is summarized from [37, 39-41]. Format-based methods use the modification of the cover-text to hide data like insertion of spaces, misspellings, font formatting etc. They do not change any word or sentence, so it does not distort the meaning of the cover-text. However, Bennett proposed that this method cannot trick a computer system. It is an open space method. There are 3 ways of encoding:

8.1.1 inserting spaces after each terminating character
8.1.2 inserting spaces at the end of lines
8.1.3 encoding data involves right-justification of text

8.2 Random and Statistical Generation Method

Random and Statistical Generation Method is surveyed from [39, 40, 42]. Random and statistical generation method is based on character sequences and word sequences. A probabilistic context-free grammar (PCFG) is a language model used to produce words by recursively using transformation rules. Another method is to generate words having same properties like word length and letter frequency of a word in the original message.

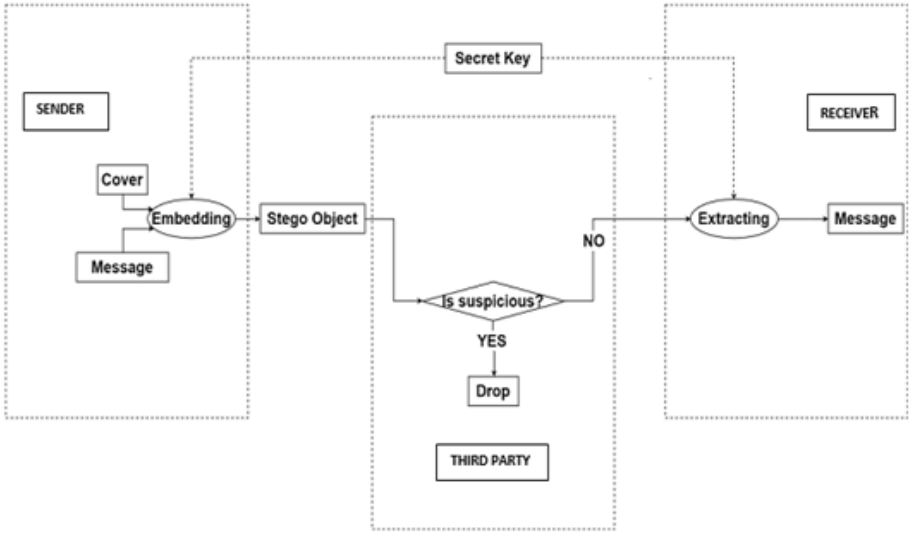
8.3 Linguistic Method

Linguistic method is summed together from [39, 40, 43]. The linguistic method is a method that uses linguistic structure as a place for hidden messages. Syntactic method and semantic method are linguistic methods where some punctuation signs like comma (,) and full-stop (.) are used in the document to embed a message in the former and synonym of words for some pre-selected words are used in the later. Semantic method assigns two synonyms: primary or secondary value and syntactic method needs identification of proper places to insert the secret message.

9 Steganographic Protocols

The following classification of the steganographic protocols are summarized from [64-67]. It is classified into the following:

Fig. 2. Stego-Key working model



9.1 Pure Steganography

Pure Steganography does not require the prior knowledge of the cipher such as a stego-key to start the communication process. The security is entirely depended on the secrecy.

Advantage- No stego-key need to be shared between the communicators.

Disadvantage- Doesn't provide any security if a third party is aware of the encoding algorithm and least secure method to communicate secretly because the sender and receiver depend on the fact that no third party is aware of the secret message.

The pure Steganography quadruple (C, M, D, EX) where each parameter are defined in table 2.

Table 2. The Pure Steganography quadruple

PARAMETER	**STANDS FOR**
C	Set of possible covers
M	Set of secret massage with $\|C\| \geq \|M\|$.
EX	Extracting algorithm
D	Embedding algorithm

9.2 Secret Key Steganography

A secret key Steganography system as shown in Fig. 5, is dependent on the secret key with which the sender embeds the secret message. The one who has knowledge of the key can extract the message. So, exchange of the key between the communication partners is required. No third party can extract the message without the key. The secret key Steganography quintuple (C, M, K, EM, EX) where parameters are defined in table 3.

Table 3. The Secret Key Steganography quadruple

PARAMETER	STANDS FOR
C	Set of covers
M	Set of secret message
K	Set of stego-key
EX	Extracting algorithm
EM	Embedding algorithm

9.3 Public Key Steganography

Public key Steganography consists of two keys for a secure communication:

9.3.1 A private or secret key

9.3.2 A public key

Public key cryptography system is followed for this technique. Exchange of the public keys of the communicators are required. The public key will be used by the sending party during the encoding process and the private key is used to decipher the secret message. It provides multiple layers of security.

10 Application of Steganography

Steganography can be widely used for the transportation of utmost secret data. Steganography is applied in the following areas:

10.1 Modern printers
10.2 Use by Intelligence Service
10.3 Distributed Steganography
10.4 Online challenge
10.5 Ecommerce

11 Conclusion

In this paper, we have reviewed different mediums via which steganography can be done. We have also reviewed the different techniques that can be applied on these mediums and their efficiency. Thus, steganography has stretched boundaries of levels of security and privacy that can be imposed during secure data transmission as data security.

References

[1] T. K. Hazra, R. Ghosh, S. Kumar, S. Dutta and A. K. Chakraborty, "File encryption using Fisher-Yates Shuffle," 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, 2015, pp. 1-7. doi: 10.1109/IEMCON.2015.7344521

[2] T. K. Hazra, S. R. Chowdhury and A. K. Chakraborty, "Encrypted Image Retrieval System: A machine learning approach," 2016 IEEE 7thAnnual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-6.doi: 10.1109/IEMCON.2016.7746351

[3] T. K. Hazra and S. Bhattacharyya, "Image encryption by blockwise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),Vancouver, BC, 2016, pp. 1-6. doi: 10.1109/IEMCON.2016.7746312

[4] T. K. Hazra, N. Kumari, Monica, S. Priya and A. K. Chakraborty,"Image encryption and decryption using phase mask over sinusoidal single and cross grating," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference(IEMCON), Vancouver, BC, 2016, pp. 1-6. doi:10.1109/IEMCON.2016.7746317

[5] N. U. Sheikh, T. K. Hazra, H. Rahman, K. Mustafi and A. K. Chakraborty, "Multi-variable bijective mapping for secure encryption and decryption," 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, 2017, pp. 338-345. doi: 10.1109/IEMECON.2017.8079619

[6] T. K. Hazra, A. Mahato, A. Mandal and A. K. Chakraborty, "A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques," 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, 2017, pp. 137-141. doi: 10.1109/IEMECON.2017.8079577

[7] Hazra, Tapan Kumar, Anurag Anand, Antra Shyam, and Ajoy Kumar Chakraborty "A New Approach to Compressed Image Steganography Using Wavelet Transform.," IOSR Journal of Computer Engineering(IOSR-JCE), volume 17, issue 5 (2015): 53-59

[8] T. K. Hazra, R. Samanta, N. Mukherjee and A. K. Chakraborty, "Hybrid image encryption and steganography using SCAN pattern for secure communication," 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, 2017, pp. 370-380. doi: 10.1109/IEMECON.2017.8079625

[9] Shirali-Shahreza M (2006) A new method for real-time steganography. In: 8th International Conference on Signal Processing

[10] N.F. Johnson and S. Jajodia, "Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, Feb. 1998.

[11] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52.

[12] T. Morkel, J.H.P. Eloff , M.S. Olivier,"An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) ,2005.

[13] Shirali-Shahreza M (2006) A new method for real-time steganography. In: 8th International Conference on Signal Processing

[14] Jonathan Watkins, "Steganography - Messages Hidden in Bits Jonathan Watkins," Dec. 2001

[15] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal,A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier, Journal of Global Research in Computer Science,2 (4), April 2011, 1-16.

[16] Richard Popa, "An Analysis of Steganographic Techniques", 1998.

[17] Pratap Chandra Mandal,Modern Steganographic Technique-A survey, International Journal of Computer Science & Engineering Technology (IJCSET),ISSN : 2229-3345 Vol. 3 No. 9 Sep 2012

[18] W. Bender, D. Gruhl, N. Morimoto, and A. Lu,"Techniques for data hiding", *IBM Systems Journal*, vol. 35,issues 3&4, 1996, pp. 313-336.

[19] Derek Upham. Jsteg, http://zooid.org/~paul/crypto/jsteg/

[20] N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F.Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[21] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52.

[22] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, Image Steganography Techniques: An Overview, International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012.

[23] Allan Latham. Jphide, http://linux01.gwdg.de/~alatham/ stego.html

[24] Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In Proceedings of the 4th Information Hiding Workshop, volume 2137 of LNCS, pages 289{302. Springer, 2001.

[25] Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography:survey and analysis of current methods." Signal Processing Journal. [On line]. 90(3), pp.727-752.

[26] B. Li, J. He, J. Huang, and Y.Q. Shi. (2011, Apr.). "A survey on image steganography and steganalysis." Journal of Information Hiding and Multimedia Signal Processing. 2(2), [Online], pp. 142-172.

[27] A.Westfeld and A. Pfittzmann. "Attacks on steganographic systems- breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned." in Proc. of the 3rd Internet Workshop on Information Hiding, 1999, pp. 61-76.

[28] J. Fridrich, M. Goljan, and D. Hogea. Attacking the outguess. In Proceedings of 2002 ACM Workshop on Multimedia and Security, pages 3{6. ACM Press, 2002.

[29] K. Solanki, A. Sarkar, and B. S. Manjunath. Yass: Yet another steganographic scheme that resists blind steganalysis. In Proceedings of the 9th Information Hiding Workshop, volume 4567 of LNCS, pages 16{31. Springer, 2007.

[30] Ali Al-Ataby and Fawzi Al-Naima. A modified high capacity image steganography technique based on wavelet transform. The International Arab Journal of Information Technology, 7:358–364, 2010.

[31] Bo Yang and Beixing Deng. Steganography in gray images using wavelet. In Proceedings of ISCCSP 2006.

[32] Po-Yueh Chen and Hung-Ju Lin. A dwt based approach for image steganography. International Journal of Applied Science and Engineering, 4:275–290, 2006.

[33] Dr.S.T.Gandhe K.T.Talele and Dr.A.G.Keskar. Steganography security for copyright protection of digital images using dwt

[34] V. Kumar and D. Kumar. Performance evaluation of dwt based image steganography. In Proceedings of Advance Computing Conference (IACC), 2010 IEEE 2nd International, pages 223–228, 2010.

[35] H S Manjunatha Reddy and K B Raja. High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security (IJCSS), 3:462–472.

[36] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. "Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.

[37] W. Bender, D. Gruhl, N. Morimoto, and A. Lu,"Techniques for data hiding", *IBM Systems Journal*, vol. 35,issues 3&4, 1996, pp. 313-336.

[38] M. Hassan Shirali-Shahreza,Mohammad Shirali-Shahreza, New Synonym Text Steganography, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 978-0-7695-32783/08 $25.00 © 2008 IEEE, DOI 10.1109/IIH-MSP.2008.6

[39] L. Y. POR1, B. Delina2, Information Hiding: A New Approach in Text Steganography,7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, April 6-8, 2008.

[40] Y. Kim, K. Moon, and I. Oh, "A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR'03), 2003, pp. 775–779.

[41] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp-685-695.

[42] P. Wayner, "Strong Theoretical Steganography", Cryptologia, XIX(3), July 1995, pp. 285-299.

[43] M. Niimi, S. Minewaki, H. Noda, and E.Kawaguchi, "A Framework of Text-based Steganography Using SD-Form Semantics Model", Pacific Rim Workshop on Digital Steganography 2003, Kyushu Institute of Technology, Kitakyushu, Japan, July 3-4, 2003.

[44] M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", in Proc. 7th IEEE International Symposium on Signal Processing and Information Technology (ISSPIT'07), December 2007, Egypt.

[45] Lisa M. Marvel, Charles G. Boncelet, Jr., and Charles T. Retter, Spread Spectrum Image Steganography.

[46] Sur A, Mukherjee J, "Adaptive data hiding in compressed video domain. In: Computer Vision, Graphics and Image Processing", 2006.

[47] M. Hussain, M. Hussain, "A Survey of Image Steganography Techniques", in, International Journal of Advanced Science and Technology, Vol. 54, May, 2013.

[48] M.M. Sadek, A. S. Khalifa , M.G. M. Mostafa, "Video steganography: a comprehensive review", Springer Science + Business Media, New York, 2014.

[49] Sherly AP, Amritha PP ,"A Compressed Video Steganography using TPVD." Int J of Database Manag Syst 2,2010.

[50] Hideki Noda, Tomonori Furuta, Michiharu Niimi, Eiji Kawaguchi, "Application of BPCS Steganography to wavelet compressed video", 2004.

[51] Jafar Mansouri, Morteza Khademi ,"An Adaptive Scheme for Compressed Video Steganography Using Temporal and Spatial Features of the Video Signal",2009.

[52] Changyong Xu, Xijian Ping, "A Steganographic Algorithm in Uncompressed Video Sequence Based on Difference between Adjacent Frames", 2007.

[53] Eltahir ME, Kiah LM, Zaidan BB, Zaidan AA (2009) High rate video streaming steganography. In: International Conference on Future Computer and Communication (ICFCC 2009) 672–675.

[54] Hanafy AA, Salama GI, Mohasseb YZ (2008) A secure covert communication model based on video steganography. In: Military Communications Conference (MILCOM 2008) 1–6.

[55] Singh S, Agarwal G (2010) Hiding image to video: a new approach of LSB replacement. Int J Eng Sci and Technol 2(12):6999–7003.

[56] Chae JJ, Manjunath BS (1999) Data hiding in video. In: Proceedings of International Conference on Image Processing (ICIP 99) 311–315.

[57] Shou-Dao W, Chuang-Bai X, Yu L A High Bitrate Information Hiding Algorithm for Video in Video.

[58] Hu S, KinTak U (2011) A Novel Video Steganography Based on Non-uniform Rectangular Partition. In: IEEE 14th International Conference on Computational Science and Engineering (CSE) 57–61.

[59] Tak UK, Tang Z, Qi D (2009) A non-uniform rectangular partition coding of digital image and its application. In: International Conference on Information and Automation (ICIA'09) 995–999.

[60] Chang K-C, Chang C-P, Huang PS, Tu T-M (2008) A novel image steganographic method using tri-way pixel-value differencing. J Multimed 3(2):37–44.

[61] Raja, K.B., Chowdary, C.R., Venugopal, K.R. & Patnaik, L.M. (2005) A secure image steganography using LSB, DCT and compression techniques on raw images. In: Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, 170–176.

[62] Dr. Ekta Walia,Payal Jain, Navdeep Navdeep,An analysis of LSB and DCT based Steganography, 2010.

[63] Mozo AJ, Obien ME, Rigor CJ, Rayel DF, Chua K, Tangonan G (2009) Video steganography using flash video (FLV). In: Instrumentation and Measurement Technology Conference (I2MTC'09) 822–827.

[64] A.A.Zaidan, A.W. Naji, Shihab A. Hameed, Fazidah Othman and B.B.Zaidan, " Approved Undetectable-Antivirus Steganography for Multimedia Information in PE-File ",International Conference on IACSIT Spring Conference (IACSIT-SC09) , Advanced

Management Science (AMS), Listed in IEEE Xplore and be indexed by both EI (Compendex) and ISI Thomson (ISTP), Session 9, P.P 425-429.

[65] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji, and S.M.Mohammed," Implementation Stage for High Securing Cover-File of Hidden Data Using Computation Between Cryptography andSteganography", International Conference on Computer Engineering and Applications (ICCEA09), Telecom Technology and Applications(TTA), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, Vol.19, Session 6, p.p 482-489.

[66] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "New Approach of Hidden Data in the portable Executable File without Change the Size of Carrier File Using Distortion Techniques",Proceeding of World Academy of Science Engineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P 493-497.

[67] Sabu M Thampi,Information Hiding Techniques: A Tutorial Review, ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

* Tapan Kumar Hazra1A Survey On Different Techniques For CovertCommunication Using Steganography." IOSR Journal of Computer Engineering (IOSR-JCE) 20.2 (2018): 42-52.