ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/1189
DOI URL: http://dx.doi.org/10.21474/IJAR01/1189

RESEARCH ARTICLE

A CLOSER LOOK AT CATEGORIES OF STEGANOGRAPHY TECHNIQUES.

Jithesh K*, S.B Kishor, P.K Butey.

Manuscript Info

Manuscript History

Received: 12 June 2016
Final Accepted: 19 July 2016
Published: August 2016

Key words:-
Steganogaphy, cryptography, security, direct sequence, hopping.

Abstract

The cryptography and steganography are techniques to provide information security. Both of these techniques are vulnerable to different kinds of attacks. It is obvious that the success rate of an attack is higher in the case of the former since it discloses the very presence of the content though it is encrypted. Why the success rate is high in case of cryptography is associated with human psychology. It prompts man to find out something when the presence of the same is known and hence it can be said that cryptography is more vulnerable to attack than steganography. This attracts researchers and students to select steganography as their area when information security is the matter of concern. This chapter describes the complete details of categories of steganography techniques that can open the door for entering into the world of steganography where secret is embedded in seemingly innocuous cover medium.

Introduction:-

Steganography is an important aspect of information hiding**.** The other side of information security is cryptography. Cryptography or secret writing protects the very content of the confidential communication by encryption whereas steganography or hidden writing that masks the very presence. Steganography is the new version of steganographia reported by Trithemius, in 1462–1516, assumed from Greek. It literally means "covered writing" and is usually known to hide information in other information [1]. The Egyptians used cryptography through their use of hieroglyphics and are considered to be the first users of cryptography. Some hieroglyphics were stylized to be read by someone who knows the presence. This is considered to be the first instance of steganography. Greeks are credited as the first users of steganography in a creative way. Herodotus reported that the conflict between Persia and Greece in the 5th century BC and Greece were saved through the elegant use of steganography. The trouble, and the use of steganography, began after Xerxes began building his new capital at the city of Persepolis. Homer mentioned the use of steganography in his great compilation named Iliad. Chinese used steganography in a different way compared with Greeks. It is reported that Mongolians were overthrown and Ming dynasty get into rule with the help of steganography.

One among the founders of modern cryptography, the monk Johannes Trithemius, had reportedly written a three volume book, Steganographia, in 1500, describes an extensive system for concealing secret messages within innocuous texts. It is considered to be a magical text, and during the 16th century this book was circulated only privately until publication in 1606. The Italian scientist Giovanni Porta contributed to steganography by describing how to hide a secret within a hard-boiled egg by making an ink from a blend of alum and a unit of vinegar to write on the surface of the egg. Girolamo Cardano contributed much to steganography. He was well remembered to his

Corresponding Author:- Jithesh K.

Cardano grille. The other important personnel who contributed much to steganography and cryptography are Blaise de Vigenere, Auguste Kerchoffs, Bishop John Wilkins and Mary Queen of Scots**.** For the past one or two decade steganography has got tremendous interest amongst researchers and still it is continuing. The reasons for the popularity are its simplicity and high security. It can be implemented using different digital areas such as image, audio, video and text and applied in spatial domain, frequency domain and both. In this study we discuss about the different steganography techniques which are currently used in different situations.

Categories of Steganography Techniques:-

In the literatures and text books it is found that basic techniques of steganography were used in the past. Now it is time to move into the digital age. To conceal messages innocuously we have different categories of steganography techniques available and they are:

Substitution system techniques:-

This is a spatial domain technique where the original physical space of the cover image is used for embedding data. It is the simplest one and is extensively used due to its high payload and quality. It replaces redundant or insignificant bits of a cover with the bits from the secret. There are plenty of tools which made use of this technique. There are different types of substitution techniques used. The most often used is least significant bit [LSB] algorithm. In this technique the least significant bits of each pixel of the original image is replaced with bits from the secret. Now substitution technique with mere LSB has become obsolete since the key is known or can be easily checked. However, substitution technique with replacing bits other than LSB is frequently used today.

The LSB-replacement embedding method replaces the right most bit which is least significant (LSB), with secret message bits, but the others replace LSB with certain conditions. In LSBM (matching), if the bit to be replaced does not match the LSB of the cover image, then the pixel value of the corresponding pixel is randomly added by ±1. Unlike LSB replacement and LSBM, which embed message bits of each pixel, LSBMR [3] replaces two pixels at a time. The distortion caused to the cover image is very small. The resistance to steganalysis and image distortion of LSBMR make it more acceptable. In general, the relationship of the size of the secret and the cover image is not taken into consideration and the positions of the bits to be replaced are selected in a pseudorandom fashion. LSBMR-EA [4], an expansion to the LSBMR applies an edge-adaptive mechanism to select the hiding location. Based on the size of secret to be embedded, LSBMR-EA hides the message from sharper edge regions to smoother edge regions. In addition to these, this study has proposed the following substitution techniques like Selected Noise Bit Replacement [5] mechanism which uses a location map to guarantee the correct extraction of the secret data.

The following example illustrate the working of the substitution technique.
10001000 10001110 10100101 10001111
00111000 01101000

Say the secret to be hidden is 63. Its binary representation is 111111
Now, with the help of LSB bit method, the secret message 63 can be inserted into the stego-cover. It is shown below:

- 1 0 0 0 1 0 0 **0**: The left most bit, 0 in bold italics is replaced by a 1 in the secret.
- 1 0 0 0 1 1 1 **0**: The 0 is replaced by a 1, the second bit in the secret.
- 1 0 1 0 0 1 0 **1:** The 1 is replaced by a 1, the third bit in the secret.
- 1 0 1 0 0 1 0 **1**: The 1 is left unaltered because it corresponds to the same bit in the secret.
- 0 0 1 1 1 0 0 **1**: The 1 is left unaltered because it corresponds to the same bit in the secret.
- 0 1 1 0 1 0 0 **0:** The 0 replaced by the last bit, 1 of the secret.

Of the six bytes of pixels, only 4 have been altered, and our secret has been embedded. This is only a small case in point, however there will be huge unwanted spaces in a cover image and it is possible to embed large secret without disturbing the original view of the picture or image. It is a common practice to select a cover image that is most suitable to the information to be concealed. LSB also works well with gray-scale as well as color images.

The main disadvantage of LSB technique is easy to attack. Any naïve intruder can see the secret by extracting the LSBs one by one. Also changing large number of LSBs may affect the original image. Also it is not robust enough to resist against cropping or rotation. The rapid growth and development of information technology and other means of communication prompted a change in steganography approach is emerged and methods that make use of frequency domain came into existence. The following section gives a glance over the frequency domain techniques currently in use.

Transform Domain Techniques:-

The spatial domain deals cover medium as it is seen whereas transform domain or in other words frequency domain deals with the rate of change of pixel values in the spatial domain. In transform domain technique the cover image is first of all converted or transformed into its frequency distribution. Frequency means the number of occurrences or instances in which a variable takes each of its possible values. A given image or signal can be converted between the time and frequency domains with a pair of mathematical operators called a transform [6]. Examples are DCT (discrete cosine transforms), which helps divide the image into parts [7] (or spectral sub-bands) of differing significance (with respect to the image's visual quality), the Fourier transform, which converts the time function into a sum of sine waves of different frequencies and the last one is discrete wavelet transform (DWT) , in which the wavelets are discretely sampled. Its ability to capture both frequency and location information is the key advantage of wavelet transform over Fourier transform.

This technique hides information in the transform space of a signal. Anything in the universe can be represented in the forms of waves that are a function of time, space or some other variables. For example images, pictures or audios etc. This technique can be best explained in terms of JPEG format data transfer. Always JPEG data compress themselves when they close. This happens when they throw out the excess data or bits that are present. While compression the JPEG will make an approximation of it to shrink and that approximation is the real transform space. That change in space is used to insert secret data. [8][9][10]

Spread Spectrum techniques:-

It is a wireless communication mechanism in which signal information is send with a bandwidth rate that is deliberately varied or make it large enough to hold the actual required bandwidth. In other words the data to be transmitted is purposefully varied using a pseudo-noise or pseudo random code independent of the information. This modulation waveform “spread” the original signal energy into a bandwidth greater than the minimum required. The receiver “de-spread” the signal using a harmonized copy of the same pseudo-noise code. The advantage of this technique in using steganography is it requires no original cover image to extract the secret at receiving end. The receiver needs only the stego-key.

A specific but complicated mathematical function is used to vary the signal bandwidth. The receiver is tuned in such a way that it can easily de-spread and intercept the varied signals. The frequency-versus-time function employed by the transmitter, and the starting-time point at which the function begins should be known to the receiver. The spread-spectrum function must be kept out of the hands of unauthorized people or entities to avoid any attack. As the name implies spread spectrum uses wide bandwidth signals seems noise. Since they are noise-like they are hard to identify. They are also hard to intercept. In addition spread spectrum signals are difficult to jam or cease than narrowband signals. The boons of this technique[1] are avoiding jamming, preventing interference, interception probability is very low, CDMA(Code Division Multiple Access),it gives maximum privacy to messages, High Resolution Ranging, Timing Resistance to fading and Accurate low power position finding [11].

Direct Sequence (DS):-

Direct sequence spread spectrum is the easiest one to implement amongst all spread spectrums. It differs with the other spread spectrum process like frequency hopping spread spectrum or frequency hopping code division multiple access (FH-CDMA. It uses a signal bandwidth that is large enough to hold the information signal bandwidth [12]. The thin band message is multiplied with a binary code, often designated as a pseudo-noise (pseudo-random) code (spreading code) to generate the wideband signal that is transmitted [13]. The original information signal can be taken back at the receiver by multiplying [14] the received data signal by the same pseudo-random code (often referred as de-spreading code) used at the transmitting end. In order to recover the intelligence the codes used at both ends must be in synchronism and amplitude should match with each other. The surplus data-rate bit pseudo-noise code helps the signal to thwart intrusion and enables the original data to be recovered if any data is lost or destructed.

Frequency Hopping (FH):-

The large bandwidth spectrum is divided into many possible broadcast frequencies [15]. It uses a different approach. As the name implies it just hops (traversing very actively) from frequency to frequency over a wide band. The code sequence associated determines the order of frequencies occupied and the information rate transmitted determines hopping of the frequency from source to destination. The FH devices are cheaper than DSSS and they use less power, but the performance is not as reliable as that of DSSS [13].

Time Hopping (TH):-

The signal is divided into frames, which in turn are sub divided into M time slots. The message is transmitted only one frame at each time slot and is modulated with information. This time slot is selected using pseudo-noise generator. The PN code generator drives an on-off switch in order to accomplish switching at a given time in the frame.

Hybrid (DS/FH):-

As the name implies this is a blend of direct-sequence and frequency hopping schemes. One data bit is divided over several carrier frequencies [16]. A hybrid DS-FH spreading scheme combines the features of both direct spread and frequency spread techniques to avoid the pitfalls associated with both techniques.

Statistical Methods:-

Statistical methods always communicate only one bit of information. This scheme is often known "1-bit" steganographic scheme. Though a slight one, this scheme hides only one bit of information in a digital carrier, and thus creates a statistical change. “1” indicates a statistical change of the stego-cover and a”0” indicates a stego-cover left unchanged. This system works based on the receiver's ability to distinguish between modified and unmodified covers. Statistical methods are best used for reversing the stego image into its original form.

A practical methodology proposed by Tomas Filler et al. [17] in 2010 uses statistical methods to improve the then existing techniques. Their method can be used in both spatial & transform domain. The paper [18] introduced by Chin-Chen Chang & Chih-Yang Lin in 2006 offered the reconstruction of the original image from stego image after the extraction of the secret. It stands ahead of the traditional reversible schemes for image compressed with VQ (vector quantization).

Distortion Techniques:-

This method of steganography makes appropriate changes to a cover object to hide information so that the embedding of secret may enhance the original view. The secret message is recovered when the algorithm compares the changed, distorted stego-cover with the original. This technique has proved its success in embedding secret inside experimental covers. There are adept codes exist to hide the data confined within tolerable distortion. In their new paper, “Universal distortion function for steganography in an arbitrary domain”, V Holub et al. proposes a universal distortion design named UNIWARD (universal wavelet relative distortion) to hide data in an arbitrary domain. Here the effective distortion is calculated as the sum of relative changes of coefficients in a directional filter bank decomposition of the stego image [19].

Cover Generation Techniques:-

This technique completely differs from other steganographic techniques in such a way that it generates a new cover for each transaction. In a typical system a cover object is selected from available image, audios or video files instead in this technique a new cover object that has never been used, is created to hide a secret message. A new innovation of this technique has been in discussion for last few years but very difficult to implement is creating a cover out of the given secret information. That is the secret data itself becomes the cover.

In Vivek S et al. audio steganography [20] a dynamic audio cover has been generated from the message being transmitted. The secret is divided into blocks of 16 bits. From each block 8 arbitrary bits or first 8 bits are selected straight away to create the cover. A musical context is created here to avoid suspicion. Another study can be seen in the literatures that made use of this technique [21]. Spam Mimic is another example.

Conclusion:-

The different techniques explained above are used in different situations. No single techniques can be good for long. At a point of time a new threat can be a hindrance over using the same method again and again. The main concerns pertaining to steganography are security, payload, robustness and cover image distortion. Each techniques mentioned above has its own pros and cons. Substitution techniques are good in payload but week in security. Frequency domain techniques such as DCT, wavelets transforms etc. are good in security than spatial domain techniques but robustness is week when comparing with spread spectrum techniques whereas spread spectrum techniques are week in payload. So which one is used when is always depends upon the message length and communication environment. A complete solution for information security is yet to be developed. A combinations of aforementioned techniques can be a solution.

References:-

1. Johnson,N.F, Jajodia,S.: Exploring steganography: seeing the unseen, IEEE Computer 31(2), 26–34. (1998).
2. Investigator's guide
3. Mielikainen, J.: LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5): 285–287 (2006).
4. Huang,J. and Luo,W.: Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security, 5: 201–214 (2010).
5. Jithesh K, S.B Kishore, P K. Butey, De-Noise Steganography by Enhancing the Cover Image: A Multi-Level Security Approach, IAJIT [to be published in 2016]
6. Mathwork.
7. https://www.cs.cf.ac.uk/Dave/Multimedia/node231.html
8. X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007).
9. A.I. Hashad, A.S. Madani, A.E.M.A. Wahdan, A robust steganography technique using discrete cosine transform insertion, in: Proceedings of IEEE/ITI Third International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society, pp. 255–264, 2005.
10. R.T. McKeon, Strange Fourier steganography in movies, in: Proceed- ings of the IEEE International Conference on Electro/Information Technology (EIT), pp. 178–182, May 2007.
11. Spread spectrum image steganography, IEEE Transactions on image processing, vol.8,issue8.
12. http://www.freepatentsonline.com/5150377.html
13. Direct sequence spread spectrum (DSSS) communications system with frequency modulation utilized to achieve spectral spreading, United States Patent 5150377.
14. http://www.google.com.jm/patents/US5150377
15. Spread Spectrum Techniques and Technology Mark A. Sturza 3C Systems Company
16. Time hopping spread spectrum, Himanshu Shekhar, term paper of ece-444, 2014
17. Tomas Filler, "Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article,pp.1-17(2010)
18. Chin-Chen Chang & Chih-Yang Lin,"Reversible Steganography for VQ-Compressed Images Using Side Matching and Relocation ", IEEE Transactions on Information Forensics and Security,Vol. 1. No.4, pp 493-501, 2006.
19. V Holub et al,"Universal distortion function for steganography in an arbitrary domain", 2014.
20. Vivek Sampat etal.,Audio Steganography using Dynamic Cover Generation,Volume-2, Issue-4, IJACTE, 2013.
21. Sampat, Vivek, et al. "A Novel Video Steganography Technique using Dynamic Cover Generation." IJCA Proceedings on National Conference on Advancement of Technologies–Information Systems & Computer Networks, 2012.