International Journal of Engineering Innovation & Research
Volume 3, Issue 6, ISSN: 2277 – 5668

A Study on Security Issues in Computer Networks and Steganography Techniques

R. Srinivasan
Prof., & Head, Department of IT,
PSV College of Engg. & Tech., Krishnagiri

V. Saravanan
Prof., Department of IT,
PSV College of Engg. & Tech., Krishnagiri

J. Saranya
PG Scholar, Department of IT,
PSV College of Engg. & Tech., Krishnagiri

***Abstract* – In today's network security is the important issues which has to be solved. The technique like cryptography alone is not sufficient for the current need. Message hiding is the important factor in security. The performance of the message hiding technique is mainly based on the security. The security of the message hiding should be high such as no hacking or vulnerability happen in the process. The three factors capacity, detective distortion and the security should be there for better performance. The capacity can increase or decrease but the security should not decrease, the message hiding should be selected in this criteria. Steganography is one of the best message hiding techniques and this paper presents a detailed study on Security Issues and Steganography Techniques**

***Keywords* – Security, Cryptography, Steganography, Image.**

I. INTRODUCTION

Steganography is the craftsmanship or practice of covering or disguising a message, picture or document inside an alternate message, picture or record. The saying steganography consolidates the old greek words steganos signifying "secured, hid, or ensured", and graphein signifying "written work" [12]. By and large, the concealed messages will have all the earmarks of being something else: images, articles, shopping records, or some other spread content. For instance, the concealed message may be in imperceptible in the middle of the obvious lines of a private letter.

The principle prerequisite of steganography is imperceptibility which approximately implies that no calculation exists which can focus, whether a message contains a shrouded message or not. Steganalysis is the methodology of identification of steganographic communications. Since steganography and steganalysis are nearly interlaced a portion of the accompanying examination will waver somewhere around one and the other.

Steganography incorporates the camouflage of data inside machine files. Computerized steganography electronic communications may incorporate steganographic coding within a vehicle layer, for example, an archive document, picture record, program or protocol. Media files are perfect for steganographic transmission on account of their substantial size. Case in point, a sender may begin with a harmless picture record and conform the shade of each 100th pixel to relate to a letter in the alphabet, a change so unpretentious that somebody not particularly searching for it is unrealistic to perceive it.

The initially recorded utilization of steganography has been followed back to 440 BC when Herodotus notice two illustrations in his Histories. Demaratus sent a cautioning around an imminent assault to Greece by composing it specifically on the wooden support of a wax tablet before applying its beeswax surface. Wax tablets were in like manner utilize then as reusable composition surfaces, frequently utilized for shorthand.

Advanced steganography arised to the world in 1985 with the assistance of the Pcs being connected to established steganography issues. Advancement after that was moderate, however has since taken off, passing by the substantial number of steganography software accessible:

1) Concealing messages inside the most reduced bits of uproarious images or sound files.
2) Concealing data inside encrypted data or inside arbitrary data. The data to be disguised are initially encrypted before being utilized to overwrite some piece of a much bigger block of encrypted data or a block of irregular data Chaffing and winnowing.
3) Mimic capacities change over one file to have the factual profile of an alternate. This can avert measurable routines that help brute-force attacks.
4) Concealed messages in altered executable files, abusing repetition in the focused on guideline set.
5) Pictures embedded in video material (alternatively played at slower or quicker speed).
6) Injecting subtle postponements to parcels sent over the network from the keyboard. Defers in key presses in a few applications (telnet or remote desktop programming) can mean a deferral in bundles, and the deferrals in the parcels can be utilized to encode data.
7) Changing the request of components in a set.
8) Content-Aware Steganography conceals data in the semantics a human client appoints to a datagram. These frameworks offer security against a non-human enemy/superintendent.
9) Blog-Steganography. Messages are fractionalized and the (encrypted) pieces are included as remarks of stranded web-logs (or pin sheets on social network platforms). For this situation the determination of websites is the symmetric key that sender and beneficiary are utilizing; the carrier of the hidden message is the entire blogosphere.
10) Modifying the reverberation of a sound file (Echo Steganography).
11) Secure Steganography for Audio Signals.
12) Image bit-plane unpredictability division steganography including data in disregarded segments of a file, for example, after the intelligent end of the carrier file.

International Journal of Engineering Innovation & Research
Volume 3, Issue 6, ISSN: 2277 – 5668

II. Basics of Digital Image

Advanced image are electronic previews taken of a scene or filtered from archives, for example, photographs, manuscripts, printed texts, and artwork [11]. The advanced image is inspected and mapped as an issue of dabs or picture components (pixels). Every pixel is appointed a tonal worth (black, white, shades of gray or shade), which is spoken to in binary code (zeros and ones). The binary digits ("bits") for every pixel are put away in a grouping by a computer and frequently diminished to a scientific representation (layered). The bits are then deciphered and read by the computer to create an analog variant

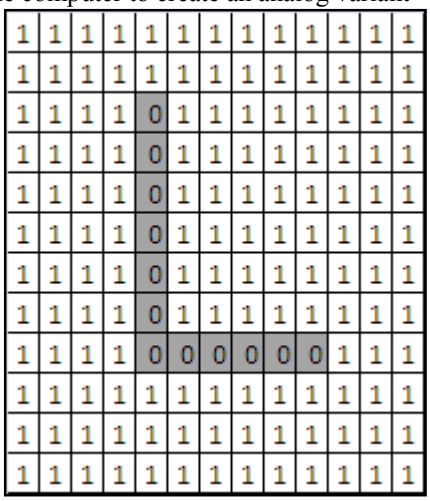

Fig.1. Bitonal Image

As shown in the above picture image, each pixel is assigned a tonal value, in this example 0 for black and 1 for white.

A. Pixel Dimension

These are the even and vertical estimations of an image communicated in pixels [10]. The pixel measurements may be controlled by duplicating both the width and the stature by the dpi. An advanced cam will likewise have pixel measurements, communicated as the quantity of pixels on a level plane and vertically that characterize its determination (e.g., 2,048 by 3,072). Ascertain the dpi attained by isolating a report's measurement into the comparing pixel measurement against which it is adjusted. A 8" x 10" report that is filtered at 300 dpi has the pixel measurements of 2,400 pixels (8" x 300 dpi) by 3,000 pixels (10" x 300 dpi).

B. Bit Rate

Bit rate is controlled by the quantity of bits used to characterize every pixel. The more prominent the bit profundity, the more prominent the quantity of tones (grayscale or color) that can be spoken to [9]. Computerized images may be delivered in black and white (bitonal), grayscale, or color.

A bitonal image is spoken to by pixels comprising of 1 bit every, which can speak to two tones (regularly black and white), utilizing the qualities 0 for black and 1 for white or the other way around.

A grayscale image is made out of pixels spoke to by different bits of information, normally going from 2 to 8 bits or more.

C. Color depth

Color depth, otherwise called bit depth, is either the quantity of bits used to show the color of a solitary pixel, in a bitmapped image or videoframe support, or the quantity of bits utilized for each one color part of a solitary pixel [9]. Color depth is stand out part of color representation, communicating how finely levels of color can be communicated; the other perspective is the manner by which expansive a scope of colors can be communicated. The meaning of both color accuracy and array is expert with a color encoding particular which allocates a digital code worth to a location in a color space.

D. File Size

File Size is figured by reproducing the surface range of an archive (height x width) to be filtered by the bit depth and the dpi [8]. Since image file size is spoken to in bytes, which are made up of 8 bits, partition this figure by 8. File Size = (height x width x bit depth x dpi)/ 8.

On the off chance that the pixel measurements are given, increase them by one another and the bit depth to focus the quantity of bits in an image file. Case in point, if a 24-bit image is caught with a digital cam with pixel measurements of 2,048 x 3,072, then the file size equivalents (2048 x 3072 x 24)/8, or 18,874,368 bytes. File Size = (pixel measurements x bit depth)/ 8.

III. Basics of Digital Video

Digital video is a kind of digital recording system that works by utilizing a digital instead of a simple video signal [7].

Digital video includes an arrangement of orthogonal bitmap digital images showed in quick progression at a consistent rate. In the connection of video these images are called frames. We measure the rate at which casings are shown in frames for every second (FPS).

A. Frame rate

Since each frame is an orthogonal bitmap digital image it contains a raster of pixels. In the event that it has a width of W pixels and a height of H pixels we say that the casing size is Wxh [6].

Frame Size = WxH

B. Pixel Representation and Color depth

Pixels have stand out property, their color. The color of a pixel is spoken to by a settled number of bits [7]. The more bits the more inconspicuous varieties of colors can be repeated. This is known as the color depth (CD) of the video. An illustration video can have a span (T) of 1 hour (3600sec), a frame size of 640x480 (Wxh) at a color depth of 24bits and a frame rate of 25fps. This illustration video has the accompanying properties:

Pixels per frame = 640 * 480 = 307,200.

Bits per frame = 307,200 * 24 = 7,372,800 = 7.37mbits.

Bit rate (BR) = 7.37 * 25 = 184.25mbits/sec.

Video size (VS) = 184mbits/sec * 3600sec = 662,400mbits = 82,800mbytes = 82.8gbytes [13].

C. Bit Rate and File Size

The most critical properties are bit rate and video size [7]. The recipes relating those two with all different properties are:

pixels_per_frame = W * H
pixels_per_second = W * H * FPS
bits_per_frame = W * H * CD

IV. STEGANOGRAPHY TECHNIQUES

Steganography has been broadly utilized including as a part of late recorded times and the present day [12]. Known samples include:

1) Hidden messages inside wax tablets
2) In the beginning of the printing press, it was regular to blend diverse typefaces on a printed page because of the printer not having enough duplicates of a few letters generally. As a result of this, a message could be hidden utilizing 2 (or more) diverse typefaces, for example, ordinary or italic.
3) During World War II, the French Resistance sent a few messages composed on the backs of dispatchs utilizing imperceptible ink.
4) Hidden messages on paper written in mystery inks, under different messages or on the clear parts of different messages.
5) Messages written in Morse code on weaving yarn and afterward weaved into a bit of garments worn by a messenger.
6) Messages composed on envelopes in the zone secured by postage stamps.
7) During and after World War II, undercover work operators utilized photographically created microdots to send data over and over again. Microdots were commonly minute, roughly short of what the extent of the period delivered by a . World War II microdots required to be inserted in the paper and secured with a glue, for example, collodion. This was intelligent and subsequently perceptible by survey against looking light. Elective systems included embeddings microdots into openings cut into the frame of post cards.

Fig2. Tree image with a steganographically hidden image.

The hidden image is shown below

Fig.3. Image of a dog extracted from the tree image above.

D. Digital messages

The hidden image is uncovered by evacuating everything except the two slightest huge bits of each one shade part and a subsequent normalization. The figure 2 covers the image of the figure 3 by message hiding technique.

Modern steganography entered the world in 1985 with the advent of the personal computers being applied to classical steganography problems [5]. Development following that was very slow, but has since taken off, going by the large number of steganography software available:

1) Concealing messages within the lowest bits of noisy images or sound files.
2) Concealing data within encrypted data or within random data. The data to be concealed are first encrypted before being used to overwrite part of a much larger block of encrypted data or a block of random data
3) Mimic functions convert one file to have the statistical profile of another. This can prevent statistical methods that help brute-force attacks.
4) Concealed messages in tampered executable files, exploiting redundancy in the targeted instruction set.
5) Pictures embedded in video material (optionally played at slower or faster speed).
6) Injecting imperceptible delays to packets sent over the network from the keyboard. Delays in keypresses in some applications (telnet or remote desktop software) can mean a delay in packets, and the delays in the packets can be used to encode data.
7) Changing the order of elements in a set.
8) Content-Aware Steganography hides information in the semantics a human user assigns to a datagram. These systems offer security against a non-human adversary/warden.
9) Blog-Steganography. Messages are fractionalized and the (encrypted) pieces are added as comments of orphaned web-logs (or pin boards on social network platforms). In this case the selection of blogs is the symmetric key that sender and recipient are using; the carrier of the hidden message is the whole blogosphere.
10) modifying the echo of a sound file (Echo Steganography).
11) Secure Steganography for Audio Signals.
12) Image bit-plane complexity segmentation steganography, Including information in ignored sections of a file, for example, after the intelligent end of the carrier file.

E. Digital text

Making text the same color as the foundation in word processor documents, e-mails, and discussion posts.

Using Unicode characters that resemble the standard ASCII character set. On most systems, there is no visual difference from normal text. Some systems may show the text styles differently, and the extra information would be easily spotted.

Using hidden (control) characters, and redundant use of markup (e.g., empty bold, underline or italics) to embed information inside HTML, which is visible by examining the document source. HTML pages can contain code for extra clear spaces and tabs toward the end of lines, and colors, textual styles and sizes, which are not visible when displayed.

Using non-printing Unicode characters Zero-Width Joiner (ZWJ) and Zero-Width Non-Joiner (ZWNJ). These characters are used for joining and detaching letters in Arabic, yet can be used in Roman alphabets for hiding information because they have no meaning in Roman alphabets: because they are "zero-width" they are not displayed. ZWJ and ZWNJ can represent "1" and "0".

F. Social Steganography

In communities with social or government taboos or censorship, people use cultural steganography: hiding messages in saying, popular culture references, and other messages that are shared freely and assumed to be monitored [4]. This relies on social context to make the underlying messages visible just to certain readers. Examples include.

Hiding a message in the title and context of a shared video or image.

Misspelling names or words that are prominent in the media in an offered week, to recommend an interchange importance.

G. Network

All information hiding strategies that may be utilized to trade steganograms in telecommunication networks can be ordered under the general term of system steganography [3]. This classification was initially presented by Krzysztof Szczypiorski in 2003. As opposed to the normal steganographic methods which use digital media (images, audio and video files) as an issue for hidden information, system steganography uses correspondence conventions' control components and their essential characteristic usefulness. As an issue, such methods are harder to locate and dispense with.

Ordinary system steganography methods include adjustment of the properties of a solitary system convention. Such adjustment can be connected to the PDU (Protocol Data Unit), to the time relations between the traded Pdus, or both (hybrid methods).

System steganography covers an expansive range of methods, which incorporate, among others: Steganophony - the covering of messages in Voice-over-IP discussions, e.g. the business of postponed or ruined packets that would ordinarily be disregarded by the recipient (this system is called LACK - Lost Audio Packets Steganography), or, on the other hand, hiding information in unused header fields.

Wlan Steganography – transmission of steganograms in Wireless Local Area Networks. A functional case of WLAN Steganography is the HICCUPS framework (Hidden Communication System for Corrupted Networks)

H. Printed

Digital steganography yield may be as printed documents. A message, the plaintext, may be initially encoded by conventional means, creating a ciphertext [12]. At that point, a harmless covertext is adjusted somehow to contain the ciphertext, bringing about the stegotext. Case in point, the letter size, separating, typeface, or different attributes of a covertext can be controlled to convey the hidden message. Just a beneficiary who knows the procedure utilized can recoup the message and after that unscramble it.

The ciphertext created by most digital steganography techniques, on the other hand, is not printable. Customary digital techniques depend on annoying noise in the channel record to hide the message, all things considered, the channel document must be transmitted to the beneficiary with no extra noise from the transmission. Printing presents much noise in the ciphertext, by and large rendering the message unrecoverable. There are techniques that address this confinement; one striking sample is ASCII Art Steganography.

V. Advantages of Steganography

The playing point of steganography is that we can hide a secret message in an alternate message; it can be text, image, audio, or whatever media you choose to hide your secret in [12]. The fundamental issue with this is that possibly you or the individual you're sending the "secret" message to need to have the capacity to discover the message. And on the off chance that you can think that it, then the crackers from whom you need to keep the message a secret can likewise discover it.

Some different points of interest are

1) It is utilized as a part of the method for hiding not the information however the password to achieve the information.
2) Difficult to discover .Only collector can distinguish.
3) Can be connected distinctively in digital image, audio and video files.
4) It is possible quicker with the bigger number of softwares.

VI. Criteria for Measuring The Performance of The Steganography Techniques

A. Improving the Capacity

The execution of the steganography procedure is mostly focused around one of the variable that is limit. The Capacity ought to be higher and likewise there ought to be slightest deductive mutilation so as the steganography system is more secure.

The application of Wavelet Transform and Genetic Algorithm is a novel steganography plan utilized for expanding the capacity of the hiding the messages. The hereditary calculation based mapping capacity is utilized to implant information as a part of Discrete Wavelet Transform Coefficient in 4 x 4 pieces on the spread image. The ideal pixel alteration procedure is connected in the wake of implanting the message. The recurrence space is utilized to enhance the strength of steganography and, we actualize Genetic Algorithm and Optimal Pixel Adjustment Process to get an ideal mapping capacity to diminish the distinction lapse between the spread and the stego-image, thusly enhancing the hiding capacity with low distortions [2].

The greater part of the steganographic algorithms offer a high capacity for hidden messages, however are feeble against visual and statistical attacks. Devices withstanding these attacks give just a little capacity. The calculation F4 consolidates both the safety against visual and statistical attacks and in addition high capacity. Lattice encoding and permutative straddling empower the client to diminishing the essential number of steganographic changes and to even out the installing rate in the steganogram. F5 performs a steganographic extent that surpasses 13 % of the JPEG record size.

B. Minimizing the Detective Distortion

The other imperative we ought to look into is the detective distortion in the steganographic strategy. The distortion implies that is the change of the first substance (image,video..). On the off chance that the stegno image is appearing to be comparable as the first image and the distinction must be discovered utilizing any lenses or somewhere in the vicinity then the distortion is said to be less. So the programmers can't find the secret in it. Anyway if the distortion is all the more then the programmers can undoubtedly discover it. So least detectable distortion ought to be there in the steganograophic technique.

There are numerous techniques utilized for this steganography. Jsteg overwrites the LSB of the quantized DCT coefficient by the secret message and adjust the histogram statistical properties of the coefficients in effectively detectable ways. Outguess holds around 50% of the accessible coefficients with the end goal of rectifying the statistical deviations in the worldwide coefficient histogram brought about by changing Lsbs in the other half, so its steganographic capacity is decreased by about half. Despite the fact that F5 keeps up the DCT coefficient histograms well, its installing operation would bring about shrinkage and still change the histograms of the coefficients in a detectable manner. The DCT coefficient histogram statistical properties as the fundamental attributes of JPEG image, are constantly used for steganalysis.

So how to devise new installing system that could save the DCT coefficient histogram factual properties without giving up the message capacity is of extraordinary investment [1].

Minimizing the distortion on cover media and enhancing the capacity is a paramount route for improving the security of steganographic techniques. Disorder coding can clearly enhance the installing proficiency and decrease the quantity of fundamental change and reduction the inserting effect. Lattice encoding is the first coding plan that is joined to enhance installing productivity in steganographic techniques. Filler et al proposed the STC system (Syndrome-Trellis Codes) in reference. The STC technique can attain higher detective distortion than lattice encoding. In view of the above investigation ,we propose another JPEG steganographic system which enhances inserting productivity by utilizing the STC and jelly the first request statistics(histogram) of DCT coefficients via compelling the extent that are utilized for data installing among the coefficients with indisputably the worth equivalent to one. Trial results demonstrate that, contrasted and Jsteg and F5, the proposed technique attains prevalent execution both in capacity and detective distortion, and opposes to histogram factual steganalysis [2].

C. Improving Security

Security is a vital element in message hiding. The execution of the Steganographic technique is principally focused around the Security. The security of the message hiding ought to be high, for example, no hacking or vulnerability happen the whole time. The three elements capacity, Detective distortion and the security ought to be there for better execution. The capacity can build or diminishing yet the security ought not diminish, the steganographic technique ought to be chosen in this criteria. All these three elements are subject to one another. Consolidating the steganography with cryptographic technique will give more security in the message hiding.

VII. CONCLUSION

In computer networks security is the challenging issue today. To solve this security issue the cryptography or steganography alone is not sufficient. Hence both cryptography and steganography has to be integrated with each other for better security. This paper highlighted the features of steganography and insisted the importance of steganography.

REFERENCES

[1] YE Xueyi, Lu Guopeng , Wang Yunlu And Zhang Yan. (2013, January 10), “A JPEG Steganographic Method Based On Syndrome-Trellis Codes”, Journal of Theoretical and Applied Information Technology, Vol. 47, No.1, pp194-200.

[2] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi. (2011, March 16 - 18), “High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm”, Proceedings of the International MultiConference of Engineers and Computer Scientists Vol I.

[3] Patrick Philippe Meier (5 June 2009). "Steganography 2.0: Digital Resistance against Repressive Regimes". Available: http://irevolution.net/2009/06/05/steganography-2-0-digital-resistance-against-repressive-regimes/

[4] Boing Boing. (2013, May 22), “Social Steganogrphy: how teens smuggle meaning past the authority figures in their lives” . Available: http://boingboing.net/2013/05/22/social-steganography-how-teen.html.
[5] “The origin of Modern Steganography”. Available: http://www.mikebarney.net/stego.html
[6] Andrew B. Watson (1986), "Temporal sensitivity", Handbook of Perception and Human Performance (Wiley).
[7] http://en.wikipedia.org/wiki/Digital_video
[8] https://www.library.cornell.edu/preservation/tutorial/intro/intro-06.html
[9] https://www.library.cornell.edu/preservation/tutorial/intro/intro-04.html
[10] https://www.library.cornell.edu/preservation/tutorial/intro/intro-03.html
[11] https://www.library.cornell.edu/preservation/tutorial/intro/intro-01.html
[12] http://en.wikipedia.org/wiki/Steganography
[13] http://www.gettingyouconnected.com/the-top-3-issues-affecting-todays-large-computer-networks/