Steganography: Current Methods and Attacks

Manoj Kumar[1], Lucky Rajput[2],

[1]*MCA, CCSIT, Teerthanker Mahaveer University, Moradabad*

[2] *Assistant Professor, CCSIT, Teerthanker Mahaveer University, Moradabad*

[1]mk25548@gmail.com

[2]lucky06jpn@gmail.com

Abstract: In the era of security transmitting information over the network securely is one of the concern. Steganography helps us in hiding the information such as data, files, images, text into other medium so that it is prevented from unauthorized access. The daily growth in number of internet users and communication through public network has led to excellence growth in use of steganography. Digital images has high frequencies on the internet, so these are widely used in compare to other file formats. It is very difficult to detect an image by any software, so the images can be used as a major tool of hacking and other security attacks. This paper provides an overview of image steganography, and its methods. And also try to identify some negative impacts of image steganography which leads to cyber crimes and various types of security attacks.

Keywords: **steganography, security attacks, confidential data , unauthorized access**

I. INTRODUCTION

Due to advancement in internet facilities and communication technologies it is essential to implement a system to securely transmit confidential data over the network. Steganography provides a basic approach for hiding confidential data. The original meaning of steganography is secret or covered writing. Steganography is a technique of hiding information in any kind of media like text, image, audio, video etc. which aims to hide data in such a way that the data may reach its intended destination and safe from the unauthorized acess. Like watermarking and cryptography the steganography is used for maintain the security of the secret data but it is much effective than others. In compare to other media images are the most widely used for staganographic purpose because it consists of more redundant information and can be easily sent through communication channel. Images contain variation in luminance of coloured vectors at higher frequency end to the visual spectrum which cannot be detect by human eye. An ordinary person which is not directly involved with the secret information will usually find it a ordinary picture or data.

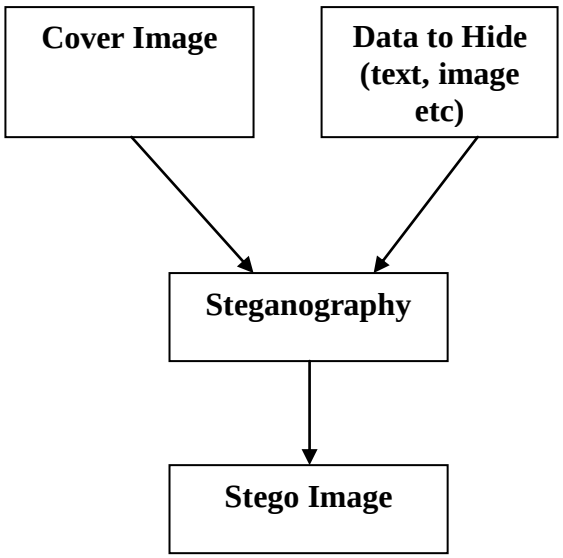

Fig 1 (Steganography Procedure)

II. TYPES OF IMAGE STEGANOGRAPHY

Image Steganography are categorized into two main categories which are mentioned as follow:

A. *Spatial Domain Based Steganography:*

In this technique contents of cover image(pixel values) modified directly to hide the secret information. This technique is easy to implement it has high embedded capacity. The spatial Domain steganography contains several techniques.

B. *LSB(Least Significant Bit) Substitution*

In LSB substitution technique the secret information is embedded in images by changing the right most bits or least significant or 8 th bit of pixel without affecting the original pixel value of image. Hiding the information in LSB's technique gives better performance in all the

parameters and the safe technique for hiding secret information. Consider a 24- bit image, a bit of each of the red, green, blue color(RGB) component can be used.
In a RGB image, information is hidden in the LSB[s] of the RGB values of each pixel. In a 24-bit bitmap, each pixel represented by 3 bytes.
8 bits represent 2^8=256 shades of RED, 256 shades of GREEN and 256 shades of BLUE.

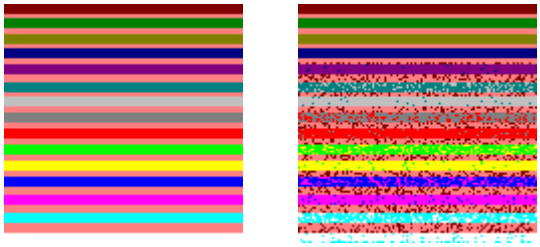

Fig. 2. Original 8-bit cover image (left), and the 8-bit stego-image (right) created With LSB.

C. *Pixel Value Differencing Technique*

This technique is the enhancement in the LSB(Least Significant Bit) technique. This technique divided the cover image into many overlapping units. It provides both high embedding capacity and outstanding imperceptibility for the stego-image. There is 24-bits per pixel color images are used where two LSB of one channel indicates the presence of data in the other two channels(indicator channel and the embedding channel). For choosing the selction channel, key is derived from the size of secret data.

D. *Pixel*

Indicator Method: It is much complex method of embedding data in digital image. This technique is use the concept of hiding the data using the difference between the pixel values. So this technique provides a better quality stego image in compare to other traditional methods with maintaining high embedded capacity.

E. *Singular Value Decomposition Method*

This is the technique of embedding data either in left singular vector, right singular vector, singular values or may be the consists of Spatial and Transform domain. This technique divides cover image into many block for embedding secret information. This technique provides protection against cropping attack, compression attack and Impulse noise attacks.

F. *Histogram Shifting Method*

A histogram is a graph used for graphical representation of the image. A histogram is useful in identifying pixel distribution, colors destiny and tonal distribution. This technique is used in order to extract or modify a certain group of pixels from an image. In histogram the highest value is known as maxima and the lowest value is known as minima. This technique divides cover image is into blocks to generate the respective peak for each block which provides more hiding capacity into more blocks.

G. *Transform or Frequency Domain Steganography:*

Every digital image contains two types of frequencies, low frequency and high frequency. Lower frequencies represent smooth and plane areas and edges are represents with high frequencies. The pixel values of image are transformed into the frequency coefficient is performed by Transformation Domain Steganography.
This technique is also called Frequency domain steganography. This technique consists of two transformation techniques.

H. *Discrete Cosine Transform(DCT)*

Discrete Cosine Transform is a data compression technique and used to convert the uncompressed image into JPEG compression. For compressing any digital image into JPEG format, the RGB colour representation is converted to a YUV representation. There is the Y component refers to the luminance (or brightness) and the U and V components refer to chrominance (or colour).
The DCT transforms a signal into a frequency domain from image domain, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT coefficients each in frequency domain.

I. *Discrete Wavelet Transform(DWT)*

Discrete Cosine Transform splits the signal into set of basic functions to provide the best result of image transformation. In DWT stores the information in the wavelet coefficients of an image, instead of changing bits of the actual pixels. There is the original signal(1-D, 2-D, 3-D) is transformed using predefined wavelets and it improve the capacity and robustness of the information hiding system features.

Table 1: A comparative study of image steganography techniques

Features	LSB	DCT	DWT
Invisibility	Low	High	High
Payload capacity	High	Medium	Low
Robustness	Low	Medium	High
PSNR	High	High	Low
MSE	Low	Low	High

The **PSNR** is Peak Signal to Noise ratio shows the image quality after hiding the data.
The **MSE** is the Mean Square Error is also use to evaluate the image quality.

III. IMAGE STEGANOGRAPHY IN HACKER WORLD

Where the steganography is play a vital role in embedding secret information in images to prevent it from unauthorized access. But on the other hand it also leads to cyber crime and various security attacks like 'phishing attack'. According to some reports and news the image steganography is used as a major tool for stealing information, floating viruses and in many more security attacks because it is very difficult to detect any image by any software. There are some areas where the attackers are using steganography in a fraudulent manner as follows:

A. *Attackers embedding back doors into image files*

Hackers are using a way to maintain access to an already compromised server by hiding backdoors inside headers of legitimate image files. This is a curious steganographic technique to hide the malware. If the web server is once compromised, hackers will modify EXIF header of image and upload that image. At this stage the image renders as normal image, so mostly no one can notice anything.

However the compromise discovered the server's security tightened, then the image provides a firm hold that the attackers will later use for regaining access.

Fig3 Backdoors into image files

B. *Steganography meets VoIP in hacker world*

Hackers are implementing programs and tools in order to execute a new data- leak threat, that is '**Sneaking Proprietary Information**', by hiding within VoIP (Voice over Internet Protocol) traffic. VoIP is used mostly in audio steganography, VoIP steganography conceals secret data within VoIP streams without severly degrading the quality of calls.
There are three basic ways used in VoIP steganography.

- For carrying secret message unused bits within internet protocols i.e. RTP(real time transport protocol) and UDP (user datagram protocol) are used in calls.
- The quality of data should be maintained which is hided inside each voice payload.
- Extra and deliberating distorted packets within VoIP flow, calls are used.

IV. TROJANIZED ANDROID GAMES HIDE MALICIOUS CODE IN IMAGES

In Google Play there are lot of games had functionality like Trojen that allow them to

download and execute the malicious code which is embedded in the images.

Google implemented various checks and it included an automated scanner known as Bouncer which is used for the emulation and behaviour-based detection. Bypassing Bouncer detection is not impossible, but it is very hard to keep most malware creators away. Most Android Trojens are distributed through third party, targeting users who installed apps from unknown sources.

The Trojanized games are functional, but in background they collect identifying information from device. It can be IMEI and IMSE number, MAC address of device, mobile operator, language setting, OS version and many more.

V. HACKERS HIDE STOLEN PAYMENT CARD DATA INSIDE WEBSITE PRODUCT IMAGES

Attackers compromise online shopping sites to skim payment card details and increasing the sophistication. This technique involves hiding malicious code and stolen information form payment card during online transactions.

Researchers form Sucuri(A web security firm) investigated an online shop, and noticed that one of core file of that site, called Cc.php, has been modified recently.

This technique of hiding data inside files with unsuspicious extensions, such as image files is intended to avoid detection.

Fig4 Steaing of Payment card detail

VI. HACKERS HIDES STEALTHY MALWARE INSIDE LEGITIMATE DIGITALLY SIGNED FILES

Hackers find out a new technique that is used to hide malicious code inside the digitally signed files without breaking their signatures and in order to further processing it is loaded into memory.

This attacking method is developed by a researcher of cyber security firm 'Tom Nipravsky'. And it can be a powerful tool for attackers in the future.

The information about digital signature is not a part of the original file at that time when it is signed. It is added later to certify that the file is configured and it has certain hash. This means the hacker can add data inside the certification field, without changing the file hash or breaking the signature.

VII. CONCLUSION

Throughout this paper a brief introduction of image steganography and its different methods are reviewed. There we have also discussed different types of security attacks performed through steganography.

So we can say that the steganography is not just the hiding secret data for preventing it from unauthenticated user but it also a major weapon for cyber crimes and attacks. There is not any software which can fully detect the images, so the attackers and hackers used image steganography to perform these types of attacks.

REFERENCES

[1] Weiqi Luo, Fangjun Huang, Jiwu Huang, (2010), "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and

[2] Security,vol.5,No.2,pp.201-214.

[3] Steganography, Wikipedia

[4] http://en.wikipedia.org/wiki/Steganography

[5] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[6] www.csoonline.com

[7] Mansi S. Subhedara, Vijay H. Mankarb. Current status and key issues in image steganography: A survey. COMPUTER SCIENCE REVIEW 13–14 (2014) 95–113

[8] N.F.Johnson,S.Jajodia,Exploringsteganography:seeingtheunseen, IEEE Computer31(2)(1998)26–34.

[9] J.C.Judge,Steganography:past,present,future.SANSInstitute publication, /http://www.sans.org/reading_room/whitepapers/ stenganography/552.phpS, 2001.

]N.Provos,P.Honeyman,Hideandseek:anintroductionto steganography,IEEESecurityandPrivacy1(3)(2003)32–44.

[10] P.Moulin,R.Koetter,Data hiding codes,ProceedingsoftheIEEE93 (12)(2005)2083–2126.

[11] S.B.Sadkhan,Cryptography:currentstatusandfuturetrends,in: ProceedingsofIEEEInternationalConferenceonInformation& Communication Technologies:FromTheorytoApplications,Damascus. Syria,April19–23,2004,pp.417–418.

[12] S.Lyu,H.Farid,Steganalysisusinghigher-orderimagestatistics, IEEE TransactionsonInformationForensicsandSecurity1(1) (2006)111–119.

[13] D.Kahn,Thecodebreakers:thecomprehensivehistoryofsecret communication fromancienttimestotheInternet,Scribner, December 5,1996