iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.43237

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Computer Forensic in Image Steganography

Dr. Sudheer. S. Marar[1], Krishnendhu R[2], Mr. Ashish L[3]
[1]*Professor & HOD, Department of MCA, Nehru College of Engineering and Research Centre*
[2]*Department of MCA, Nehru College of Engineering and Research Centre*
[3]*Assistant Professor, Nehru College of Engineering and Research Centre*

Abstract: ***The advancement of strong imaging tools, modifying photographs to change their data content is becoming a common task. In the computer forensic world, adding, erasing, or copying/moving image data without leaving a trace or unable to be discovered by the inquiry is a problem. The security of information exchanged over the Internet, such as photos and other confidential data, is critical. The goal of today's forensic Image investigation tools and methodologies is to uncover the tempering strategies and restore trust in digital media's trustworthiness. The difficulties of detecting steganography in computer forensics are investigated in this paper. These issues were investigated using open source software. The experiment focuses on steganography applications that employ the same methods to obsure and secure.***
Keywords: ***Image steganography, LSB steganography, LSB Spatial Algorithm, steganoanalysis***

I. INTRODUCTION

The digital media revolution has resulted in an increase in the availability of computer options that are both cost-effective and efficient. Those who require power and logic to handle issues in computer forensic examination tools and strategy to improve a robust computer forensic environment are of primary concern. Steganography is a method of concealing information in plain sight, similar to camouflage that is invisible to an intruder or unintentional recipient . This research tries to address the possibilities in computer forensic investigation by employing tool X to decode concealed information encoded by other tools with similar characteristics and methodologies. Because both tools employ the same algorithms, it is assumed that tool X will be able to uncover the secret information. It will be expressed in a practical perspective, with the end result likely to pave the way for more research. If the results don't match expectations, it's a difficulty in computer forensics, and it could lead to the development of a new steganography decoding algorithm.

The follows develops deeper into various studies on the era of steganography and its detection techniques. It includes a brief review of steganography uses and techniques based on literature review. The methodologies used in steganalysis will also be investigated in order to lay the groundwork for any proposed solution. The experimental effort of decoding information encoded using steganography tools that employ the same approach is presented in followed by the findings and discussion that leads to the conclusion.

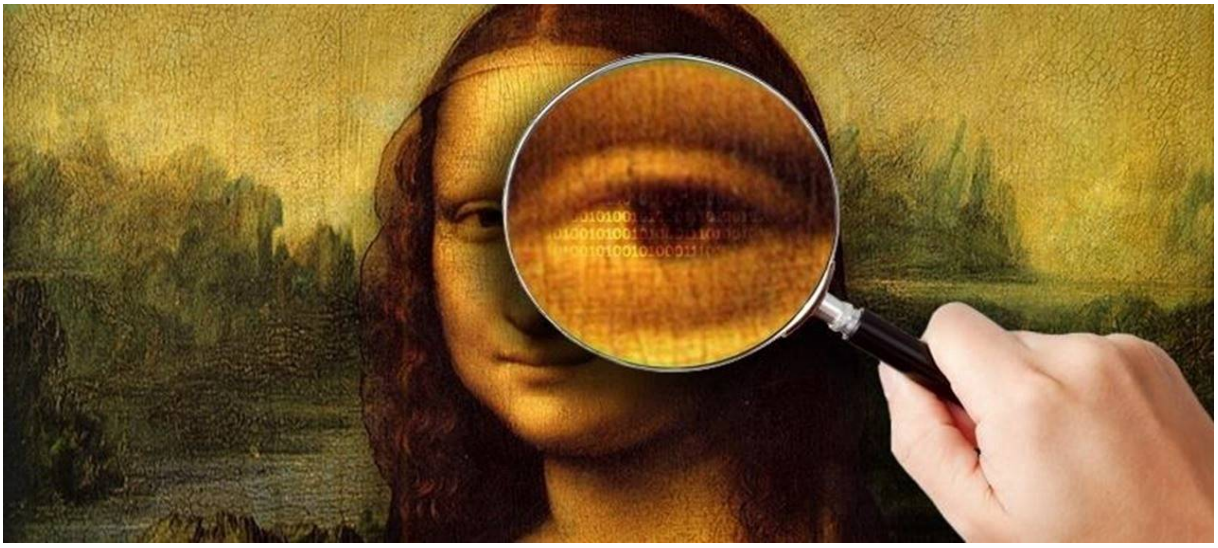


FIGURE 1: Computer forensics in image steganography

©IJRASET: All Rights are Reserved

A. Steganography in the Digital Era

With the employment of signal data processing programming and data theories, the time of digital steganography plays a vital role in the sphere of the digital world . Steganography's evolving technological innovation patterns are being applied in a variety of fields, including networking, military, health, interactive media, and so on . Furthermore, the progress of steganography is quickly becoming a place where people aren't just interested in hiding messages. They are also willing to obtain concealed data in interactive media without altering or eliminating the real message. It was examined at Michi University.

Because they are all used for secret communication, steganography, watermarking, and cryptology are all linked. Watermarking is a type of marker that is secretly put into digital data as an image and used to prove ownership of that data . Furthermore, it is argued that steganography does not provide integrity in terms of privacy or encryption on its own, but that combining these functions can result in a better scrambled information . These findings suggest that employing a stenographic framework to protect information without incorporating other functions such as cryptography is difficult. The purpose of cryptography is to conceal a communication by making it incomprehensible without sacrificing privacy or the intention of being hidden as an art of encryption that converts plain text to cipher text .

B. Detection Techniques for Steganography

In a never-ending battle, steganalysis is an attack aimed at breaking steganography techniques. It is designed to resemble cryptanalysis and employs stenographers to assess the quality of their algorithm instructions step by step in order to avoid discovery [Several image processing algorithms, such as code translation, are used to create steganalysis. The attack succeeds by detecting hidden information in a file, which appears to be different from a watermarking attack that only removes the watermark. However, current advancements in steganography necessitate a robust technique for detecting hidden contents with the lowest false alarm rate. Furthermore, the natural eye is the easiest and simplest way to identify or suspect the presence of steganography. When each bit of a pixel is altered, steganography is detected by experts in steganalysis. The EncaseApps C-TAK is based on a dataset that aids in computer forensic investigation by assisting in the analysis of accurate information in the investigation of cyber threats and steganography. The precision element entails determining even the sort of steganography tool that was utilized for encoding. This type of tool is designed to look at known poor hash-sets that are embedded in datasets rather than outliers. A recent study reveals a novel technique for detecting and finding hidden objects that can be implemented into the Encase forensic tool.

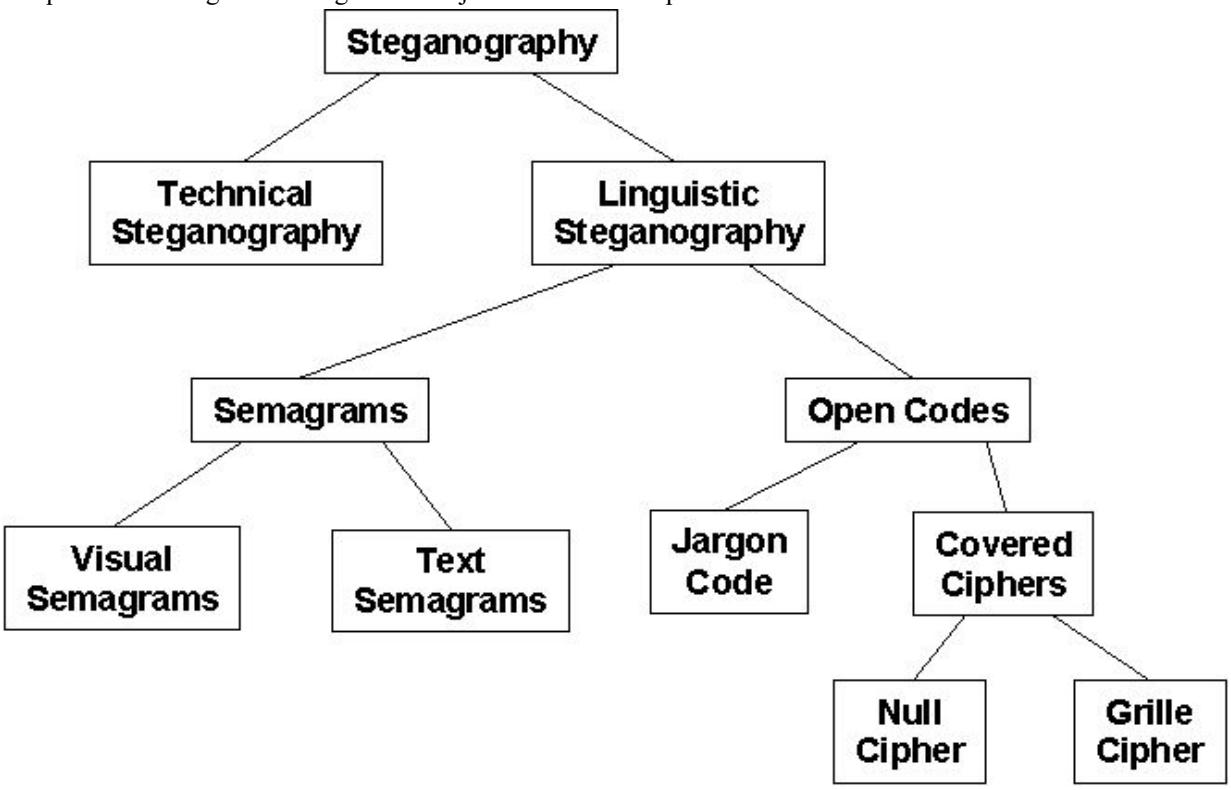


Figure 2: Steganography model

C. *Steganalysis*

Steganalysis, or the detection of steganography by a third party, is a relatively new study field, with only a few studies published prior to the late 1990s. Steganalysis is a technique for detecting or estimating hidden information based on the observation of data transmission without making any assumptions about the steganography process (Chandramouli 2002). Detecting concealed data might not be enough. The steganalyst may also want to extract the hidden message, disable the hidden message so that it cannot be extracted by the recipient, and/or change the secret message to send the recipient false information (Jackson et al. 2003). If the goal is to acquire evidence for a past crime, steganography detection and extraction are usually adequate, though destruction and/or change of the hidden information may also be necessary.

1) Only the steganography medium is available for examination in a steganography-only attack.
2) The carrier and steganography media are both available for analysis in a known-carrier attack.
3) The secret message is known in a known-message attack.
4) The steganography medium and algorithm are both known in a chosen-steganography assault.
5) A known message and steganography algorithm are used to create steganography media that may be analysed and compared afterwards.
6) The carrier and steganography medium, as well as the steganography technique, are all known in a known-steganography attack.

II. LITERATURE SURVEY

In 2013, Chakraborty, Jalal, and Bhatnagar devised an algorithm for distributing secret data (payload) among many matrices to generate the same visual distortion. Using the XOR operation, data is encoded in the second least significant bit plane. The method's shortcoming is the need to keep track of several matrices. Sarreshtedari and Akhaee (2014) proposed a strategy for improving visual imperceptibility by lowering cover picture distortion. With a 1/3 pixel change, this approach provides 1 bit per pixel embedding capability. This approach is immune to LSB detection attacks, such as HCF-COM. This approach has a drawback in terms of embedding capacity. GLSB++ was proposed by Qazanfari and Safabakhsh in 2014. They made the lock key.The lock key is determined by the cover image. using lock key Some cover components that will not be used are locked to conceal the information.

In 2015, Uma Maheswari and Jude Hemanth proposed an approach based on the Fresnelet transform (FT). Data is embedded using the LSB of high frequency sub-bands.

OR code is used to make a secret message more secure.

"This method's average PNSR is 45.40 Db, and its embedding capacity is 352,332 bits". LSB, Discrete Cosine Transformation (DCT), and compression techniques were used by Raja, Chowdary, Venugopal, and Patnaik to improve security. To create the stego image, the data is first embedded into the cover image using a basic LSB approach. To boost security, DCT is applied to the stego image, and then the image is compressed using quantization and the run length coding algorithm.

To retain image quality, Po-Yueh Chen and Hung-Ju Lin presented an approach in which the low frequency sub band LL of the DWT transformation is left unaltered. Fixed (fixed bits per pixel) or variable (varying bits per pixel) data is embedded. A key matrix is generated during embedding and is also embedded in the image. Without a key matrix, data cannot be extracted. For increased capacity, this approach produces acceptable PSNR values. Huffman encoding is used by Amitava Nag and colleagues to encrypt a secret message. On the cover image, DWT frequency transformation is used. Data is embedded in the image's high frequency area. Atawneh et al., 2016 developed a method in which the secret image is transformed to base 5 and then embedded into the cover using the DE methodology.

III. METHODOLOGY

It's critical to have certain criteria for analysing different image steganography techniques in order to improve existing algorithms or develop new ones. The numerous analysis parameters that are utilised to examine different steganography techniques are listed below. The goal of the proposed effort is to create reliable algorithms for the following tasks:

A. *Proposed Methodology*

The goal of the proposed effort is to create reliable algorithms for the following tasks:

1) Increase resilience by using random and virtual bit-plane embedding instead of static layer embedding, using value amendment instead of direct
2) Maintain imperceptibility through bit or value change and consideration of human perception characteristics.

3) Increase capacity by using multi-bit embedding in 24bit images and music, as well as compressing data.
4) The benefit of steganography over cryptography alone is that the intended hidden communication does not draw attention to itself as a target for investigation. Plainly visible encrypted messages, no matter how impenetrable, generate curiosity and may be incriminating in nations where encryption is prohibited.
5) Computer forensics is the preservation, identification, extraction, documentation, and interpretation of computer media for the purpose of obtaining evidence. It may be necessary in a variety of computer crimes and misuses.
6) Thousands of deleted emails were recovered, and an inquiry was conducted after numerous individuals took over the system.
7) Steganography is becoming increasingly widely employed in the digital world; however, there are numerous concerns to be aware of in computer forensics; there are numerous tools and methodologies, each with its own set of strengths and drawbacks.
8) Initially, the overview of digital era steganography provides computer forensic experts in the industry with recommendations and an understanding of steganography.
9) As surveyed, the employment of instruments to notice changes in bits of data may likewise raise doubts. The techniques and algorithms employed in steganography are examined in order to have a better grasp of how it works.
10) The most extensively used digital media format is picture files, therefore our study is limited to the LSB approach because it is commonly used in digital image steganography and has no effect on the real colour.
11) This makes normal visualisation difficult to identify.

The following are the basic words used in digital image steganography:

a) *Image:* A visual perception is represented by an image (of an object, scene, person or abstraction). An image I is a discrete function that assigns the pixel I j) a colour vector c(i, j) .
b) *Cover Picture:* A cover image is an image that is used to transport secret information in a secure manner. It's utilised by the sender to insert the necessary information.
c) *Stego Image:* The stego image is the cover image once the hidden information has been embedded in it. It could be a password or a number generated by a pseudo-random number generator to determine potential embedding spots.
d) *Stego Key:* A stego key is a key that is used to embed data in a cover and then used to retrieve the data embedded. It could be a password or a number generated by a pseudo-random number generator to determine potential embedding spots.
e) *Embedding Domain:* The properties of the cover media that are exploited for secret information embedding are referred to as the embedding domain. The domain might be either spatial or frequency. The secret embedding is done directly into the cover in the spatial domain, however in the frequency domain or transform domain, the carrier media is first transformed into frequency domain, and then the secret embedding is done using the altered contents of the cover (eg. frequency coefficients).
f) *PSNR (Peak Signal to Noise Ratio):* It determines how good a stego image is. This performance parameter is used to determine the stego image's perceived transparency.

PSNR = MN maxx,y Px,y2Px,y Px,y Px,y 2x,y

Where M and N are the number of rows and columns in the cover picture, respectively, and Px,y and Px,y are the pixels of the original and stego images.

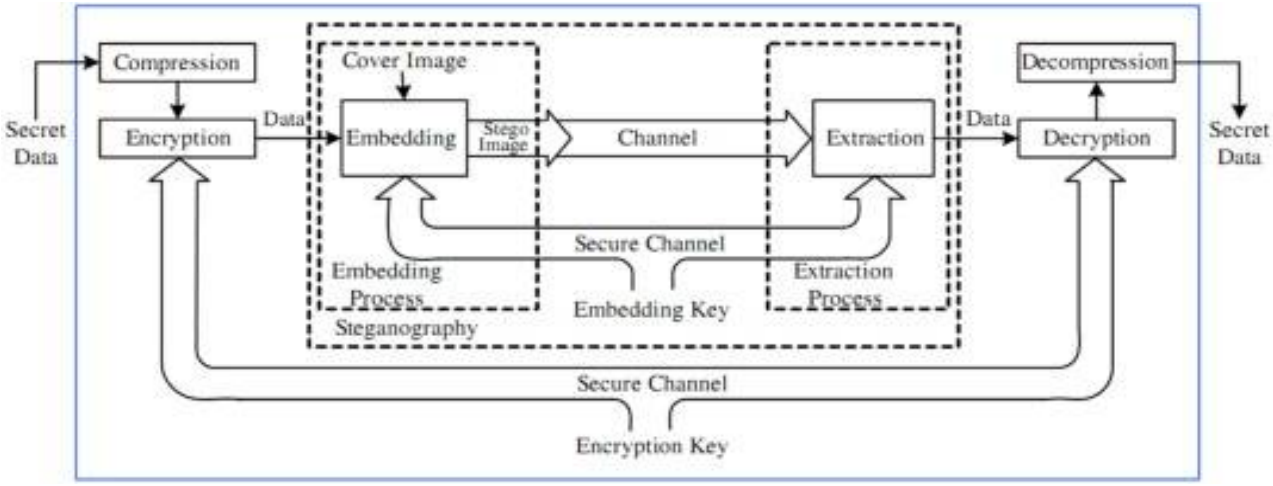


Figure 3: STENGANOGRAPHY

g) *Bit Error Rate:* When retrieving secret information, the Bit Error Rate (BER) is utilised to calculate the error. The lack of an ideal conduit for transferring the secret information between the sender and intended receiver causes this problem . In the given equation, the cover image is covg and the stego image is steg, where I is the pixel location.

- 1image covg imagecovg imagesteg all pixelsi=0
- BER = 1image covg imagecovg imagesteg all pixelsi=0

B. *Image Steganography*

The main goal of digital picture steganography is to hide secret information inside the cover image with the least amount of visual distortion and the most amount of embedding capacity possible in order to achieve secret communication. In order to do so, a vast number of research efforts in the field of digital picture steganography have taken place, resulting in several varieties of steganography. As a result, image steganography can be divided into three categories: spatial domain, transform domain, and frequency domain, as well as model-based steganography.

1) *Steganography on Spatial:* To embed the secret information, this technique entails directly altering the contents (pixel values) of the cover image. This approach is appealing because of its ease of execution and strong embedding potential. However, this method is less effective.
2) *Domain Transform Steganography:* Steganography based on the transform domain There are two sorts of frequency in a digital image: high frequency and low frequency. Low frequency values represent smooth and plane areas, and high frequency values represent edges. Unlike high frequency areas, changes in low frequency regions are visible to the Human Visual System (HVS), and the pixel values of low frequency regions have a strong correlation. As a result, high-frequency zones are preferred over low-frequency regions. In the transform domain technique, pixel values are transformed into frequency coefficients using any of the transforms available, such as the Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and so on. After that, the secret information is encoded in the coefficients. Methods for transforming domains are more to image processing operations, less susceptible to stego attacks. As a result, they outperform spatial domain-based approaches.
3) *Adaptive Steganography:* Adaptive steganography is a type of steganography that is a combination of two previous approaches. P. Sallee presented it for the first time in 2003, based on the statistical features of the cover media. "Statistics-aware embedding" or "Model-Based" are other terms for it. This method determines suitable embedding locations into pixel values or frequency coefficients prior to embedding by using statistical global properties of the image in either the spatial or frequency domain. This unique technique allows the secret message to be embedded with an extra layer of security, robustness, and large capacity while maintaining acceptable perceptual transparency.

C. *Algorithms And Steganography Techniques*

The procedure entails embedding the sender's cover file and using a convenient approach to reveal the secret message at the predicted beneficiary's end. The ability of the secret data to remain hidden with the strong algorithm used, enough space to allocate the hidden data, and the algorithm's robustness in delivering the message safely from one end to the other without data loss during compression and being resistant to attack during data transmission are all factors that influence the strength of steganography. Furthermore, the algorithm and pass used should be kept secret so that even if the attacker detects the presence of steganography, the hidden data cannot be revealed because the algorithm is not protected.

The cover file utilised (image, text, audio, video, or protocol), the file format type (JPEG, BMP, or GIF), or the method of steganography can all be classified.

The type of compression (lossy or lossless, for example, JPEG), the domain type (transformed domain, for example, DCT method or spatial, for example, LSB method), the embedding method (Spread Spectrum, masking, statistical, or distortion), and so on.

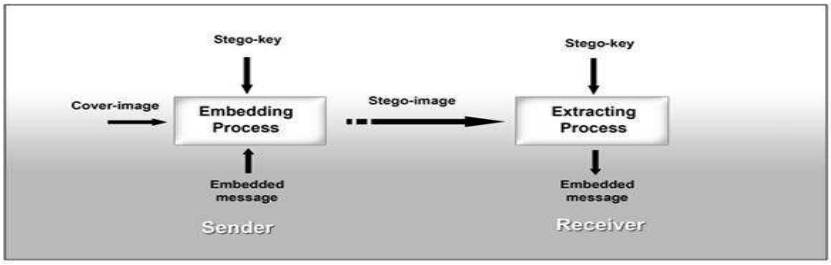


FIGURE 4: Steganography of images

1) *Steganography of Images:* The hidden information is disguised as noise, making it nearly impossible to see with the naked eye. Images have a high degree of redundancy and twisting tolerance. A type of compression methodology is expected to play a significant effect in determining which algorithm method of steganography to employ. A lossy compression approach is used in the JPEG image file format, resulting in tiny image sizes with the risk that the hidden message will be lost due to the deletion of much of the image data information. GIF is an example of a lossless image compression method. Although the lossless method does not compress the image to the same small size as the lossy method, there is a good chance that the digital image contents will not be lost.
2) *The LSB Algorithm of Spatial Domain:* Because some steganography tools that use LSB substitution for encoding consider modifying the least bit, while others randomise all of the original bits in the altered cover file, it is difficult to identify. The secret information is stored by modifying the bit of the image using LSB. The difference in intensity is minor, but the human eye perceives no change. Because of their peculiar size during transmission, bigger images are more vulnerable to attack. Every image contains a pixel that is responsible for a specific colour. R(red)G(green)B(blue) (blue). The LSB method converts the data to binary depending on the intensity.
3) *Image and Sound in Digital Format:* The carrier material for many typical digital steganography techniques is graphical graphics or audio files. Before understanding how steganography and steganalysis function with these carriers, it's helpful to review image and audio encoding.

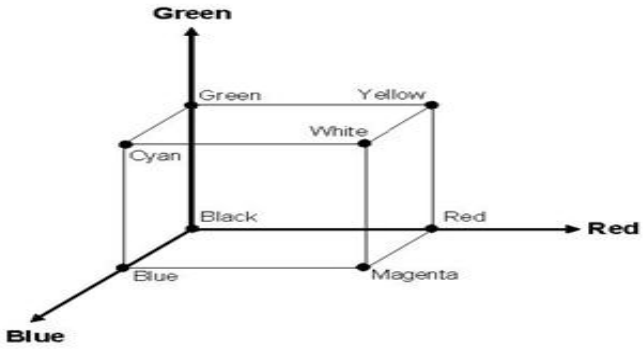


Figure 5: The RGB Color Cube.

The RGB colour cube is a typical way to represent a colour by the relative intensity of its three component colors—red, green, and blue—each with its own axis (moreCrayons 2003). The absence of all colours results in darkness, which is represented by the intersection of the three-color axes at zero. Magenta is made up of 100 percent red, 100 percent blue, and no green; cyan is made up of 100 percent green and 100 percent blue without any red; and yellow is made up of 100 percent green and 100 percent red with no blue. All three hues are present in white.

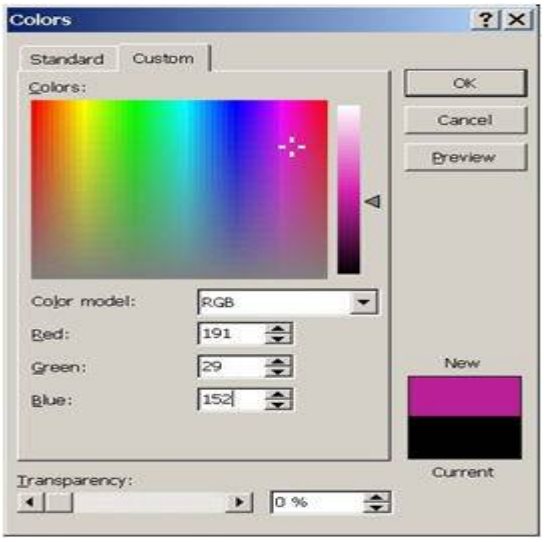


Figure 6: This color selection dialogue box shows red, green, and blue (RGB) levels of this selected color.

Some random color's RGB intensity levels Each RGB component is given by a single byte, allowing colour intensity values to range from 0-255. A red level of 191 (hex BF), a green level of 29 (hex 1D), and a blue level of 152 define this colour (hex 98). One magenta pixel would be represented as 0xBF1D98 using 24 bits. This 24-bit encoding technique can handle 16,777,216 (224) different colour combinations (Curran and Bailey 2003; Johnson and Jajodia 1998A).

Most digital image applications currently offer 24-bit true colour, which entails encoding each picture element (pixel) in 24 bits, which includes the three RGB bytes stated above. Other applications use eight bits per pixel to encode colour.

Converting an analogue signal to a bit stream is what audio encoding is all about. Sine waves of various frequencies describe analogue sound, such as voice and music. The human ear can detect frequencies between 20 and 20,000 cycles per second (Hertz or Hz). Sound is an analogue signal, which means it is continuous. The continuous sound wave must be transformed to a series of samples that can be represented by a sequence of zeros and ones before being stored digitally.

Analog-to-digital conversion is carried out by sampling the analogue signal (using a microphone or other audio detector) and converting the samples to voltage levels. Using a pulse code modulation technique, the voltage or signal level is subsequently transformed to a numeric number. This conversion is carried out via a gadget.

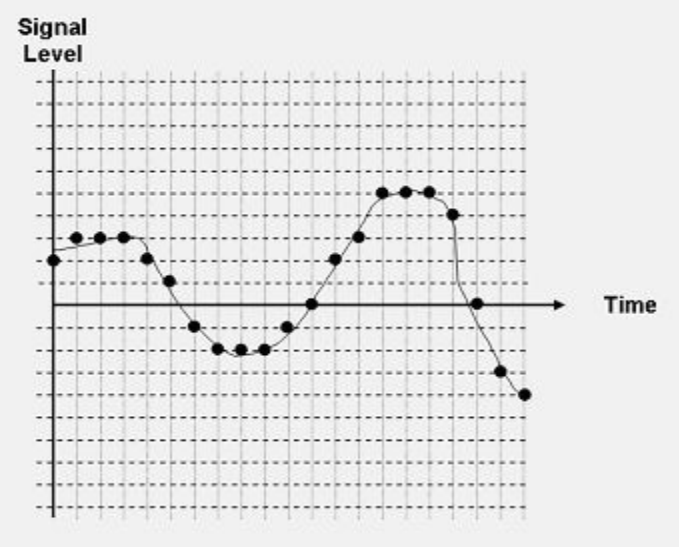


Figure 7: Simple Pulse Code Modulation.

IV. METHODS OF DIGITAL CARRIER

In digital media, messages can be disguised in a variety of ways. Data that remains in file slack or unallocated space as the vestiges of earlier files is recognisable to digital forensics researchers, and tools can be created to directly access slack and unallocated space. In the unused area of file headers, small quantities of data can also be buried (Curran and Bailey 2003).

A secret partition on a hard drive can also be used to conceal information. Under typical conditions, a hidden partition will not be visible, yet disc configuration and other tools may enable complete access to the hidden partition (Johnson et al. 2001). This notion has been implemented in the Linux ext2fs steganographic file system.

In audio and visual files, the most frequent steganography approach is some type of least significant bit replacement or overwriting. The numeric significance of the bits in a byte gives rise to the term "least significant bit." The highest-order or most significant bit has the largest arithmetic value (27=128), whereas the lowest-order or least significant bit has the lowest arithmetic value (i.e., 20=1).

Consider "hiding" the character "G" throughout the following eight bytes of a carrier file (the least significant bits are underlined) as a simple example of least significant bit substitution:

10010101 00001101 11001001 10010110
00001111 11001011 10011111 00010000

The binary string 01000111 represents a 'G' in the American Standard Code for Information Interchange (ASCII). These eight bits can be "written" to each of the eight carrier bytes' least significant bit as follows:

10010100 00001101 11001000 10010110
00001110 11001011 10011111 00010001

Only half of the least significant bits were modified in the example above (shown above in italics). When one set of zeros and ones is exchanged with another set of zeros and ones, this makes sense.

To overwrite valid RGB colour encodings or palette pointers in GIF and BMP files, coefficients in JPEG files, and pulse code modulation levels in audio files, least significant bit substitution can be employed. The numeric value of the byte changes very little when the least significant bit is overwritten, making it less likely to be noticed by humans.

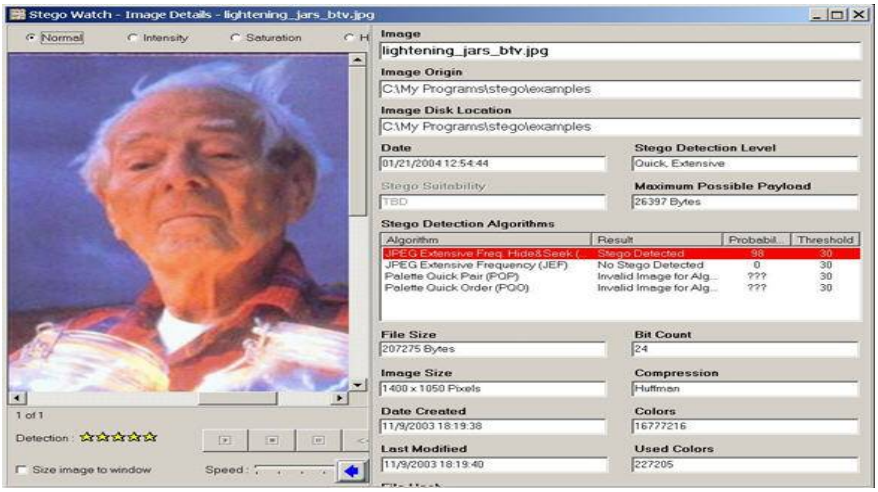


FIGURE 8: Information from Stego Watch about a JPEG file suspected to be a steganography carrier.

When compared to extracting hidden data, finding steganography in a file suspected of containing it is rather simple. For anonymity, randomization, and/or encryption, most steganography software employs passwords. Stegbreak, a companion software to stegdetect, employs a dictionary attack against JSteg-Shell, JPHide, and OutGuess to find the password of the concealed data, but only for JPEG files (OutGuess 2003). Stego Break, a companion application to WetStone's Stego Watch, employs a dictionary attack on suspicious files (WetStone Technologies 2004B). Steganography detection systems do not immediately aid in password recovery. The rest of the inquiry and computer forensics are focused on finding acceptable clues. A computer forensics examiner looking at evidence in a criminal case is unlikely to make any changes to the evidence files. Even if the secret information cannot be recovered, an inspection conducted as part of an ongoing terrorist surveillance programme may wish to disrupt it. Hidden content, such as steganography and digital watermarks, can be deleted or manipulated in a variety of ways (Hernandez Martin and Kutter 2001; Voloshynovskiy et al. 2001), and software built particularly to attack digital watermarks is available. Such attacks have one of two effects: they either lower the carrier's steganography carrying capacity (which is required to evade the attack) or they completely disable the carrier's steganography medium capabilities.

Steganography methods are becoming more complicated as time goes on. Spread-spectrum steganography methods are similar to spread-spectrum radio transmissions (first developed in WWII and now widely used in data communications systems), in which the signal's "energy" is spread across a wide frequency spectrum rather than focused on a single frequency to make detection and jamming more difficult. The identical function of spread-spectrum steganography is to evade detection. These solutions take advantage of the fact that image and sound file distortions are least noticeable in the carrier's high-energy parts (i.e., high intensity in sound files or bright colours in image files). When tiny modifications to loudness are applied, it is easier to trick human senses even when seen side by side.

V. STEGANOGRAPHY DETECTION

In a pure steganography model, William knows nothing about the steganography method employed by Alice and Bob. This is a poor assumption on Alice and Bob's part since security through obscurity rarely works and is particularly disastrous when applied to cryptography. This is, however, often the model of the digital forensics analyst searching a Website or hard drive for the possible use of steganography.

Secret key steganography assumes that William knows the steganography algorithm but does not know the secret stego/crypto key employed by Alice and Bob. This is consistent with the assumption that a user of cryptography should make, per Kerckhoff's Principle (i.e., "the security of the crypto scheme is in key management, not secrecy of the algorithm.") . This may also be too strong of an assumption for practice, however, because complete information would include access to the carrier file source.

VI. RESEARCH AND EXPERIMENTAL:

This section seeks to investigate the issues of computer forensic inquiry in image steganography in practise using computer forensic techniques. There are many steganography tools available, but only those that meet our analytical requirements.

A. Steganography in the Spatial Domain

By simply changing the pixel values of the cover image, spatial domain based steganography is the simplest of data concealment techniques. LSB technique (least significant bit substitution): The primary idea behind the LSB substitution approach is to incorporate secret information at random in the rightmost bits of a pixel (bits with the smallest weight) without materially changing the original pixel value. The distortion caused by LSB replacement impacts pixels by a factor of one, making the mechanism perceptually transparent. This is the simplest way, but it is susceptible to signal processing or disturbances, as well as picture processing processes such as cropping and scaling. Because of the PoVs (Pair of Values) in the image, steganalysis of LSB embedding is simple.

B. Pixel Indicator Technique (PIT)

This technique uses a pixel as an indicator. Pixel Indicator Technique was created in order to improve the security of the existing LSB system. Two LSB of one channel indicates the presence of data in the other two channels when using 24-bit/pixel colour pictures. The size of the secret data is used to determine the selection channel. RGB, RBG, GBR, GRB, BRG, and BGR are the names of the two channels (indicator channel and embedding channel) in this order: RGB, RBG, GBR, GRB, BRG, and BGR. When the embedding rate is less than 3 bits, PIT causes relatively little visual distortion, making it vulnerable to histogram and visual attacks.

C. OPAP: Optimal Pixel Adjustment Procedure

The OPAP algorithm outperforms the LSB-based technique. The pixel disparities between the original pixel and the stego-image pixel are calculated to improve the image. The OPAP technique alters the contained bits in order to improve the stego image's overall visibility. For conventional test pictures, OPAP offers high PSNR values. Lena and Baboon.

D. Secure Key Based Image Realization Steganography

Image realisation has been offered in this study as an alternative to incorporating the secret information directly into the cover image. Matrix Encoding Technique is used to embed some mapping information linked to the secret information into the cover image, and the secret is realised using a highly secure pass key. The first phase involves mapping the secret message, key generation, and embedding, followed by the extraction technique in the second phase. The mapping matrix is created using one of the RGB image's planes (the red plane in this case). The selected plane (Ci) is divided into several blocks and rendered as multiples of the hidden image. Cg plane and blue plane (Cb). S stands for secret information. Cmin S=M is the mathematical expression for the mapping operation, where M is the mapping matrix, Cmin is the block in Ci with the smallest difference from S, and is the mapping operator, which can be any discrete operator or function.

The extraction algorithm is the inverse of the embedding process. The key is used to extract the size of the secret information and the location of the matrix, and the secret information is retrieved by calculating the difference between the matrix obtained from the key and the original matrix value. Because the decoding key has a sufficiently wide key space, this strategy is secure against Brute Force attacks. This method also achieves high security against statistical as well as histogram assaults.

E. Image Realization Steganography with LCS based Mapping

Realization of Images Steganography based on LCS Mapping: Ratnakirti Roy and Suvamoy Changder have created a new cover-secret mapping technique that uses secret information as a Least Common Subsequence (LCS) of the Least Common Subsequence (LCS) of the Least Common Subsequence (LCS) of the Least Common covers image for mapping. The map is generated by selecting one of the cover image's planes (RGB), with the other two planes being utilised to incorporate any secret information. The secret image's LCS is calculated row by row. The embedding is required if the mapping between the cover image and the hidden information is not perfect. The map generation step generates two maps, one with the information needed for secret-cover mapping and the other with the information needed for extraction if any secret information is embedded (the number of bits embedded for each row of the secret image). If the row of hidden image is totally found as an LCS of cover image, the latter map will be empty.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Because the length of the binary string representation of the cover picture is much longer than the length of the binary string corresponding to each row of the secret image, and each of these binary strings is random in nature, the mapping level of this method is quite high. Because the possibility of accurately decoding the secret is very minimal, the strength of the key employed in this method is very high. As a result, the approach is very resistant to Brute-Force attacks. As demonstrated in complete mapping of the hidden image to the cover image is achievable, resulting in a larger payload carrying capacity than the current steganography technique. The map is not, however, incorporated in the cover image because it reduces the size of the image.

VII. RESULTS ANALYSIS

There are many steganography tools available, but only those that meet our analytical requirements. The hidden data from the same stego-file that OpenStego failed to extract was now extracted utilising a tool used in the encoding procedure.

Steganography tool	LSB method	Method of Encryption	Platform	Password support
JPHIDE (jphs)	√	blowfish	multi	√
SilentEye	√	AES	cross	√
S-tool	√	DES	Windows	√
OpenPuff		Joined Multi		√
OpenStego	√	DES	cross	√
QuickStego		none	Windows	

Figure: 10 Analysis Of Steganography Tools

As indicated in the table above, the steganography tools S-tool and OpenStego meet the requirements for this study. There are, however, some minor variances in terms of their support. The only significant difference between S-tool and OpenStego is that S-tool supports more encryption methods than OpenStego, which only supports DES, which has no effect on the steganography process. Two files were used in this experiment: a secret and a cover file. The cover picture file is cover.bmp, and the secret.txt file contains a message that is intended to be kept secret. The file properties, as well as screenshots of the entire procedure.
S-tool is used to demonstrate the encoding process with a secret.txt and cover.bmp. A text file measuring 81 bytes is placed in the cover. Drag and drop a bmp file into S-tool and pass it. The passphrase is 2-0, and the encryption method is DES.

A. Encoding Method: Hiding Process using S-tool



The stego-file and the real cover file are depicted in the two images to the right. There is no discernible difference between the files before and after steganography. The hidden.bmp file contains the stego-image. The steganalysis tool StegExpose is used to distinguish and Detection method: StegExpose was used to detect the process.

FIGURE: Online hexeditor: Comparing the files hashes



Decoding method: decoding method at the OpenStego

To compare and view the files, an online hex editor is utilised. The original data was revealed by browsing the stored file and using the same password.



To compare and view the files, an online hex editor is utilised. The original data was revealed by browsing the stored file and using the same password. The notice in the pop-up indicates that the data was properly extracted. However, a notification message from the java terminal, indicates that there is a problem with the extraction. The message was read, but the embedded data was corrupt, or an invalid password was provided, or there was no method that could handle it.

Decoding method: decoding method at the S-tool

The identical stego-file from which OpenStego failed to extract the concealed data was now extracted using the encoding method's tool. All of the passwords and encryption methods are identical. The size of the disclosed files is the same as it was before they were encoded. The hidden data from the same stego-file that OpenStego failed to extract was now extracted utilising a tool used in the encoding procedure. All of the passwords and encryption methods are identical. The size of the disclosed files is the same as it was before they were encoded.

Because both programmes utilise the same methodology and the same password for encoding, it is believed that the other tool will be able to decode and reveal the hidden information. Even though they use the identical techniques and features, the results of this experiment reveal that a tool A in steganography cannot recover data encoded by a tool B. The file may have been corrupted on the way, which is unlikely given that the S-tool was able to decode the message, or the OpenStego may have detected the file as corrupt. Second, the possibility that the password used is invalid is ruled out because the same password was used for the encoding technique. A probable error is an algorithm that could produce a problem.

Both of these tools, however, employ the LSB substitution approach.

The problem is that various tools may utilise a different technique of selecting the Least Significant Bit in their substitution approach, such as randomness, the last two digits, or the last digit alone.

This is the same concept as Kessa's 2015 study, which was discussed in the literature section. The impacts of corruption and an unknown steganography approach are difficult to detect.

As a result, finding tools and strategies to break the hidden information in steganography presents a problem in computer forensic investigation. This type of generic steganography detection and classification tool development is still in the works.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VIII. CONCLUSION

As steganography becomes more widely employed in the digital world, there are a number of difficulties to be aware of in computer forensic testing. There are numerous tools and strategies available, each with its own set of strengths and weaknesses. Continuous change and more modern adjustments are required. Initially, the overview of digital era steganography provides computer forensic experts in the industry with recommendations and an understanding of steganography.

As surveyed, the employment of instruments to notice changes in bits of data may likewise raise doubts. s. Initially, the overview of digital era steganography provides computer forensic experts in the industry with recommendations and an understanding of steganography. As surveyed, the employment of instruments to notice changes in bits of data may likewise raise doubts. The techniques and algorithms employed in steganography are examined in order to have a better grasp of how it works. Picture file type is the most extensively used medium of digital media, and this research is limited to LSB technique since it is largely utilised in digital image steganography and has little influence in altering the actual colour. This makes normal visualisation difficult to identify. Furthermore, the practical outcome clarifies whether or not a computer forensic expert should employ a steganography programme.

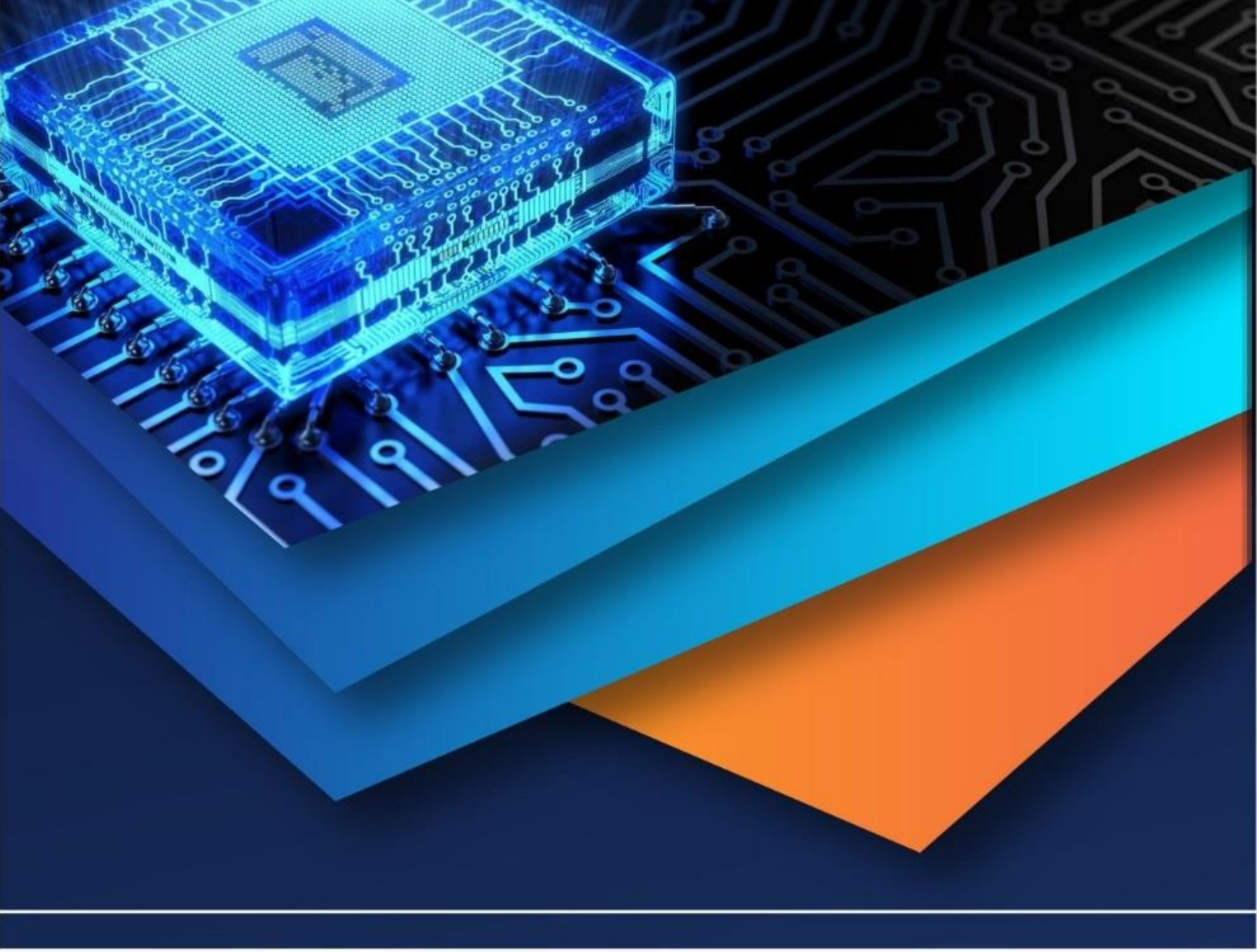
The techniques and algorithms employed in steganography are examined in order to have a better grasp of how it works. The most extensively used digital media format is picture files, therefore our study is limited to the LSB approach because it is commonly used in digital image steganography and has no effect on the real colour. This makes normal visualisation difficult to identify. Furthermore, the practical outcome clarifies a computer forensic expert's concept of substituting steganography tool A for steganography tool B to extract secret data, which is not achievable as confined to this experiment, despite the fact that they share the same qualities and techniques.

Finally, this study provides insight into why knowing the type of steganography tool installed, hidden, or deleted in the victim's computer is critical for computer forensic examiners. Finding evidence that the suspect uses a specific steganography tool raises suspicions, especially when the victim also uses steganography, leaving a gap for further inquiry into the hidden data on the computer. Furthermore, as demonstrated by the experiment results, knowing the type of steganography tool used is essential to decode the secret information, even when the investigation tool has the same features and uses the same procedures

REFERENCES

[1] "Steganography integrated into linear predictive coding for low bit-rate speech codec," Multi-media Tools Appl, vol.76, issue.2, pp.2837-2859, 2017. P. Liu, S. Li, and H. Wang.2003.
[2] G. J. Simmons, "The Prisoners Problem and the Subliminal Channel," Advances in Cryptology, vol. 51, no. 67, 1987, pp. 51-67.363"An evaluation of the history, demand, and contemporary technologies for digital steganography," by J. E. Storms, 2016.
[3] "Reversible and irreversible datahiding approach," T. Sarkar and S. Sanyal, 2014. N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy, vol.99, no.3, pp.32-44, 2003.
[4] "Image watermarking with biometric data for copyright protection," by M. Barbier, J. L. Bars, and C. Rosenberger. 2015.
[5] "Exploring steganography: See-ing the invisible," Computer, vol.31, no.2, pp.26-34, 1998.
[6] "Digitalimage steganography: Survey and analysis of current approaches," Signal Process, vol.90, no.3, pp.727-752, 2010.
[7] M. S. Sutaone and M. V. Khandare, "Image-based steganography with LSB insertion," no.535, pp.146-151, 2008.
[8] A. Latham, [Online], "JPHIDE and JPSEEK stenog-raphy programmes." [Accessed: 26-March-2016], 1999, http://linux01.gwdg.de/ alatham/stego.html "Reconstructive steganalysis by source bytes leaddigit distribution study," A. Zaharis, A. Martini, T. Tryfonas, C. Illioudis, and G. Pangas, 2011.
[9] A. Chorein,, http://www.silenteye.org/about.html?i6, [Accessed: 27-March-2016].
[10] K. Magee, [Online], "CISSP steganography, an introduction using S-tools." [Accessed: 29-March-2016.
[11] S. Vaidya, [Online], "OpenStego, the free steganography solution."
[12] Domain 3-chapter 4:Cryptography, E. Conrad, S. Misenar, and J. Feldman, 2010.
[13] "Cyber warfare: Steganography versus. Steganalysis," Commun ACM, vol.47, no.10, pp.76-82, 2004.
[14] G. Luo, X. M. Sun, L. Y. Xiang, and J. W. Huang, "An evaluation method for stegano-graphic algorithms' steganalysis-proof ability," IIHMSP 2007. Third InternationalConference on, pp.126-129, 2007.
[15] R. J. Anderson and F. A. P. Petitcolas, "On the Boundaries of Steganography," IEEE Journal on Selected Areas in Communications, vol.16, no.4, pp.474-481, 1998.
[16] "Blindsteganography detection utilising a computational immune system: A work in progress," International Journal of DigitalEvidence, vol.4(1), pp.19, 2003.
[17] Miller, [Online], "Unveiling cyber dangers that can hinder investigations." http://encase-forensic-blog.guidancesoftware.com/2013/07/c-tak-by-wetstone.html.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)