International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

Information Security through Image Steganography

Vimanyu Chopra, Devinder Priyadarshi

Abstract: ***Information security is an arduous task these days especially due to advancement in technology. Sending or receiving confidential information in an undetected form has been a major challenge. Steganography is the art or process of concealing information inside a text, audio or image file. The process of embedding information inside an image is known as Image steganography. The objective unlike cryptography is not to make the information difficult to understand but to hide it in plain sight. The concealed information is harder to detect and is only detected only by the receiver who is aware of its existence. Image Steganography is used to secure private files and documents, hide passwords and encryption keys as well as to transport highly confidential documents between international governments and organizations without revealing the existence of the hidden message. This also makes it essential in military and banking field for secure communication of information. This provides better security to the information being shared. This paper discusses history, techniques, applications, benefits and shortcomings of Image steganography. Further a discussion on the challenges and the future direction and trends of image steganography are also presented.***

Keywords: ***Information security, Stegnanalysis, Image Steganography.***

I. INTRODUCTION

Steganography is very important in today's world because of the need of secure communication. Steganography as a word has Greek origin and is formed by using two words "Steganos" and "Graphe" meaning concealed and writing or drawing respectively. As the name suggests steganography can be described as an art or process of concealing data or secret information within a text, audio or an image file. The process of embedding information inside an image is known as Image steganography. By using image steganography, it is possible to pass secret messages unbeknown the third party who maybe looking for it. It can hide the message in plain sight [1]. It is coupled with cryptography and provides an extra layer of protection along with encryption which strengthens the security of the object [2]. Some technologies like watermarking which are used for intellectual property protection are related to steganography [3]. Prisoner's problem is a good example of contemporary formulation of steganography even though it has been in use since ancient times [4].The problem as be described as having two prisoners named Alice and Bob who are imprisoned in isolated cells and they have to exchange information through a messenger in order to design a scheme to escape from prison while under surveillance of Eve who is the warden assigned to them. If Eve gets suspicious of any activity going on Alice and Bob will be sent to solitary confinement. They can't use only cryptography here as Eve would get suspicious thus, they use steganography to hide the information. Eve will try to find any hidden communication between the two prisoners so as to undo their plans. She can be passive where she would try to detect the message or active where she would actively try and modify or insert information with embedded messages. To send these concealed messages Alice would embed the secret message in information. Alice and Bob can use private or public key steganography. In private key steganography they both share a secret key used for embedding the message while in public key steganography both parties employ private-public pairs of keys while having access to the other persons' public. They have their private key pairs along with a public key. The warden eve examines all communication between the two inmates and the test is to plan the whole jailbreak without her knowing about it [5].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Vimanyu Chopra*, UG Scholar, DAV Institute of Engineering & Technology, Jalandhar, India. Email: vimanyuchopra2@gmail.com
Devinder Priyadarshi, Faculty, DAV Institute of Engineering & Technology, Jalandhar, India. Email: priyadarshidevinder@gmail.com

II. STEGANALYSIS

Steganalysis can be described as the process of finding the hidden message in the information. The techniques also improve along with steganographic techniques. It is used as a measure to test the effectiveness of various steganographic techniques. If the message is easily detected then it is not deemed usable and this technique helps us to improve the existing steganographic techniques as well as in the formulation of new ones. Steganalysis can be universal or targeted [6]. In universal method the steganographic algorithms are detected without knowledge of embedding process. This process is very effective but its detection accuracy rate is very low. The targeted steganalysis method uses specific steganographic algorithms to detect the messages embedded using the defined algorithms. These have a higher detection efficiency than universal techniques as it uses well established algorithms for its search. Nevertheless, in practical scenarios one doesn't generally know the steganographic technique that the persons communicating will use to embed the images thus universal technique is employed if the specific algorithm used to embed images is not known [5]. If we can't find the hidden message it is also possible to destroy the message without understanding it. One such method to defeat the image steganography is compressing the image which will remove the information hidden by LSB method.

Changing the image format is also used to destroy the secret information.

III. Performance Evaluation Factors

For performing these statistical analyses, we mainly use two techniques: Peak-Signal -to-Noise-Ratio (PSNR) which is used to measure distortion while Mean Square Error (MSE) is used to measure capacity of image which can be modified. The PSNR value is used to measure the distortion in the image. It measures the quality of photo in question by comparing the cover image and the image with the hidden message embedded in it. It is calculated as:

$$PSNR\ (C,S) = \frac{10*\log10(2d-1)}{MSE}\ dB \qquad [7]$$

Here in the cover image bit depth is denoted by d which for grey scale images always comes out to 8.
The Mean Square error can be computed with help of following equation which computes the MSE between the image before and after information is added.

$$MSE(A,B) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (A_{ij} - B_{ij}) \qquad [8]$$

Here *Aij* and *Bij* represent the cover image and embedded image pixel values respectively while the variables denoting the dimensions of cover image are M and N.

A PSNR value under 40dB generally is optimal for image steganography purposes as it generally undetectable wile PSNR under 30dB represents a low-quality image [6].

Capacity
Capacity is the total cover image data size which can be modified without changes to cover image becoming noticeable. In the cover image the statistical properties and perceptual aspect also need to be kept intact while performing the embedding operation. Capacity is dependent upon two factors –
1.Number of bits embedded in individual pixel
2.The entire number of bits per pixel
Capacity is denoted by bits per pixel (bpp) and Maximum Hiding Capacity in percentage form.

Robustness
It refers to the ability of the image embedded with information to remain the same and protect the secret message when it undergoes transformation, inclusion of noise, rotation, scaling, cropping or lossy compression.

Imperceptibility
It refers to the ability of the stego-image to have the same statistical properties as the plain image and remain undetected and appear same to the human eye as any non-embedded image.

Signal-to-noise ratio
SNR ratio is the ratio of signal and noise power. The desired signal to level of background noise is determined. This tells us the amount of background noise the image has and whether it affects the hidden information [9].

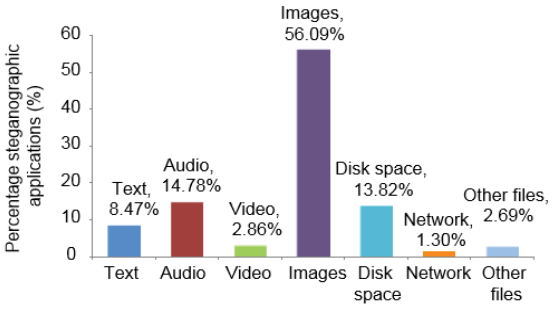

Fig 1- Distribution of media used in steganography [6]

IV. History

Image steganography is by far the most popular way for media steganography ahead of audio, video and text steganography among others. Digital images are considered one of the best media for steganography and for communicating secret information [10]. Digital images are a combination of pixels placed horizontally and vertically to form a matrix. Digital images are used widely in modern time and are attached to email and shared on the web, thus they provide a useful vessel to hide information. Monochrome images use 8 bits out of every pixel and represent 256(2^8) different colours or shades of gray.24-bit files of images of digital colours are kept and these images use RGB colour model .Pixels form combinations of colour of these 24-bit images are made from three primary colours - Red (R), Green(G) and Blue(B) .The combination of these colours are used to represent various colours in an image with each pixel having 256 varying intensities of red, blue and green combine to form colours. The selection of cover images to be used and the steganographic algorithm are important aspects during steganography process.
Using cover images with large block areas of solid colours and famous images like The Last Supper is generally not recommended as it is easy to detect changes in these images. It is optimal to use cover images created for steganography according to the specifications of the message and should be destroyed after being used once.
The algorithm to be chosen depends upon many aspects including the kind of format and the image compression used. There are mainly two types of image compressions: namely lossy and lossless compression. The lossy compression reduces size of image by removing the extra data from native image by removing the details not detected by the human eye. Mainly JPEG (Joint Photographic Experts Group) format files are compressed using this technique and this is the most popular file format. The lossy compression can lead to removal of embedded data thus it is important to choose the steganographic algorithm carefully to prevent loss of essential data while Lossless compression prevents the loss of any type of message but is unable to reduce the size of the file [6].

V. Applications

Image Steganography is used to secure private files and documents, hide passwords and encryption keys as well as to deliver highly confidential documents between governments globally and corporations without revealing the existence of the hidden message.

This also makes it essential in military as their communication can be monitored by other nations and banking field for secure communication of information like vault codes and personal information of clients and employees. It was very popular during World War II when spies on both sides of the war used steganography to pass secret messages [6]. It can also be used for criminal activities as it was suspected that Al-Qaeda used steganography in their attack on World Trade Centre [11]. Nowadays with the advent of Internet there is ever burgeoning need to protect and hide sensitive data. It is also used in copyright control, to improve efficiency of search engines which focus on images and for creating Identification Documents in which there are certain hidden characteristics in photos. It is also employed in the medical field where there is a need for separation of patient details from their medical imaging systems. Thus, image steganography plays a vital role in security as well as the communication of highly secret information [6]. It is generally used in tandem with cryptography for an additional layer of protection.

VI. TECHNIQUES

There are many techniques for implementing image steganography. Five of the major image steganographic techniques are:

A. Statistical technique
B. Distortion techniques
C. Spatial domain techniques
D. Transform domain techniques
E. Spread spectrum [1]

A. Statistical Technique

This technique takes the advantage of a weakness in human vision for not detecting luminance variation to modify the images' statistical properties while embedding the image in the cover file. These techniques are also called model-based techniques [5]. Statistical Steganalysis is performed by studying the changes in statistical properties to look for hidden data or any modification in the image [12]. Significant changes are made to statistical properties of the image only if the bit "1" is transmitted while it is unchanged in other cases. Thus, this technique exploits the existence of the "1-bit" in the image, where nearly a bit of data is embedded in a digital carrier [13]. Each image is divided into sub-images with each of this divided image referring to a single bit of the communication while sending multiple bits [14]. The disadvantage of this technique that it is susceptible to rotating, scaling and other attacks which can be prevented to some extent by using the elements in an image to select the sub-images.

B. Distortion Techniques

In the decoding process the variations between initial and transmitted image are analysed and for this complete information regarding both images is required. The original image is subjected to a series of alterations to create a steganographic object in this method. The information to be exchanged determines the alterations that must take place to achieve the desired result. Pixels are randomly chosen to encode the image. Any difference between the steganographic image and image used as cover results in the data bit being considered "1" but if the pixel is same for cover and embedded photo then the message bit is '0'. The unit '1' valued pixels are modified by encoder in a way that its statistical properties remain the same. This technique is also susceptible to rotating, scaling, resizing attacks. The cover image should be destroyed after using once. Most of the text-based steganography use distortion techniques [1].

C. Spatial Domain

In spatial sphere the information to be concealed is directly embedded in cover images within the intensity of pixels. The secret message is embedded in the image in place of the noise or least/insignificant bits present in the image in such a way that it is undetectable by human vision. The task is accomplished by any of the following methods:

- Least Significant Bit Substitution (LSB)
- Most Significant Bit (MSB) steganography
- RGB Based Steganography
- Pixel Value Differencing (PVD)

Least Significant Bit Substitution (LSB)

This is the most popular and the easiest image steganography technique in the spatial domain. The secret information to be transmitted is placed straight into the image which is to be used as cover by modifying pixels of image by replacing their least significant bits. At most four least significant values can be changed with the change being imperceptible by the human eye. The secret key chosen and exchanged by the two parties the sender and receiver determine the way in which this replacing is implemented in which of the two ways: differentially or randomly. This can be done by changing LSB in intensity or grey-scale or 24-bit images. There are two LSB steganography approaches namely: LSB replacement and LSB matching. In the first approach the secret message replaces the least significant bits of cover image. However, as the name suggests the bits which are least significant of both secret message and image used as cover are compared. If it's the same then it remains unaffected but wherever found different it's changed to secret message bits [6].

Most Significant Bit (MSB) steganography

Most Significant Bit (MSB) steganography approach is similar to aforementioned Least Significant Bit technique with the difference being that in MSB the most significant bits carry the hidden information rather than the least significant bits [15]. The advantage of this technique over its counterparts is that it allows copious amounts of data to be hidden and shared whereas the disadvantages are that the secret message may be easily detected using steganalytic techniques. Any compression, rotation or cropping of stego image will lead to the destruction of embedded information.

RGB Based Steganography

Each pixel in a coloured image of 24 bits consists of three components each comprising of 8 bits of Red, Green and Blue respectively with each of the primary colours representing 1 byte in each pixel. This technique works in the principle of modifying least significant bits of 3 or at times 4 to create parity bit patterns by rearranging colours which correspond to the hidden message [15]. LSB technique is used in RGB steganography but it is generally not very secure.

Thus, many other techniques are developed. One such technique corresponding to RGB steganography is pixel indicator technique in which one of the primary colours is chosen as the indicator of data present in the remaining channels. The indicator channels are employed sequentially with Red(R) being the first indicator in the first pixel while Green(G) and Blue(B) act as channel 1 and 2 respectively. In the following pixel G will be the indicator and R as well as B will be channel 1 and 2. Similarly, in pixel 3 is indicator while R and G are channel 1 and 2. The cover image contains the length of hidden information in the first 8 bytes. The downside of using this technique is that the capacity is dependent upon indicator bits and on image used as cover [16].

Pixel Value Differencing (PVD)

Wu and Tsai devised a new steganographic technique which came to be known as Pixel Value Differencing [17] in 2003. Pixel value differencing starkly contrasts the two earlier discussed steganography techniques. The number of bits of text which can be implanted in the image is determined with use of difference value between two successive pixels in a block in Pixel-value differencing steganography technique. A pair quantization range tables are employed in the technique proposed by the two scientists. In this technique the width range (8, 8, 16, 32, 64 ,128) is employed by the initial table in order to allow huge capacity whereas the other table employs the range of (2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64) that is used in providing a high degree of imperceptibility to the cover image [17]. A difference value d is computed from every block of two consecutive pixels which are non-overlapping of the cover image. All rows are scanned in a zig-zag manner to find two such pixel blocks. The difference is mapped in a range table which is divided into various ranges of specific width which indicates the number of bits of information which can be concealed in a block [16]. The value of d is replaced by separate value once the secret message is. This technique provides high imperceptibility and capacity to store the secret message.

It was observed that pixel value differencing steganography was vulnerable to histogram analysis attacks and a method for countering it was presented by Wang and Zhang [18] in which instead of taking fixed ranges, they proposed to utilize different ranges corresponding to various blocks [18].

D. Transform Domain Techniques

Transform domain steganography techniques employ the principle of first converting the image to frequency domain then transforming by embedding the secret information in the transform coefficients which is different form the techniques of spatial domain which alter the pixels directly [19]. This makes these techniques more complex than spatial domain techniques computationally. These techniques are also more resistant to attacks as they use more significant areas of the cover image to hide the information and are thus also used in to watermark the images [20]. Some of the most widely used techniques are:

- DCT (Discrete Cosine Transformation)
- DWT (Discrete Wavelet Transformation)
- DWT & SVD Image Steganography

DCT Image Steganography

This is the most popular transform domain image steganography technique. DCT image steganography has the advantage that it is based on digital image processing and thus it enjoyes virtues such as superior information incorporation, better compression and smaller amount of bit errors. This technique converts the image pixels in spatial domain to frequency domain for the detection of redundancy in pixels. Various spectral sub bands – high, middle and low frequency components are separated based on the visual quality. DCT coefficients determine the insertion of image. A lower than the threshold value of the coefficients results in embedding of secret information in the carrier image [20]. A technique has been introduced for JPEG images which uses every block of DCT coefficients. This technique is considered lossless while embedding information as in each block of medium frequency two successive zero coefficients are used for storing the data [21].

The image is split into 8 × 8 blocks which is followed by application of algorithm of two-dimensional form to each of these blocks in the chosen compression format which is generally jpeg. Confidential information is hidden in the least significant bit (LSB) of each DCT coefficient. Each block is transformed into the DCT using the equation

$$D(u,v) = \frac{1}{4}\mathrm{C(u)C(v)}\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right] \quad [22]$$

Here f(x, y) is the block of image pixels, and C(x) can have two values and is dependent upon value of x. If x is 0 then C(x) has value $1/\sqrt{2}$ and in all other cases it has value 1.

Inverse Discrete Cosine Transform (IDCT) is applied to each block of 8*8 in the JPEG decompression format. Most of the signal energy appears in top left corner of the DCT at low frequency for most images. Thus, compression is achieved at bottom dextral values which indicate greater frequencies which are generally so small that they can be skipped with negligible distortion compression imperceptible to the human eye can be obtained [23].

Algorithms to embed and retrieve the message in an image are given as follows:

Reading the cover image.

Reading the secret information and transforming it to binary form.

Splitting the image into blocks of 8×8 pixels.

Traversing horizontally from left to right and vertically from top to bottom and subtracting 128 in every pixel block.

Application of DCT to every block.

Compression of every block through quantization tables.

Calculating Least significant bits of coefficient and replacing them with secret message bits.

Write image obtained [20].

Algorithm to recover the secret information:

Read transmitted image.

This image is split into blocks of 8×8 pixels.

Traversing horizontally from left to right and vertically from top to bottom and

subtracting 128 in every pixel block.
Application of DCT to every block.
Each block is compressed through quantization table.
Calculating least significant bits of each discrete cosine coefficient.
Retrieval and conversion to character of each of 8 bits [20].

DWT Image Steganography

Discrete Wavelet Transformation unlike DCT does not affect the whole image but will affect it in a localised manner. The signal is divided forming high frequency and low frequency sections. The latter is further divided similarly into frequency sections high and low. The higher sections correspond to edges and this is where information is embedded as the human eye is less likely to notice changes in the edges [19].
Division of image by DWT results in four parts designated as lower (LL), horizontal (HL), vertical (LH) and diagonal (HH) components. Both rows and columns are subjected to low-pass filtering to obtain LL sub band which holds a crude account of the photo. In two dimensional applications there are levels of decompositions. Four sub-bands are formed after the first decomposition:

- LL_1
- LH_1
- HL_1
- HH_1

The lower resolution approximation component bands of preceding levels are utilized for input for decompositions that follow. After performing secondary decomposition on the band LL_1, it further decomposes to form the following bands:

- LL_2
- LH_2
- HL_2
- HH_2

Horizontal decomposition is followed by vertical decomposition at each level.
Discrete wavelet transform is performed on digital images. The image divides into 4 parts -

1. LL – This part contains the most important information regarding the overall image and is required in the image reconstruction process [24]. On the coordinates (x, y) low pass filter (LPF) is applied to obtain this component.

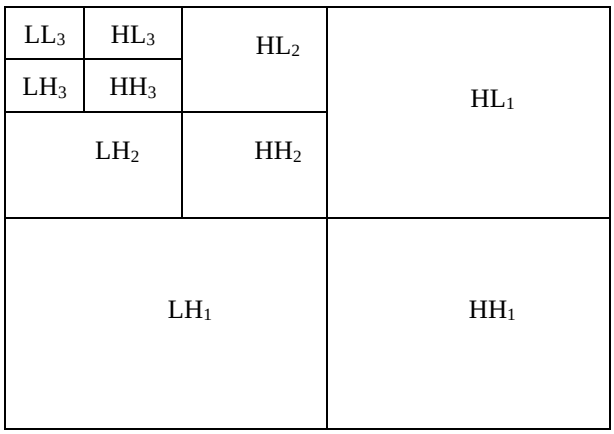

Fig- 2 Three phase decomposition [19]

2. LH & HL – On one coordinate Low-Pass filter is applied while on the other coordinate High-Pass filter is used and thus the two components are obtained.
3. HH - Apply High-Pass Filter on each of the coordinates to obtain component having large frequency in the crosswise direction [6].

As the LL sub-band carries the most significant details of an image and thus the secret information is embedded in this part to prevent it from attacks [19]. Quality of images remains intact and human eye cannot discern the changes [25]. Wavelets are relatively new in the image processing and offer lesser distortion and are less resource hungry as compared to DCT and are thus employed for noise reduction, edge detection in image processing [11].

Algorithm for embedding information:
Analysing the information to be embedded as well as the image to be used as cover.
On this image apply the two-dimensional haar transform and convert the text to be transmitted to binary,
In both the directions search the coefficients of filtering. Cover image is attached with data For discrete wavelet transform coefficients attach data bits to image used as cover.
Obtain the embedded image.
Determine various parameters like PSNR for evaluating the concealment of image.

Algorithm for recovering secret information
Analyse the embedded steganographic image.
Filtering coefficients in both directions – horizontal and vertical are identified and the secret information is reconstructed one bit at a time.[26]
Differentiate the message vector obtained by translating the data with the initial information.

DWT and SVD Steganography

This technique in addition to having DWT also has decomposition of singles value done to cover as well as the embedded images for increased imperceptibility. The singular value decomposition (SVD) is matrix factorization having a large number of uses including processing signals as well as analysing data.
Algorithm to implement this technique is as follows

Ideal image to be used as cover as well as secret are selected.
The four sub bands are obtained by applying DWT on both images.
SVD is applied to isolate the RGB parts of both images.
The secret information is implanted into the cover image after the components of SVD matrix are integrated. This gives the embedded/steganographic image.
IDWT is taken.
Secret information is extracted by reversing the steps mentioned above [23].

The image quality of the image obtained from DWT and SVD method is high as it has been found to have the best PSNR value and the lowest bit error rate.

E. Spread Spectrum

Spread spectrum transmission communication is generally utilized for radio communication as it is used to transmit messages below noise level. Spread spectrum image steganography can follow two approaches – either using the cover image as noise or by adding pseudo noise to the cover image. In the first approach the system introduces to the cover image a single value which is below noise level. In the second scenario a pseudo or false noise/data is added throughout the cover image. This makes it almost impossible to detect the hidden information [1] and is more popular of the two methods. For the restoration of the message the cover image is not needed as a cross-correlation among steganographic image and the regenerated carrier is done [27].

The process of encoding using this technique consists of the following major steps:

Redundancy is introduced to create encoded information through error correcting code
It is ensured that the message which has been encoded remains of a fixed size by including padding
Message to be encoded is interspersed.
A pseudorandom sequence of noise (n) is created.
Use encoded message, m using advanced encryption standard (AES) to modulate the sequence, generating noise, s.
This noise is then added to the image being used as cover (f) for the secret information [28].

Extraction of hidden information is done by following the steps below:

A rough idea of original image (f) is by filtering the steganographic image (g) which has been transmitted.
An estimate of noise (s) which was added by the embedder is calculated by subtracting estimate of original image obtained in above step and the steganographic image.
A pseudorandom sequence of noise (n) is created.
Noise extracted is then compared with the regenerated noise to demodulate image.
Advanced decryption standard (ADS) is used and padding is removed to deinterleave the approximation of message encoded.
The secret information is repaired using error correcting decoder [28].

Given below are two methods which are analogous to spread spectrum and are often combined with Spread Spectrum Image Steganography System (SSIS).

Image Restoration

Extraction must be done at the receiver side in order to decode information properly. The implementation of image restoration by the system is done to filter a significant amount of the embedded signal with low power from the image which was received in order to obtain an approximation of native image. An approximate signal is obtained by continuously deducting the image restored from the received image [29]. Alpha trimmed mean filter is applied for this purpose, thus generating targeted pixels by using a mean average concept [30].

Error Control Coding (ECC)

The secret message decoded after restoring the original image contains a large number of error bits. This happens because the embedded signal works on low power mode and the approximation of this signal can be very inaccurate which resilts in the information obtained being riddled with error bits [29]. Spread Spectrum Image Steganography System can also use ECC which has the ability of high signal approximation. Using error correction by SSIS compensates for optimal estimation of the embedded signal, in addition to battling with distortion present.

VII. Challenges and Future of Image Steganography

With the advent of internet image steganography is more prevalent than ever as images have become one of the most widely shared forms of media and its security is also important and steganography is used in tandem with cryptography and becomes especially crucial where cryptography is not an option. There are some challenges being faced in the field of image steganography.

The main requirements of image steganography are that the information hidden in the cover image should be undetectable, highly secure and should be robust to steganographic attacks while having high payload capacity. Even after extensive research in the field all these requirements are not achieved fully. As the steganographic properties are related improving some of them might lead to decrease in efficiency of others and this is a major problem whose solution is yet to be found [31].

Some of the changes and improvements that can be done to the current practices in the domain of image steganography are:

1. As nowadays the processors are extremely capable and computation cost is not a major factor therefore transform domain techniques should be utilized for advance steganographic techniques as they while being more complex than spatial domain techniques offer many host planes from original image providing better locations for embedding the secret information.
2. Adaptive embedding techniques should be utilized more they in addition to improving the efficiency of information embedding also provide better protection to steganographic attacks. Machine learning should be utilized to store the data with lower distortion than conventional techniques and for choosing coefficients.
3. Secret keys and encryption algorithms can be incorporated into image steganography for more robust security and protection from attacks as compared to the traditional approach. This will provide an added layer of security to the secret message.

4. As two-dimensional (2D) images are more popular and provide a more efficient throughput than three-dimensional (3D) image as embedding process in 3D images are very complex. So, efforts should be done to improve 2D steganography while 3D images should be used for advanced steganography [31].
5. It has been recently observed that the choice of appropriate cover images also has an effect on the steganographic attacks. So, in addition to focusing on the best location for embedding secret data the choice of cover image is also of great significance [32]
6. Use of optimization algorithms like genetic algorithms, fuzzy logic, neural networks should be incorporated to improve the embedding process and encryption algorithms like RSA, DES should be used to improve security [32].

Research on image steganography is being carried out primarily in the following areas:

1. Security and Mathematics relationship in Steganography

Capacity expansion in region of data transferring often leads to decreased security.

We have discovered that increasing capacity has resulted in decreased security and there appears to be a trade-off between the two. Some mathematical model should be devised relating the two and observing their relationship. Further optimized algorithms should be developed to increase capacity without sacrificing security [33]. A roadblock in this area of research has been that it is very difficult to model the statistical features of images [34].

2. Developing algorithms based on objects in images

Due to advancement in staganalysis object-oriented algorithms are being developed which aim to target specific parts of images [34]. Embedding of secret information is performed over areas known as Regions of Interests which offer minimum distortion in the cover image. Human skin-tone is an example of these objects as it falls inside the threshold value in HSV colour space [35]. Various algorithms are being devised for this method. In one such algorithm, information is embedded using a skin tone detector mechanism is used to find pixels of skin tones by using Discrete Wavelet Transform (DWT) for selecting sub band from images in RGB format [36]. A drawback of this technique is that steganalysis methods can detect the changes in integrity of the cover image caused by overwriting of bits. Thus, algorithms which causes smallest amount of replacement of bits should be chosen.

3. Improving steganographic algorithms

Following are the approaches that can be adopted to increase robustness and performance of algorithms

- Increasing embedding efficiency.

Overwriting of bits in current techniques like overwriting of LSB in spatial domain remains a major problem as it alters the properties of image and thus it is important to develop algorithms which offer the lowest rate of overwriting [33]. An example is the F5 algorithm which has one of the lowest overwriting properties [37]. One such way is to integrate the secret message right at the creation of the cover image as opposed to altering it afterwards.

- Decreasing embedding distortion

The embedding process can produce distortion in the images. The statistical properties should be adjusted after the embedding process; In the spatial techniques overwriting of bits should be avoided by changing pixel component while in transform techniques when all transform coefficients are not utilized modification should be done into the coefficients which result in lowest distortion after the embedding process [33]. For reducing these embedding distortions schemes based on perturbed quantization can be utilized [38].

- Choosing alternate color spaces

Most of the steganographic technique use RGB and Grey scale images but it has been observed that colour spaces like HSV (Hue Saturation Value) and the YCbCr (Yellow Blue Chromaticity Red-Chromaticity) provide a better performance with regards to image steganography as the level of distortion is noticeably less as compared to the traditional colour spaces and thus provide an exciting area for further research [33].

VIII. CONCLUSIONS

Image steganography over the decades has advanced very much as digital images have become the most popular form of media in large part due to the introduction of the internet and it is now common for people to post their images on various social media platforms [39]. When coupled with cryptography, Image steganography provides increased protection and is thus employed by banks ,military and the educational field.. The various types of techniques have been developed in spatial and transform domain and are still being improved in regards to performance evaluation parameters like PSNR values with help of steganalysis. Research in this field is being done to improve techniques further in areas like improving capacity without compromising security, more robust encryption integration etc.

REFERENCES

1. Hamid, N., Yahya, A., Ahmad, R.B. and Al-Qershi, O.M. (2012). “Image steganography techniques: an Overview”. International Journal of Computer Science and Security (IJCSS), Volume 6, Issue 3, pp.168-187.
2. Halim, S.A., Sani, M.F.A. (2010). “Embedding using spread spectrum image steganography with GF (2^m),” in Proc. IMT-GT-ICMSA, pp. 659-666.
3. Morkel, T., Eloff, J.H.P., Oliver, M.S. (2005). “An overview of image steganography.” in Proc. ISSA, pp. 1-11.
4. Simmons, G.J. (1983). “The prisoners problem and the subliminal channel,” Advances in Cryptology, pp.51–67.
5. Chandramouli, R., Kharrazi, M., Memon N. (2004). “Image Steganography and Steganalysis: Concepts and Practice”. In: Kalker T., Cox I., Ro Y.M. (eds) Digital Watermarking. IWDW 2003. Lecture Notes in Computer Science, Vol 2939. Springer, Berlin, Heidelberg
6. Atawneh, S., Ammar Almomani, A., Putra, S. (2013). “Steganography in digital images: Common approaches and tools” IETE Technical Review, Volume 30, Issue 4, pp. 344-358

7. Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R., Shamsuddin, M.Z.I. (2003). "Information hiding using steganography," 4th National Conference of Telecommunication Technology. NCTT Proceedings., Shah Alam, Malaysia, pp. 21-25.
8. Krenn, R. (2004). "Steganography and steganalysis" An Article, Santa Barbara, California, January, available from: http://www.krenn.nl/univ/cry/steg/article.pdf [Last accessed on 17 August 2019]
9. Pradhan, A., Sahu, A., Swain, G., Krovi, R.S. (2016). "Performance Evaluation Parameters of Image Steganography Techniques". International Conference on Research Advances in Integrated Navigation Systems. pp 1-8.
10. Lin,C.C. (2011). "An information hiding scheme with minimal image distortion," Computer Standards and Interfaces, Volume 33, Issue 5, pp. 477-84.
11. Bachrach, M., Shih, F.Y. (2011). "Image Steganography and Steganalysis," Wiley Interdisciplinary Reviews: Computational Statistics, Volume 3, pp. 251-259.
12. McBride, B.T., Peterson, G.L., Gustafson,S.C. (2005). A new blind method for detecting novel steganography, Digital Investigation, Volume 2, pp. 50-70.
13. Katzenbeisser, S.C. (2000). "Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, pp. 43-78
14. Kruus, P., Scace C., Heyman, M., Mundy, M. (2003). "A survey of steganography techniques for image files." Advanced Security Research Journal, pp. 41-52
15. Rejani., R., Murugan, D., Krishnan D.V. (2015). "Comparative Study of Spatial Domain Image Steganography Techniques." Int. J. Advanced Networking and Applications, Volume 7, Issue -2 pp. 2650-2657
16. Swain ,G., Lenka, S. (2014). "Classification image steganography techniques in spatial domain: A study". Int J Comput Sci Eng Tech, Volume 5, pp 219-232.
17. Hsien-Wen Tseng, Hui-Shih Leng, (2013). "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics, Volume 2013, Article ID 189706, pp. 1-8. http://dx.doi.org/10.1155/2013/189706]
18. Zhang, X., Wang, S. (2004). "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, Volume 25, Issue 3 pp.331-339
19. Tushara M., Navas, K.A. (2016). "Image Steganography Using Discrete Wavelet Transform – A Review", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEIC) nCORETech , Volume 3, Special Issue 1, February 2016.
20. Purohit, A., Sridhar, P.S.V.S. (2014). "Image steganography: A review." International Journal of Computer Science and Information Technologies, Volume 5, Issue 4, pp. 4891-4893.
21. Chang, C.C., Lin, C.C., Tseng C.S., Tai, W.L. (2007). "Reversible hiding in DCT based compressed images", Information Sciences, Issue 177, pp. 2768–2786.
22. Johnson, N.F., Jajodia, S. (1998), "Exploring steganography: Seeing the unseen," IEEE Computer Society Press, Volume 31, Issue 2, pp. 26-34.
23. Vaishali P, Bhat, P. (2015). "Transform Domain Techniques for Image." International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering and National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015), Alva's Institute of Engineering and Technology, Moodbidri, Volume 3, Special Issue 1, pp. 65-68
24. Abdelwahab, A.A., Hassaan, L.A. (2008). "A discrete wavelet transform based technique for image data hiding" in National Radio Science Conference, Tanta Univ., Cairo, pp. 1-9.
25. Zagade, S., Bhosale, S. (2001). "Secret Data Hiding in Images by using DWT Technique's", International Journal of Engineering and Advanced Technology (IJEAT), Volume 3, Issue 5, pp. 230-235.
26. Kaur, G., Kochhar, A. (2013). "Transform Domain Analysis of Image Steganography", International ournal for Science and Engineering Technologies with Latest Trends", Volume 6, Issue 1, pp 29-37.
27. Bhatia, M.P.S., Muttoo, S.K., Bhatia, M. (2015). "An Image Steganography Method Using Spread Spectrum Technique", Proceedings of Fourth International Conference on Soft Computing for Problem Solving, Volume 336, pp. 219-236.
28. Padmasri, B., Amutha Surabi, M. (2013). "Spread Spectrum Image Steganography with Advanced Encryption Key Implementation", International Journal of Advanced Research in computer Science and Software Engineering, Volume 3, Issue 3.
29. Marvel, L.M., Boncelet, C.G., & Retter, C.T. (1999). "Spread spectrum image steganography" in IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, Volume 8, Issue 8, p.p. 1075-83. doi: 10.1109/83.777088
30. Bednar, J.B., Watt, T.L. (1984). "Alpha-trimmed means and their relationship to the median filters," IEEE Trans. Acoustics, Speech, Signal Processing, Volume ASSP-32, no. 1, pp. 145–153.
31. Kadhim, I.J., Premaratne, P., Vial, P.J., & Halloran, B. (2019). "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research". Neurocomputing, Volume 335, *pp. 299-326.* https://doi.org/10.1016/j.neucom.2018.06.075
32. Subhedar, M.S, Mankar, V.H. (2014). "Current status and key issues in image steganography: A survey." Computer Science Review, Volumes 13-14, pp. 95-113. https:// doi.org/10.1016/j.cosrev.2014.09.001
33. Roy, R., Changder, S., Sarkar, A., Debnath, N.C. (2013). "Evaluating image steganography techniques: Future research challenges." 2013 International Conference on Computing, Management and Telecommunications (ComManTel), Ho Chi Minh City, pp. 309-314. doi: 10.1109/ComManTel.2013.6482411.
34. A. Cheddad, A., Condell, J., Curran, K., Kevitt, P. Mc. (2008). "Biometric inspired digital image Steganography", Proceedings of the 15th Annual IEEE International Conference and Workshops on the Engg.of Computer-Based Systems (ECBS'08), Belfast, pp. 159-168.
35. Sobottka, K., Pitas, I. (1996). "Extraction of facial regions and features using color and shape information.", Proc. IEEE International Conference on Image Processing, pp. 483-486.
36. Shejul, A.A., Kulkarni, U.L. (2011). "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Volume 3, Issue 1, pp. 16-22.
37. Westfeld, A. (2001). "F5-A Steganographic Algorithm: High capacity despite better steganalysis," Proc. 4th International Workshop on Information Hiding, Volume 2137, pp. 289-302, Springer, 2001.
38. Fridrich, J., Pevný, T., Kodovský, J. (2007). "Statistically Undetectable JPEG Steganography: Dead Ends, Challenges and Opportunities", Proc. 9th Workshop on Multimedia and Security, ACM, New York, USA, pp. 3-14. Doi - 10.1145/1288869.1288872
39. Mandal, M., Banik, G., Chattopadhyay, D., Nandi, D. (2012). "An image encryption process based on Chaotic logistic map," IETE Technical Review, Volume 29, Issue 5, pp. 395-404.

AUTHORS PROFILE

Vimanyu Chopra is an undergraduate scholar at DAV Institute of Engineering and Technology, Jalandhar, Punjab, India.

Devinder Priyadarshi is Assistant Professor in Department of Mechanical Engineering at DAV Institute of Engineering and Technology, Jalandhar, Punjab, India.