“ It's great to say you have an app or an idea that does X, Y, or Z, but unless that solves a real problem for people they're not going to use it. And the question is what problem are you solving?”
-Kevin Systrom,instagram creator-

Before discussing the main existing solutions in image steganography,the question is “What problem is image steganography solving ?”

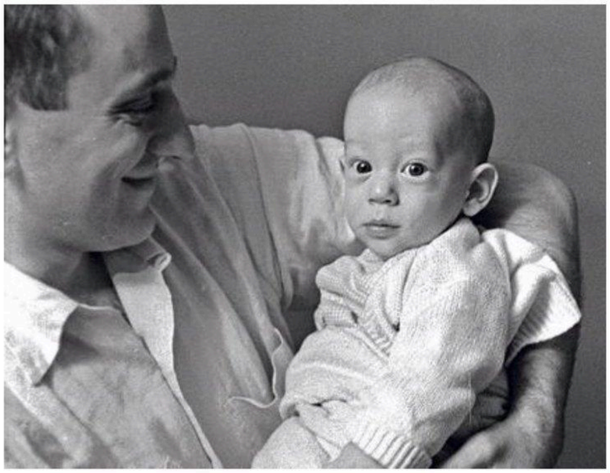
The primary challenge facing image steganography is maintaining a balance between hiding data effectively while ensuring the imperceptibility of the modifications to the carrier image.

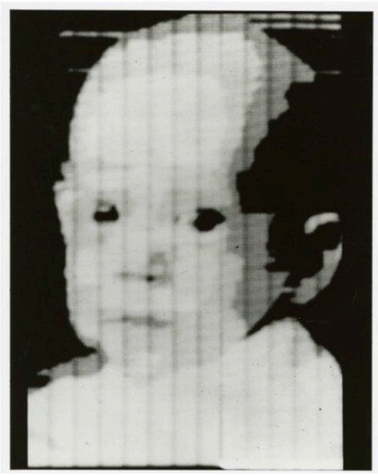
Image Files

“Every pixel tells a story, waiting to be revealed”

What is a pixel, and what story does it conceal? How does this concept pave the way for understanding steganographic techniques?

When people first faced the problem of how to show a picture on a screen, they had to come up with a way to break the image down into data. In 1957, an early computer engineer named Russell Kirsch took a picture of his infant son and scanned it.It was the first digital image, a grainy black and white baby picture, and that's how the pixel was born.





Pixels are an interesting concept because you can't see them very easily, but actually if you get a magnifying glass and you go up to a screen, you actually can see that your screen is made up of tiny dots of little light. What's more interesting is that those tiny dots of little light are actually multiple tiny dots of little light of different colors. There's red, green, and blue.Pixels together,from far away,create an image.

We use our computers daily. That's why we're hearing the term resolution a lot, both in computer science and manufacturers of devices.Resolution is basically the dimensions by which we can measure how many pixels are on a screen. Back in the days it was 640 by 480. And today it's a lot bigger. And then there's the question, not only of resolution but also of density. So for instance, on modern smartphones, they fit the same number of little lights called pixels, but in a denser space. And it's what allows us to get sharper images.

Now, how do we store those values of the pixels in a file?

So what we do is we store the red, green and blue values in little triplets, effectively with different values that each make up a single pixel. So the values range from 0 to 255. Zero would be very dark, 255 would be very bright, and triplets of these values together compose a single pixel.

An image file, whether it's a Jpeg, GIF, PNG, etc. contains millions of these RGB triplets.
So how does a computer store all that data?

All computing and digital data are represented by **bits**. A bit has two states. It's on or it's off, but instead of on or off, computers use ones and zeros.So an image file is actually just a bunch of ones and zeros.

But why do RGB values go from 0 to 255?

Turns out that each color channel RGB is represented by eight bits, which together are called a byte. If you know the binary number system, you know that the maximum number eight bits can represent is 255, which is equal to eight ones in a row, and the lowest is 0 or 8 zeros in a row. Therefore, 0 to 255 gives us 256 different intensities per color channel. We could represent a pixel of the color turquoise, for example, and our traditional decimal based number system as 64 for a little red, 224 for a lot of green and 208 for some blue. But a computer would have stored it as 010000001110000011010000. We use 24 binary digits to represent this one pixel.

The most prominent **image formats**, exclusively on the internet, are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, and to a lesser degree, the portable network graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure

Image compression

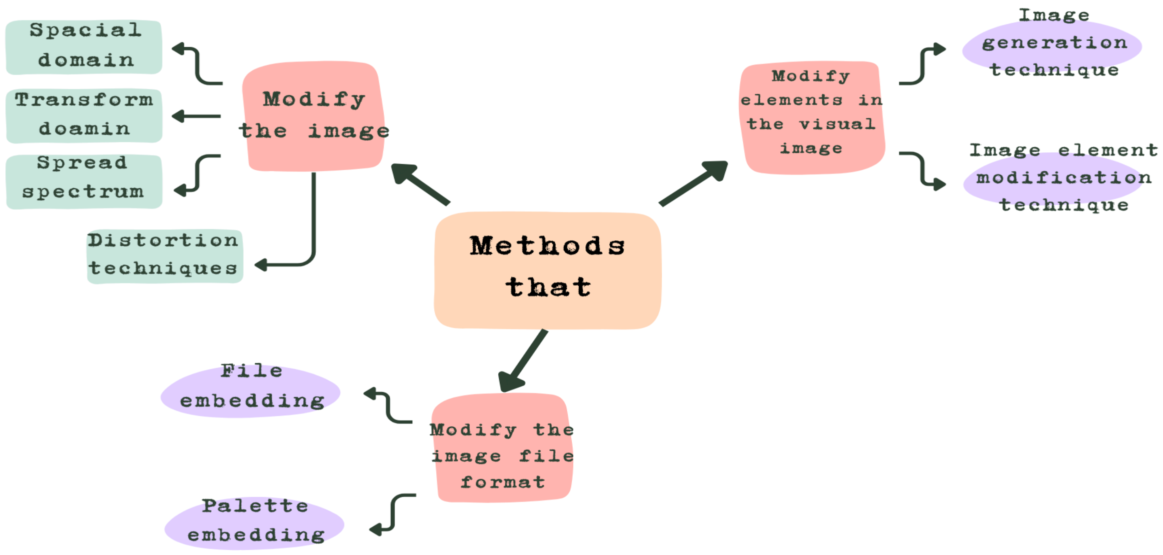
The objective of image compression is to reduce irrelevance and redundancy of the image data to be able to store or transmit data in an efficient form. It is concerned with minimizing the number of bits required to represent an image. Image compression may be lossy or lossless.

- **Lossless compression** is known for being preferable when the original data should stay in its entirety. In this manner, the original image information will never be removed, and this makes it possible to reconstruct the original data from the compressed data. This is typical of images in GIF and BMP

- **Lossy compression** saves storage space by discarding the points the human eyes find difficult to identify. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. JPEG compression uses this technique. A cover image is the image designated to carry the embedded bits or secret information

The main advantages of compression are reductions in storage hardware, data transmission time, and communication bandwidth. This can result in significant cost savings. Compressed files require significantly less storage capacity than uncompressed files, meaning a significant decrease in expenses for storage.

Classification of Steganographic techniques


Spacial domain
Transform doamin
Spread spectrum
Distortion techniques
Modify the image
Modify elements in the visual image
Image generation technique
Image element modification technique
Methods that
File embedding
Modify the image file format
Palette embedding

There are numerous approaches to classifying steganographic techniques, although in some cases, exact classification is not possible.

In general, the process of embedding can be defined as follows: Let C denote the cover carrier, and $C^{\sim}$ the stego-image. Let K represent an optional key (as a seed used to encrypt the message or to generate a pseudo-random noise, which can be set to {φ} for simplicity), and let M be the message to be sent. Then, Em represents an embedded message and Ex represents the extracted message. Therefore,

$Em : C \oplus K \oplus M \rightarrow C^{\sim}$

$\therefore Ex(Em(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M$

To distinguish between different steganographic techniques in a wide sense, one must take into consideration both the methods that :

- modify the image

- modify the image file format.

The important issue to mention here is the main role compression usually plays when it comes to deciding which steganographic algorithm is better. Though lossy compression methods result in smaller image file sizes, they increase the possibility of the partial loss of an embedded message because surplus image data is to be eliminated in these techniques. Lossless compression does not compress the image file as much. As a result, researchers have come up with different steganographic algorithms that suit such compression types.

Steganographic techniques that modify image files for hiding information include the following:

- Spatial domain
- Transform domain
- Spread spectrum
- Statistical methods and
- Distortion techniques

Steganographic techniques that modify the image file format involve

- file embedding and
- palette embedding.

In addition, there are techniques that modify the elements in the visual image including:

- The image generation technique and
- The image element modification technique

Finally, there is a special type of the spatial and transform domain techniques called the adaptive steganography technique.

Spatial domain steganographic techniques

Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be a bit negligible when compared to the human visual system (HVS).One of the ways to do so is to hide information in the least significant bit (LSB) of the image data. This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image.

The embedding operation of LSB steganography is described by the following equation:

$$Yi = 2\left|\frac{x_i}{2}\right| + m_i$$

where mi, xi , and yi are the i-th message bit, and the i-th selected pixel value before and after embedding, respectively.

Let $\{P_x(x=0), P_x(x=1)\}$ denote the distribution of the least significant bits of the cover image, and $\{P_m(m=0), P_m(m=1)\}$ denote the distribution of the secret binary message bits. The message is to be compressed or encrypted before being embedded just to protect its secrecy. According to this, the distribution of the message may be assumed to equal an averaged distribution, such that

$\left\{P_m(m=0) \approx P_m(m=1) \approx {}^{1}\!/_{2}\right\}$.

In addition, the cover image and the message may also be assumed to be independent. Therefore, the noise introduced into the image may be modeled as:

$$P_{+1} = \frac{P}{2} P_x(x=0),\ P_0 = 1 - \frac{P}{2},\ P_{-1} = \frac{P}{2} P_x(x=1)$$

Where P is the embedding rate, measured in bits per pixel (bpp). The embedding process described above makes it clear to what extent it is possible to extract the secret message bits directly from the LSBs of these pixels already selected during this process. When hiding the message bits in the image using LSB algorithms, there are two schemes, namely sequential and scattered. The LSBs of the image, in the sequential embedding scheme are replaced by the message bits, whereas in the case of the scattered embedding scheme, the message bits are randomly scattered throughout the image using a random sequence to control the embedding sequence. The well-known steganographic tools based on LSB embedding are different as far as the way they hide information is concerned. Some of them change the LSB of pixels randomly, others modify pixels not in the whole image but in selected areas of it, and still others increase or decrease the pixel value of the LSB, rather than change the value.

Advantages

From the above, we conclude that the resulting changes to the cover image using LSB techniques are very difficult to be recognized by the human eye due to their being too small.
Moreover, such techniques are simple and popular.

The disadvantage of this technique is that it uses each pixel in the image. As a result, if lossy compression is used, some of the hidden information might be lost

Transform Domain Techniques

The transform based techniques utilizes the domain specific characteristics of image to embed data on it and for performing it the image firstly transformed to that domain like frequency domain (DCT, DFT), wavelet domain (DWT), curvelet domain etc. in these techniques the data is embedded on the transformed image instead of direct pixels (as in spatial domain) and then the image is retransformed to spatial domain the advantage of the algorithm is that the information can be embedded in are as of the image that are less exposed to compression, cropping, and image processing also the information in one component of transformed domain spreads over larger number of pixels or even in whole image. This reduces the possibility of removal of information by any attack or operation. Although this is a more complex way of hiding information in an image. Transform domain techniques are broadly classified into:

- Discrete Cosine transform (DCT) based technique
- Discrete Fourier transform (DFT) based technique.
- Discrete Wavelet transform (DWT) based technique.
- Integer Wavelet Transform (IWT) based techniques.

- Discrete Curvelet Transform (DCVT) Based techniques.

Discrete Cosine transform (DCT) based technique

DCT is a general orthogonal transform for digital image processing and signal processing. It has the advantage of high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted . The literature survey reveals that mostly the middle frequency bands are chosen because embedding the information in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted. Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to\ embed a single bit of information into a DCT block.

Discrete Fourier transform (DFT) based technique

The DFT based technique is similar to the DCT based technique but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions. Although it increases the overall complexity of the process.

Discrete Wavelet transform (DWT) based technique

A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyze a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). This method transforms the object in wavelet domain, processes the coefficients and then performs an inverse wavelet transform to represent the original format of the stego-image object. Wavelet analysis can be of two types: continuous and discrete. Analyzing the signal at different frequencies with different resolutions is Called multi-resolution analysis (MRA). The DWT divides an image into four parts namely a lower resolution approximation component (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL subband is obtained after low-pass filtering both the rows and columns and contains a rough description of the image. The HH sub-band is high-pass filtered in both directions and has high-frequency components along the diagonals. The HL and LH sub bands are the results of low-pass filtering in one direction and high-pass filtering in the other direction. After the image is processed by the wavelet transform, most of the information contained in the host image is concentrated into the LL image. The LH sub band contains mostly the vertical detail information which corresponds to horizontal edges. HL band represents the horizontal detail information from the vertical edges. The process can be repeated to obtain multiple scale‟ wavelet decomposition”

Integer Wavelet Transform (IWT) based techniques

Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers the output can be completely characterized with integers .

Discrete Curvelet Transform (DCVT) Based techniques

This curvelet transform is one of the new forms / members of this family of multiscale geometric transforms. This concept is used for showing edges better than the forms of wavelet, Curvelet transform offers an effective solution to the problems associated with image steganography using Wavelets and DCT (Discrete Cosine Transform).

Advantages of transform domain techniques are:

1. There is less chance for removal or loss of the hidden data.
2. Information is distributed over the whole image.
3. Provides much higher flexibility for hiding data.
4. Typically independent of the image format.

Disadvantages of transform techniques are:

1. Greater understanding of the embedding domain required.
2. Careful selection of embedding coefficients required otherwise it can cause degradation of image.
3. Higher Mathematical Complexity.
4. Relatively Low embedding capacity.

Spread Spectrum Technique

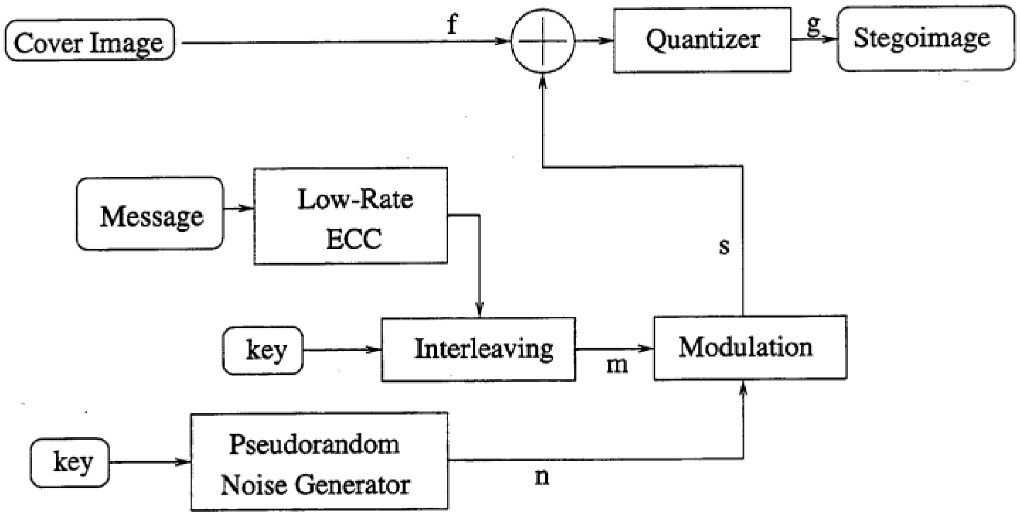
Spread Spectrum Image Steganography (SSIS) works by storing a message as Gaussian noise in an image (Marvel, Boncelet, and Retter 1998, Marvel et al. 1999).

In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible not only to the human eye but also through computer analysis without access to the original image.

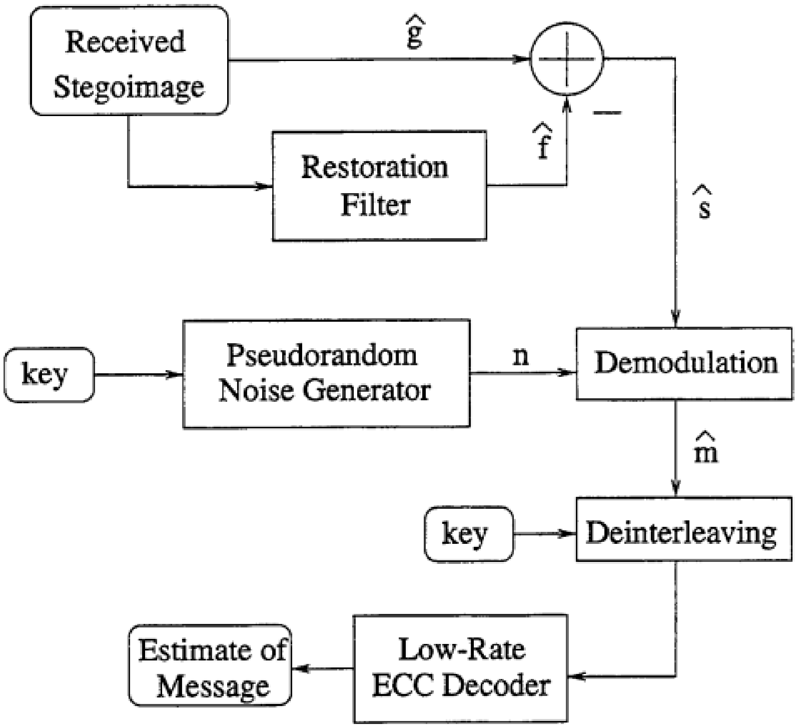
The process consists of the following major steps:

1. Create encoded messages by adding redundancy via error-correcting code.
2. Add padding to make the encoded message the same size as the image.
3. Interleave the encoded message.
4. Generate a pseudorandom noise sequence, n.
5. Use encoded message, m, to modulate the sequence, generating noise, s.

6. Combine the noise with the original image, f.



Simplified Steganography Embedder



Simplified Steganography Extractor

The reverse process, of extracting and restoring the original message, is of course very similar:

1. Filter the stego image, g, to get an approximation of the original image, f^.
2. Subtract the approximation of the original image from the stego image to get an estimate of the noise, s^, added by the embedder.
3. Generate the same pseudorandom noise sequence, n.
4. Demodulate by comparing the extracted noise with the regenerated noise.
5. Deinterleave the estimate of the encoded message, m^, and remove the padding.
6. Use error-correcting decoder to repair the message as needed.

Distortion Techniques

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion.

Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit.

The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, then the message bit is a “1.” Otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected (which is different from many LSB methods). However, the need for sending the cover image limits the benefits of this technique. As in any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, rotating, or scaling, the receiver can easily detect the modification. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be fully recovered.

An early approach to hiding information was to do so in text. Most text-based hiding techniques are of the distortion type. For example, the layout of a document or the arrangement of words might show or reflect the presence of information. Considering one of these techniques, it can show the adjustment of the positions of lines and words where spaces and “invisible” characters are added to the text, providing a method of sending hidden information .

File Embedding

Different image file formats are known for having different header file structures. In addition to the data values, such as pixels, palette, and DCT coefficients, secret information can also be hidden in either a header structure or at the end of the file. For example, the comment fields in the header of JPEG images usually contain data hidden by the invisible Secrets and Steganozorus. Camouflage, JpegX, PGE10, and PGE20 add data to the end of a JPEG image.

Image storage formats such as TIFF, GIF, PNG, and WMF have a file header that can be exploited to hide arbitrary information. In this case, that arbitrary data may be a secret message. It is possible to append data to many image storage formats without affecting the image. When the image is processed for display, the image user will decode the image size from the file header, and any tracking information attached to the end of the file will be ignored. Using this technique, it is possible to attach a message of any size to a cover image. However, the message could be removed from the cover image by simply resaving the image in the same file format. The limitations of this method are that despite the large payload, it is not that difficult to identify and defeat, it is weak when lossy compression and image filtering are concerned, and the resaving of the image implies complete loss of hidden data.

Pallet Embedding

In a palette-based image, what matters is the fact that only a subset of colors from a particular color space is used to colorize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colors as a list of indexed pairs ,(i ,ci), assigning a color vector ci to every index i , and the actual image data, which specifies a palette index for each pixel, rather than the color value itself. The file size gets decreased via this approach when only a limited number of color values are used in the image. Two of the most popular formats are the graphics interchange format (GIF) and the bitmap format (BMP). However, owing to the availability of advanced compression techniques, their use has diminished .

In some cases, the palette itself can be used to hide secret information. Because the order of the colors in the palette usually does not matter, the ordering of colors can be used to transfer information. In essence, a hidden message can be embedded using the difference between two colors in the palette (i.e., one secret message bit for every two colors in the palette). Color palettes are used to minimize the amount of information images that are used to represent colors .

Since steganographic messages within the bits of the palette and/or the indices are embedded in the palette-based steganography, one must be careful not to exceed the maximum number of colors.

Image Generation Technique

Many techniques have been proposed that encrypt messages so that they are unreadable or as secret as possible. Big Playmaker hides information by converting the secret text message into a larger and a slightly manipulated text format. The same principle can be employed in image creation, in which a message is converted to picture elements and then collected into a complete stego-image. This method cannot be broken by rotating or scaling the image, or by lossy compression. Parts of the message may be destroyed or lost because of cropping, but it is still possible to recover other parts of the message by encoding the message with error correcting information. Generally, this technique uses pseudo-random images, because if a malicious third party detects a group of images passing through a network without any reason for them being there (i.e., random images), he or she may suspect that the images contain secret information and block their transmission.

Image Element Modification Techniques

Some steganographic techniques do not try to hide information using the actual elements of the image. Instead, they adjust the image elements in completely undetectable ways, for example, by modifying the eye color or hair color of some person in a photograph. These modifications can then be used to carry the hidden information. In addition, this information will survive rotations, scaling, and lossy compression. The feasibility of modifying objects within images as a tactic for hiding information has been discussed by . It is important to keep in mind that when this method is used, the same cover image must not be used more than once, because the elements used will become apparent. This technique can be achieved manually with any photo editing software. With the advent of computer vision systems that identify objects within pictures, these methods have become more viable.

Adaptive Steganography

Adaptive steganography is a special case of the spatial and transform techniques. Moreover, it is introduced as statistics-aware embedding and masking. Global statistical characteristics of the image are basically used before any attempt to deal with its frequency transformed coefficients. These statistics decide what changes can be made. A random adaptive selection of pixels actually characterizes this method, relying on the cover image and the selection of pixels in a block with a large standard deviation (STD). The latter is intended to avoid areas of uniform color, such as smooth areas. This technique is known for exploiting images with existing or deliberately added noise and with images that show color complexity.

An adaptive technique applied to the LSB substitution method has been proposed in [56]. The idea behind this method is to make use of the correlation between neighboring pixels so as to calculate the degree of smoothness. The researchers shed light on the options of having two-, three-, and four-sided matches. The payload (embedding capacity) they were able to obtain was high.

A technique called the “adaptive more surrounding pixels using” (A-MSPU) technique, which improves the imperceptibility problems of multiple base notational systems (MBNS). This technique pays attention to the edge areas of a cover image while reexpressing the secret bits in multiple base notational systems. The suggested approach uses the same probability parameter to get the secret bits scattered and it also uses surrounding pixels with the maximum number to determine the capacity of every target pixel. Most steganographic techniques use either three or four adjacent pixels of a target pixel. The proposed technique is able to utilize all eight adjacent neighbors, which improves the imperceptibility value.

The competing parameters

- Undetectability (imperceptibility): this parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fails to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.

- Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique (out of the scope of this paper).
- Payload capacity: it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, which requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests.

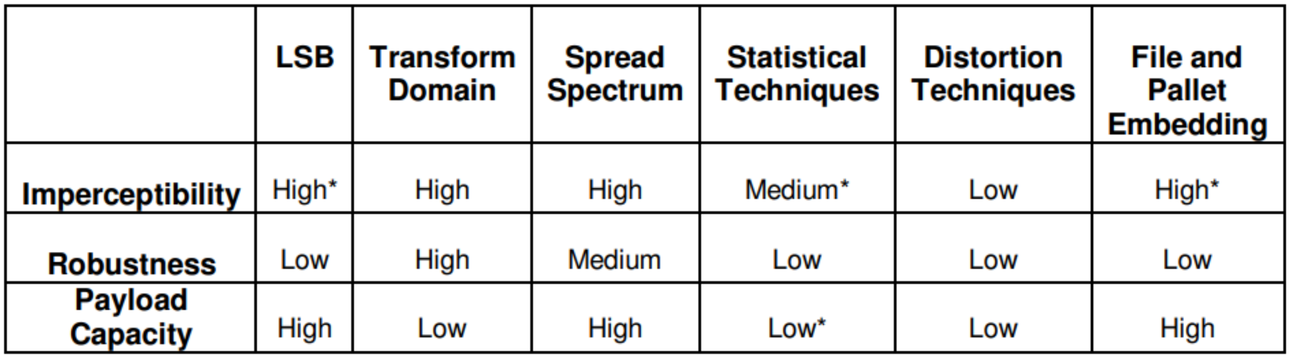
Evaluation of different techniques

Comparison of the previously mentioned steganographic techniques in terms of the competing parameters.

- LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression. Although LSB techniques can hide large quantities of information i.e., high payload capacity, they often compensate for the statistical properties of the image and thus indicate a low robustness against statistical attacks as well as image manipulation.
- The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms . The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers’ attention towards JPEG images. Working at some level like that of DCT makes steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive result and outperforms DCT embedding, especially in terms of compression survival .
- Spread spectrum techniques are generally quite robust against statistical attacks, since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be

difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction.

- Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of the embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS.
- Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data .
- Hiding information via steganographic techniques that modify the elements in the visual image results in a stego image that will survive rotation, scaling and much lossy compression like JPEG. A reasonable payload capacity can be achieved with this technique as well.



	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet Embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

A comparison of Image Steganography Techniques

Conclusion

The field of image steganography offers a diverse range of solutions for hiding data within images, each with its own set of characteristics, advantages, and limitations.

These techniques have demonstrated varying levels of data hiding capacity, robustness against image processing operations, and compatibility with different types of images.

Furthermore, as technology advances, new trends and advancements in image steganography are constantly emerging, influencing the effectiveness and relevance of existing solutions.

In future studies, it would be beneficial to explore these emerging trends further and conduct more in-depth analyses of specific steganographic algorithms to better understand their strengths and weaknesses in different scenarios.

Overall, the study of image steganography is a dynamic and evolving field that continues to offer new challenges and opportunities for researchers and practitioners alike.

References

Mehtap Ulker,Bilgehan Arslan.March 2018. "A novel secure model: Image steganography with logistic map and secret key", Conference Paper.

Nagham Hamid ,R.Badlishah Ahmad ,Abid Yahya ,Osamah Al-qershi .June 2012 ."Image Steganography Techniques: An Overview", Article.

Ajith Abraham ,Marcin Paprzycki .May 2004.”Significance of steganography on data security”,Conference Paper

Frederick S. Brundick ,Lisa M. Marvel.March 2001.”Implementation of Spread Spectrum Image Steganography “,ARMY RESEARCH LABORATORY.

Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi .March 2010.”Overview: Main Fundamentals for Steganography”,JOURNAL OF COMPUTING, VOLUME 2.

Mandavilli Kavya, RamBabu M. April 2018.”A review paper on transform domain techniques of image steganography in text and image”.