Academic City University College – Accra Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART) Africa
Tony Blair Institute for Global Change
FAIR Forward – Artificial Intelligence for All - Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Accra Bespoke Multidisciplinary Innovations Conference (ABMIC)

& The Africa AI Stakeholders' Summit 14th December, 2021

Steganography Schemes for Data & Information Protection

Sarumi, J.A. , Omotosho, O.M. & Longe, O.B
Department of Computer Science, Lagos State Polytechnic, Ikorodu, Lagos, Nigeria
Department of Computer Science, Federal School of Statistics, Ibadan, Nigeria
Faculty of Computational Sciences & Informatics, Academic City University, Accra, Ghana

Emails:
jerrytechnologies@yahoo.co.uk
Seyiblack2@yahoo.com
olumide.longe@acity.edu.gh

Phones
+2348023408122
+2348066965401
+233595479930

Proceedings Citation Format

Sarumi, J.A., Omotosho, O.M. & Longe, O.B. (2021): Steganographic Schemes for Data & Information Protection. Proceedings of the Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. December 2021. Pp 83-104. www.isteams.net/ghanabespoke2021.
DOI https://doi.org/ 10.22624/AIMS/ABMIC2021P7x

Steganographic Schemes for Data & Information Protection

Sarumi, J.A (PhD), Omotosho, O.M. (MCS) & Longe, O.B (PhD)

ABSTRACT

In this digital world of data transmission, information is at the heart of computers, transactions and international economic dealings. In ensuring the security of data and information researchers have come up with different schemes and techniques that can provide protection for data and information during transmission. The protection of sensitive information involves many interdependent policies and technological issues relating to information confidentiality, integrity, authenticity, anonymity, and utility. In this paper, we review literature on steganography protection schemes and highlight several developments that has ensured intellectual property protection over time.

Keywords: Watermarking, Steganography, Fingerprinting, Cryptography, Intellectual Properties, Protection, Concealment, Adaptive Image Steganography

1. INTRODUCTION

One of the reasons why data breaches are successful is that most of the information acquired from a computer system is in forms that are comprehensible, Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack (Identity Theft). One resolution to the current problem is, through the utilization of steganography. Steganography is a technique of hiding information in digital media. In distinction to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Steganography becomes more important as millions join the internet revolution. Steganography is the art of concealing information through mediums that prevents the detection of hidden messages. Steganography includes an array of secret communication methods that hide the message from being seen or discovered.

Brief History

According to Wikipedia, steganography has been widely used for centuries, its first ever recorded use can be traced back to 440 BC when Herodotus mentioned two examples in his Histories. *(Wikipedia)* Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, "marking" a message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, “When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon.”, another example is when Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. *(Wikipedia).*

What is Steganography?

Steganography combines the Greek words “steganos”, meaning “covered, concealed, or protected”, and “graphein” meaning "writing". In theory, it is the art or practice of concealing a file, message, image, or video within innocuous carriers, another form of digital media. i.e. another file, message, image, or video. *(Wikipedia)*

2. THEORETICAL BACKGROUND

In order to completely understand how steganography is achieved in computer science, some background knowledge of how computers work is necessary. All information in a computer system is represented as bits, each with a value of 0 or 1. A similar sequence of bits might represent a number, a sequence of text, or a machine instruction in different contexts. For example, the bit sequence "0110 1000 0110 0101 0110 1100 0110 1100 0110 1111" means "hello" if translated using the ASCII standard. It will be most likely meaningless if translated using some other standards. Other forms of digital media ie image, audio, and video files are also no exception. They are all sequences of bits stored in a disk.

An article on U.K. Essays posits that during the 15th and 16th centuries, several writers including Johannes Trithemius (author of Steganographia) and Gaspari Schotti (author or Steganographica) wrote on Steganographic techniques such as coding techniques for text, usage of invisible inks, and incorporating hidden messages in music. Between 1883 and 1907, further, development can be attributed to the publications of Auguste Kerckhoff (author of Cryptographic Militaire) and Charles Briquet (author of Les Filigranes). These books were majorly about Cryptography, but both can be attributed to the foundation of some steganographic systems. Concepts such as null cyphers, image substitution and microdots were introduced and embraced as steganographic techniques. *(U.K. Essays, 2018)*

In the digital world today, Steganography is being used all over the world, with many tools and technologies being created that take advantage of old steganographic techniques. With the level of research this topic is now getting, there is hope to see a lot of great applications of Steganography in the near future. Steganography replaces unneeded or unused bits in regular computer digital files with bits of different and invisible information. *(U.K. Essays, 2018)* Information to be hidden can be any other regular computer file or encrypted data. It is sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is still not seen. *(U.K. Essays, 2018)*

3. TYPES OF STEGANOGRAPHY

There are different ways of hiding information in a file, some well-known techniques include; the least significant bits and Injection. When a media file is created there are few bytes in the file which are not necessary or not important to store the file's information. These bytes can be replaced with a message without damaging or replacing the original file, by which the secret message is hidden in the file. Another way is that a message can be directly injected into a file. But this way, the size of the file would be increased accordingly depending on the secret message

3.1 Steganography in Image

Digital images are some of the most widely used cover objects for steganography. This is due to the availability of various file formats for various application, the algorithms that can be used differ for these different formats. When dealing with digital images for the purpose of steganography, 8-bit and 24-bit per pixel images are typically used. Both image types have their own advantages and disadvantages, 8-bit image files are a great format to use because of their relatively small size. The only disadvantage is that there are only 256 possible colours used which can be a potential problem during encoding. *(U.K. Essays, 2018).* According to the same article, it posits that grayscale colour palette is usually used when dealing with 8-bit images such as (.GIF images) because its gradual degrading change in colour would be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexible when used for image steganography. *(U.K. Essays, 2018)* The same article further explains that the large numbers of colours used in 24-bit images with over 16 million colours can be used, the number of colours go well beyond what the human visual system could easily recognize, which makes it very hard to detect changes in the image once a secret message has been encoded. A large amount of data can be encoded into 24-bit images as it is compared to 8-bit images. The disadvantage of 24-bit digital images is their size which is very high and this makes them suspicious on the internet due to their heavy size when compared to 8-bit images*. (U.K. Essays, 2018)* Depending on the type of message and type of image, different algorithms are used.

A few of the algorithms used in Image Steganography include:

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

Least Significant Bit Insertion

Least Significant Bit (LSB) insertion is the most widely known algorithm for image steganography, it involves the modification of least significant bit layer of the image. In this technique, the message is stored in the least significant bit of the pixels which could be considered as random noise. Thus, altering them does not have any obvious effect or cause any distortion on the image. (U.K. Essays, 2016)

Masking and Filtering

This technique works better with 24-bit and grey scale images. It hides information in a way similar to watermarks on actual paper and is sometimes used as digital watermarks. Masking the images changes the images. It ensures that changes cannot be detected by making changes in multiple small proportions*. (U.K. Essays, 2016).* It starts with the analysis of the image, then finds areas where their image will be more integrated and embeds them there. (Rajesh et al., 2010) Compared to the Least Significant Bit insertion, masking is more robust and the masked images can pass through cropping, compression and some other forms of image processing. It is more suitable for lossy images. *(U.K. Essays, 2016)*

Redundant Pattern Encoding

In this technique, the message is scattered all throughout the image based on some algorithm. It makes the imaging technique resistant and ineffective for cropping and rotation. Multiple smaller images with redundancy increase the chance of recovering even when the stegano-image is manipulated*. (Ganguly et al., 2008)*

Encrypt and Scatter

Encrypt and Scatter techniques hides the message as white noise, which uses spread spectrum and frequency hopping. Previous window size and the data channel are used to generate a random number. Within this random number, on all the different eight channels message is scattered throughout the message. *(Ganguly et al., 2008)* Each channel rotates, swaps and interlaces with every other channel. A single channel represents one bit and as a result, there are many unaffected bits in each channel. In this technique, it is very complex to draw out the actual message from stegano-image. This technique is more secure compared to LSB as it needs both the algorithm and a key to decode the bit message from stegano-image. Some users prefer these methods for its security as it needs both algorithm and key despite the stegano-image. This method like LSB allows image degradation in terms of image processing and compression. *(U.K. Essays, 2016)*

Algorithms and Transformations

Least Significant Bit modification technique for an image is sufficient if any kind of compression is done on the resultant stegano-image e.g. JPEG, GIF. JPEG images use a Discrete Cosine Transformation (DCT) to achieve compression. *(U.K. Essays, 2016)* DCT is a lossy compression transformation because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depending on the method used to calculate DCT. *(Ganguly et al., 2008)*

3.2 Steganography in Audio

Encoding secret messages into an audio file is one of the most challenging technique in steganography. As stated in the U.K. Essays article, this is because the Human Auditory System (HAS) has such a vibrant range that it can listen over. To put this in perspective, the human auditory system recognizes over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure*. (U.K. Essays, 2016)*. To embed messages in the audio, slight altering of the binary sequence of the audio file is done and the secret message is then embedded in that binary sequence. Audio steganography can be done in formats like MP3, WAV, and AU. *(Ganguly et al., 2008)*

Below are the lists of methods which are commonly used for audio steganography:

- Least significant bit coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

Least Significant Bit Coding

Using the least-significant bit insertion is possible for audio, as modifications usually would not create recognizable audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are indistinct to the human ear. Using frequencies above 20.000Hz, messages can be hidden inside sound files and cannot be detected by human checks. *(Ganguly et al., 2008)*

Parity Coding

This involves breaking a single signal down into separate regions of samples, instead of breaking a signal down into individual samples, it then encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the least significant bit of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more obfuscating fashion. *(Ganguly et al., 2008)*

Phase Coding

Phase coding attends to the disadvantages of the noise-inducing methods of audio Steganography. Phase coding uses the fact that the phase components of sound are not as audible to the human ear as noise is. Rather than introducing perturbations, this technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, attaining an indistinct encoding in terms of signal-to-perceived noise ratio. *(Ganguly et al., 2008)*

Spread Spectrum

In this context, the basic Spread Spectrum method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. *(Ganguly et al., 2008)* This is comparable to a system using an implementation of the least significant bit coding that randomly spreads the message bits over the entire audio file. However, unlike the least significant bit coding, the spread spectrum method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for broadcast. *(U.K. Essays, 2016)*

Echo Hiding

In echo hiding, information is hidden in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it also provides advantages in that it allows for a high data transmission rate and provides superior strength and robustness when compared to the noise-inducing methods. *(Ganguly et al., 2008)* If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal. *(U.K. Essays, 2016)*

3.3 Steganography in Video:

Steganography in videos poses a very interesting challenge because video files are generally a collection of sounds and images. Ganguly et al argued that video steganography can employ some of the techniques uses in both image and audio steganography, and since videos are a stream of motion images, any slight distortion might go unnoticed. This factor also allows it to store large files in the videos file. *(Ganguly et al., 2008)*

To achieve video steganography, a video file would be embedded with supplementary data to hide secret messages. In the process, an intermediate signal which is a function of hidden message data and data of content signal would be generated. Content data (video file) is then combined with this intermediate signal to result in encoding. The supplementary data can include copy control data which can be brained by consumer electronic device and used to disable copying. The intermediate signal may also contain a pseudo-arbitrary key data so as to hide encoding, and decoding needs a corresponding key to extract hidden information from encoded content. In some implementations, regulation data is embedded in the content signal with auxiliary data. This regulation data consists of known properties enabling its identification in the embedded content signal. *(U.K. Essays, 2016)*

This encoding is robust against scaling, resampling and other forms of content degradation so that the supplementary data can be detected from the content which might have been degraded. There are different approaches for video steganography apart from the above mentioned. Most widely known are listed and discussed below.

- Least Significant Bit Insertion
- Real Time video steganography

Least Significant Bit Insertion

This is the simplest and popular approach for all types of steganography. In this method, the digital video file is considered as separate frames and changes the displayed image of each video frame. LSB of 1 byte in the image is used to store the secret information. Effecting changes are too small to be recognized by the human eye. This method enhances the capacity of the hidden message but compromises the security requirements such as data integrity. *(U.K. Essays, 2016)*

Real-Time Video Steganography

This kind of steganography involves hiding information on the output image on the device. This method considers each frame shown at any moment irrespective of whether it is image or text. The image is then divided into blocks. If pixel colours of the blocks are similar, then it changes the colour characteristics of a number of these pixels to some extent. By labelling each frame with a sequence number it would even be easy to identify missing parts of information. To extract the information, the displayed image should be recorded first and the relevant program is then used. *(U.K. Essays, 2016)*

3.4 Steganography in Document:

Steganography in documents just focuses on altering some of its characteristics. They can either be characteristics of text or even text formatting. Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, one can see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways. *(U.K. Essays, 2016)* One way is by simply adding white space and tabs to the ends of the lines of the document. This technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source leads to the hidden message. Discovering it depends exclusively on gaining knowledge of the secret key. *(U.K. Essays, 2016)*

Another article states that setting the background colour and font colour is one of the widely used steganographic approaches. This method is focused on Microsoft word documents. Choose predefined colours and set font and background colours of invisible characters such as space, tab or the carriage return characters. R.G.B. values are 8-bits means we have allowed a range of 0 to 255. Most of the viewers would not feel interested about colour values of these invisible characters hence 3 bytes of information is easily hidden in each occurrence of space, tab or carriage return. This approach needs no extra information to hide the required bits *(U.K. Essays, 2018).*

4. WHAT ARE IMAGES STEGANOGRAPHY

Images are a pictorial representation of objects, in computing Images or Digital Images are the binary representation of visual data, they are collections of numbers that constitute different light intensities in different areas of the image. *(Nidhi, 2016).* This numeric representation forms a grid(lattices) and the individual points are referred to as pixels. The pixels in an image are displayed horizontally row by row. The number of bits in a colour scheme called the bit depth, it refers to the number of bits used for each pixel. *(Wikipedia).*

Ndihi in her 2016 paper "Image Steganography Using Enhanced Lsb Technique" also stated that smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. She noted that digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8bits. Thus, in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours. *(Nidhi, 2016).*

4.1 Image Compression:

To perform image steganography, we also need to understand the concept of how images can be compressed and how it affects their outputs after compression. In images, there are two types of compression: lossless and lossy compression. ***Lossless compression*** is a known data compression technique, where the original data should stay in its entirety. In this manner, the original image information will never be removed, and this makes it possible for the reconstruction of the original data from the compressed data. This is typical of images in GIF and BMP. *(Tiwary et al., 2016).* ***Lossy compression*** also known as irreversible 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. *(Tiwary et al., 2016).* It uses inexact approximations and partial data discarding to represent the image, but not the same as the original. JPEG compression uses this technique. *(Wikipedia).* A cover image is an image designated to carry the embedded bits or secret information. *(Tiwary et al., 2016).* A ***stego-image*** or ***stegano-image*** refers to the image carrying the hidden or embedded message. *(Tiwary et al., 2016).*

4.2 Techniques For Image Steganography

There are quite a number of techniques used to achieve adaptive image steganography, but first, we look at the evaluation criteria for steganography techniques.

Evaluation Criteria for Steganography Techniques

Invisibility/ Imperceptibility:

The invisibility of the steganography algorithm is the first requirement since the strength of steganography lies in its ability to be unnoticed by the human eye.

Payload Capacity:

Steganography aims at hiding information so; this represents the maximum amount of information that can be hidden and retrieved successfully. *(Hamid et al., 2012)*

Robustness

When the steganography algorithms are applied then sometimes, they add a signature when embedding information; this can be easily detected through various statistical methods. There may be some cases where the image is cropped or its pixel values are altered before it reaches the target destination, so the steganography algorithms should be robust against such malicious changes.

Independent of the File Format:

Only one format is used for secure communication even though there are different formats available on the internet, hence the steganography algorithms should be robust even that it should be able to embed the message in any kind of formats available on the internet.

Unsuspicious Files:

This requirement includes all characteristics of a steganography algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden. *(Morkel et al., 2005)*

Peak signal-to-noise ratio (PSNR):

High is the PSNR, High is the secure communication because high PSNR refers to the fact that the difference between the stegano-image and cover image is less *(Hamid et al., 2012)*.

4.3 Evaluation and Taxonomy Of Steganography Techniques

There are quite a lot of approaches in classifying steganographic techniques. These approaches can be classified in accordance with the type of covers used with secret communications. Another possibility is done via sorting such approaches depending on the type of cover modification already applied in the process of embedding. The second approach is adopted in this work, although in some cases an exact classification is not possible. *(Hamid et al., 2012)* Hamid et al., describe the taxonomy with the equation; Let C denote the cover carrier, and C~ the stegano-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,

$$Em: C \oplus K \oplus M \rightarrow C \qquad (1)$$

$$\therefore Ex(Em(c,k, m)) \approx m, \forall c \in C, k \in K, m \in M \qquad (2)$$

In the same report, Hamid et al stated that to further distinguish between different steganographic techniques in a wide sense, one must take into consideration both the methods that modify the image and those that modify the image file format. However, the modifications to the file format are less robust. *(Hamid et al., 2012)* Hamid et al., also stated that 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. *(Hamid et al., 2012)* As a result, researchers have come up with different steganographic algorithms that suit such compression types.

4.4 Steganographic techniques that modify image files

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, which we also describe for completeness *(Hamid et al., 2012)*. The next section explains each steganographic approach in more detail.

Spatial Domain Technique

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 scant 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. *(Hamid et al., 2012)*

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

$$Yi = 2\frac{xi}{2} + mi \qquad (3)$$

Where m_i, x_i, and Y_i 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 {Pm (m = 0) ≈ Pm (m = 1) ≈ 12}. In addition, the cover image and the message may also be assumed to be independent. *(Hamid et al., 2012)* Therefore, the noise introduced into the image may be modelled as:

$$P_{+1} = P/2\ P_{x\ x} = 0),\ P_0 = 1 - P/2,\ P_{-1} = P/2\ P_x\ (x = 1) \qquad (4)$$

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 LSB of these pixels already selected during this process. *(Hamid et al., 2012)*.

When hiding the message bits in the image using LSB algorithms, there are two schemes, namely sequential and scattered. The LSB of the image, in the sequential embedding scheme, is 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 *(Hamid et al., 2012)*.

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. They also describe a substitution technique for embedding a secret message into the LSB bits of the palette of GIF or BMP image format using steganography. Bailey and Curran provide an evaluation of various techniques concerning spatial steganographic and such techniques can principally apply to GIF images. 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 them 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 *(Hamid et al., 2012)*.

5. TRANSFORM DOMAIN TECHNIQUES

The report also stated that transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. It is worth saying that most of the strong steganographic systems today operate within the transform domain. Transform domain techniques have an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions *(Hamid et al., 2012)*. The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it.

5.1 JPEG Compression

If an image is to compress into JPEG format, the RGB colour space is first turned into a YUV representation. Through this representation, the Y component represents brightness (or luminance) and the U and V components stand for colour (or chrominance). It is known that the human eye is more sensitive to changes in the brightness of a pixel than to changes in its colour. *(Morkel et al., 2005)* Downsampling the colour information is taken as an advantage of the JPEG to reduce the size of the file Where the colour components (U and V) are split in the horizontal and vertical directions and consequently reducing the file size by a factor of 2. Then, the image is transformed. For JPEG images, the discrete cosine transforms (DCT) is used; the pixels can be converted with such mathematical processing by simply “spreading” the position of the pixel values over the image or part of it *(Kharazi et al., 2004)*. With DCT transformation, a signal is transformed from the representation of an image into the frequency domain, this is done by sorting the pixels into (8 × 8) pixel blocks and transforming these blocks into 64-DCT coefficients which are affected by any modification of a single DCT coefficient. *(Morkel et al., 2005)*.

The quantization phase of the compression is counted as the next step. Besides, it is considered as the biological property where the human eye is imposed. Basically, the human eye is known for being capable of identifying small differences in brightness over a relatively large area. The same does not apply when considering the distinction between different strengths in high-frequency brightness. *(Morkel et al., 2005)* Consequently, the strength of higher frequencies can be reduced without any change in the image appearance. The JPEG format is done by dividing all the values in a block via a quantization coefficient, so the results are made approximate to integer values. The last point is to encode the coefficients by using Huffman coding just to reduce the size. *(Morkel et al., 2005)*

5.2 JPEG Steganography

Previously, it was believed that steganography could not be used with JPEG images owing to the lossy compression, which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise. Data in most of the steganographic systems seems to be embedded into the non-zero discrete cosine transforms (DCT) coefficients of JPEG images. The major JPEG steganographic methods can be described as follows:

- JSteg/JPHide. Jsteg and JPHide are two classic JPEG steganographic tools that employ the LSB embedding technique. *(Morkel et al., 2005)* JSteg functions to hide the secret data in a cover image by simply exchanging the LSBs of non-zero quantized DCT coefficients with secret message bits. The quantized DCT coefficients, already used to conceal secret message bits in JPHide, are selected randomly by a pseudo-random number generator. JPHide, on the other hand, tends not only to modify the LSB of the selected coefficients, but it can also switch to a process where bits of the second-least-significant bit-plane are likely to be worked out. *(Hamid et al., 2012)*
- F5. The F5 steganographic algorithm was introduced by Westfield. Rather than replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is reduced by the F5 algorithm by one if it needs modification. *(Kharazi et al., 2004)*. Due to the author's argument, the use of the chi-square attack can never detect this type of embedding. In addition to embedding message bits into randomly chosen DCT coefficients, the F5 algorithm employs matrix embedding that reduces the number of changes necessary for hiding a message of a certain length. Both, the message length and the number of non-zero coefficients are required in the embedding process to determine the matrix embedding needed to decrease the number of modifications required in the cover image. *(Hamid et al., 2012)*.
- OutGuess. OutGuess is provided by Provos as a UNIX source code for which there are two widely known released versions. *(Kharazi et al., 2004)*. The first one is the OutGuess-0.13b, which is exposed to statistical analysis, and the second is OutGuess-0.2, which includes the ability to safeguard statistical properties. Hereafter, OutGuess refers to OutGuess-0.2. There are two stages representing the embedding process of OutGuess. The first of which is that OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0s and 1s. Soon after modifications are made to the coefficients already left during embedding to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be subjected to a chi-square attack. *(Hamid et al., 2012)*.
- MB. Model-based steganography (MB) can be defined as a general framework for conducting both steganography and steganalysis by simply using a statistical model of the cover media. The MB method for JPEG images is capable of having high message

capacity while remaining secure against many first-order statistical attacks. *(Hamid et al., 2012)*.

- YASS. Yet another steganographic scheme (YASS) belongs to JPEG steganography but does not conceal data in JPEG DCT coefficients directly. Instead, an input image in the spatial domain is divided into blocks with a fixed large size, called big blocks (or B-blocks). A later stage is to randomly select within each B-block, an 8 × 8 sub-blocks known as embedding host block (or H-block). Then via using error correction codes, secret data is encoded and embedded in the DCT coefficients of the H-blocks. Finally, the entire image is compressed and distributed as a JPEG image after inversing DCT on the H-blocks. *(Hamid et al., 2012)*.

5.3 Wavelet Transform Technique

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transforms clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. The discrete wavelet transforms (DWT) method is favoured over the discrete cosine transforms (DCT) method, owing to the resolution that the WT provides to the image at various levels. *(Kaur et al., 2011)*

Wavelets are mathematical functions that divide data into frequency components, which makes them ideal for image compression. In contrast with the JPEG format, they are far better at approximating data with sharp discontinuities. *(Morkel et al., 2005)*

In the report published by *Syed et al in 2000,* the writers discuss a steganography technique, based on wavelet compression techniques, that attaches attribute information to images in order to reduce the amount of information stored in a database of images. They use the homogenous connected region interested ordered transmission (HCRIOT) wavelet algorithm for image encoding and compression. This technique embeds secret information in the edge and detail regions of the image where the human eye is less sensitive to the noise generated by the technique. In general, the human eye is more sensitive to noise in the smooth regions of an image. In the project described in, researchers use vector quantization, called Linde-Buzo-Gray (LBG), associated with block codes, known as BCH codes, and one-stage discrete Haar wavelet transforms. They emphasize that modifying data by using a wavelet transformation produces good quality with few perceptual artefacts. *(Syed et al., 2000)*

A group of scientists at Iowa State University are developing an advanced application called artificial neural network technology for steganography (ANNTS), with the aim of detecting all current steganography methods, which include DCT, DWT, and DFT. They found that the inverse discrete Fourier transform (IDFT) includes a rounding error that makes DFT inappropriate for steganography applications. The research proposes, a data hiding technique in the DWT domain. DWT with the first level is used to decompose both secret and cover images, where each is broken into disjoint (4 × 4) blocks. Then a comparison is made between the blocks of the secret image and the cover blocks to determine the best match. Later, error blocks are produced and embedded into the coefficients of the best-matched blocks in the HL part of the cover image. *(Morkel et al., 2005)*

In another report by Paulson, the author proposed high capacity and high-security steganography using the discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and the payload are merged into a single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to minimize the pixel range to ensure accurate recovery of the payload at the receiving end. *(Paulsonl, 2006)*. The capacity of the proposed algorithm is increased as only the approximation band of the payload is considered. The entropy, mean square error (MSE) and capacity are improved with an acceptable peak signal to noise ratio (PSNR). *(Hamid et al., 2012)*

5.4 Spread Spectrum Technique

Spread spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image. *(Hamid et al., 2012)*

Cover image as noise

A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub-images. (*Morkel et al., 2005)* When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum steganography. When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum steganography. These techniques require searching the image for the carrier in order to then retrieve the data. These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier. In this case, after the carrier is created, and before the message is added, the carrier is compressed using JPEG compression and decompression such that it will be unaffected by later JPEG compression of the cover image. The capacity can be traded directly for robustness, and it depends greatly on the image. (*Hamid et al., 2012)*

Pseudo-noise

This technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect. Spread spectrum image steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error coding, and image processing to hide information in images, is an example of this technique. (*Paulson, 2006)* The general additive embedding scheme can be described as follows:

$$Y_i = X_i + \gamma W_i \text{ for } _i = 1,2 \qquad (5)$$

Where X_i is a sequence of the original data from the cover, W_i is a pseudo-random sequence generated from a pseudo-random number generator (PRNG) initialized by a secret stego key, γ is an embedding strength parameter (gain factor), and Yi is a sequence of possibly altered data. (*Hamid et al., 2012)* 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 stegano 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. (*Kaur et al., 2011)*

The last few years witnessed the development of several steganography techniques one of which is spread spectrum steganography. In 1996, Smith and Comiskey described three schemes, namely direct sequence, frequency hopping, and chirp. In image steganography, it is noticed that high frequencies usually aid the invisibility of the hidden information, but at the same time, they are not efficient as far as robustness is concerned. In contrast, low frequencies are better with respect to robustness but are far too visible to be useful. Such conflicting points are reconciled by the spread spectrum technique via allowing the embedding of a low-energy signal in each one of the frequency bands. (*Hamid et al., 2012)*

Instead of using direct sequences, two new processing methods are proposed. Such methods include block spread spectrum and duplicate spreading. Spread spectrum techniques are capable of being combined with transform embedding by using transformation techniques in order to get the payload capacity increased. (*Kaur et al., 2011)* Other authors like Paulson introduce a technique based on discrete Fourier transform (DFT) that can significantly increase the number of transform coefficients that can transmit hidden information. Blind image steganography, based on a hybrid direct sequence/frequency hopping (DS/FH) technique, in which the system retrieves the hidden message without needing the original image.

These authors found that using a signature vector, when embedding a spread spectrum (SS) message, maximizes the signal-to-interference-plus-noise ratio (SINR) at the output of the corresponding maximum-SINR linear filter. The research describes the benefits of combining the spread spectrum technique with the advantages of error correction coding and DFT simply to the robustness of the system increased. (*Paulson, 2006)*

Finally, an analysis is presented proposes using a code division multiple access
(CDMA) spread spectrum for both the spatial domain and the transform domain for image steganography in MMS. Their experimental results reveal that the spread spectrum detection method is highly robust for normal signal manipulation. (*Hamid et al., 2012)*

5.5 Statistical Methods

This is also known as model-based techniques; these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation. (*Paulson, 2006)* Statistical steganographic techniques exploit the existence of a “1-bit”, where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a “1” is transmitted, otherwise it is left unchanged. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message. (*Hamid et al., 2012)*

Another technique, called data masking, has been proposed by Paulson. According to this technique, the message signal is processed such that it views the properties of an arbitrary cover signal. The authors propose a method where the transformed image coefficients are broken down into two parts to allow the coded message signal to replace the perceptually insignificant component. (*Paulson, 2006)* Hence, the statistics of the quantized (non-zero) AC DCT coefficients are modified taking into consideration the parametric density function. This process requires a low precision histogram of each frequency channel in addition to matching the model with each histogram by deciding the corresponding model parameters. (*Hamid et al., 2012)*

However, statistical steganographic methods in their simplest form, for which sub-images are simply sub-rectangles of the original image, are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. To counter these attacks, the sub-images could be selected based on picture elements, for example, the faces in a crowd, and error correction coding could be utilized within the message. These defences can make the statistical steganographic method approximately as robust as the underlying watermarking scheme. (*Hamid et al., 2012)*

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. (*Kaur et al., 2011).*

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 manner that the statistical properties of the image are not affected (which is different from many LSB methods). (*Hamid et al., 2012)*

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 the 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 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. (*Katzenbeisser, 2000)*

6. 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 in either a header structure or at the end of the file. (*Hamid et al., 2012)*. 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, 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 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 (*Kruus et al., 2003)*.

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 re-saving of the image implies a complete loss of hidden data. (*Kruus et al., 2003)*

Pallet Embedding

In a palette-based image, what matters is the fact that only a subset of colours from a particular colour space is used to colourize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colours as a list of indexed pairs I, (c_i), assigning a colour vector c_i to every index I, and the actual image data, which specifies a palette index for each pixel, rather than the colour value itself. The file size gets decreased via this approach when only a limited number of colour 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. (*Hamid et al., 2012)*

In some cases, the palette itself can be used to hide secret information. Because the order of the colours in the palette usually does not matter, the ordering of colours can be used to transfer information. In essence, a hidden message can be embedded using the difference between two colours in the palette (i.e., one secret message bit for every two colours in the palette). Colour palettes are used to minimize the number of bits of images used to represent colours. (*Kruus et al., 2003)* Since steganographic message 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 colours. (*Hamid et al., 2012)*

7. IMAGE GENERATION TECHNIQUE

Many techniques have been proposed that encrypt messages so that they are unreadable or as secret as possible. Big Play Maker hides information by converting the secret text message into a larger and 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 an error correcting information. (*Kruus et al., 2003)*

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. (*Hamid et al., 2012)*

2.5.10 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 colour or hair colour of some person in a photograph. These modifications can then be used to carry hidden information. (*Kruus et al., 2003)* 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. 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. (*Hamid et al., 2012)*

7.1 Adaptive Steganography

Adaptive steganography is a special case of spatial and transforms 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 (*Hamid et al., 2012)*. 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 colour, such as smooth areas. This technique is known for exploiting images with existing or deliberately added noise and with images that show colour complexity. (*Shaddad et al., 2008)*

An adaptive technique applied to the LSB substitution method has been proposed. The idea behind this method is to make use of the correlation between neighbouring 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. (*Shaddad et al., 2008)*. 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 re-expressing 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 neighbours, which improves the imperceptibility value. (*Hamid et al., 2012)*

8. PERFORMANCE MEASURE

As a performance measure for image distortion due to embedding, the well-known peak-signal-to-noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. In addition, x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the resultant stego image, and C_{xy} is the cover image. In the report posted by Hamid et al., C_{xy} is set to 255, as an agreed default value for 8-bit images. It can be that an image has only up to 253, or fewer, grey colours. Having C_{max} is raised to the power of 2 results in a strong change to the PSNR value. (*Shaddad et al., 2008)*.

For this reason, C_{max} is considered as the actual maximum value rather than the largest possible value. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is clear). A high-quality stego-image should strive for a PSNR of 40 dB, or higher. (*Shaddad et al., 2008)*

8.1 Evaluation of Different Techniques

All the above-mentioned algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. (*Shaddad et al., 2008)* The fig below shows the relationship between the 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 the statistical properties of the image and thus indicate low robustness against statistical attacks as well as image manipulation. (*Hamid et al., 2012)*
- The promising techniques such as DCT, DWT and the adaptive steganography are not susceptible 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 turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival. (*Hamid et al., 2012).*
- 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. (*Hamid et al., 2012)*
- The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. Defences could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depend on the cover image selected. (*Hamid et al., 2012)*
- 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. (*Hamid et al., 2012)*

- 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. (*Hamid et al., 2012)*
- 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. Table 1 summarizes the evaluation of the mentioned techniques. *(Hamid et al., 2012)*

Table 1: Evaluation of Different Techniques

Performance Parameter	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

8.2 Least Significant Bit Insertion.

This technique chosen the Least Significant Bit Insertion as the steganography technique I wish to implement in this project. In the LSB method, an image is used. An image is more than strings and string of bytes. Each byte in an image represents different colours. The last few bits in a colour byte do not hold much significance as the first few bits. Therefore, only two bits differ in the last few bits that represent a colour which is indistinguishable to human eyes. In the LSB method, least significant bits of a cover image is altered such that we can embed information. The example shows how letter A is hidden in the first 8 bits of 3 pixels in a 24-bit image. Since the 8-bit letter A requires only 8 bytes to hide it, the ninth byte of the 3 pixels used to hide the next character of the hidden message. *(U.K. Essays, 2018)*

The example shows that in a 24-bit image, letter A can be hidden in the first 8 bits of 3 pixels.
Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 01000010
Result: (00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001001 00100110 11101001)

The five underlined bits are the 5 bits which were altered. With LSB insertion technique, on average half of the bits of an image are changed. 'A' is an 8-bit letter and requires 8 bits for hiding. The ninth byte of 3 pixels is used for hiding the next character of the secret message. *(Kaur et al., 2011).* The slight variations of this technique allow the messages to embed into two or more least significant bits per bytes and increases the information hidden capacity of the cover object, but the cover object is degraded and easily detectable. LSB insertion is easy to implement and is also easily attacked if the modifications are done wrong. Improper modifications in colour palette and simple image calculations will destroy the hidden message. Image resizing and image cropping are same examples of image manipulations. *(U.K. Essays, 2018).*

9. CONCLUSING REMARKS & FUTURE WORKS

In this discourse, we reviewed several steganography techniques highlighting their strengths and applications. Our future work will look at how to utilize some of this techniques for the development of an android-based steganography system for concealing data Using Adaptive Image Steganography

REFERENCES

1. Arbind Tiwary, A. G. (2015). Different Image Steganography Techniques. International Journal for Computer Engineering and Applications, 13.
2. Essays, U. (2018). Steganography Using Lsb Insertion Technique Computer Science Essay. London: UK Essays.
3. Hamid, N. &.-q. (2012). Image Steganography Techniques: An Overview. International Journal of Computer Science and Security.
4. Jagvinder Kaur, s. K. (2011). Study Of Various Image Steganography Techniques. Amritsar: Amritsar College of Engineering and Technology, Amritsar, India.
5. Kashyap, N. (2016). Image Steganography Using Enhanced LSB Technique. International Journal of Scientific & Engineering Research, 6.
6. Katzenbeisser, S. (2000). Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking. London: Artech House.
7. Kavita Kavitha, A. K. (2012). Steganography Using Least Significant Bit Algorithm. International Journal of Engineering Research and Applications , 338-341.
8. Laskar, S. A. (2012). High capacity data hiding using LSB steganography and encryption. International Journal of Database Management System. 57.
9. M. Kharazi, H. S. (2004). Image steganography: Concepts and practice.
10. Nagham Hamid, A. Y.-Q. (2012). Image Steganography Techniques. Perlis: University of Malaysia Perlis School of Communication and Computer Engineering, .
11. P. Kruus, C. S. (2003). A survey of steganography techniques for image files. Advanced Security Research Journal, 41-52.
12. S. Areepongsa, N. K. (2000). Steganography for low bitrate Wavelet based image coder. IEEE, 597-600.
13. Sahoo, R. K. (2012). Some New Methodologies for Image Hiding using Steganographic Techniques. International Journal of Computer Engineering and Applications, 7.
14. Samir K Bandyopadhyay, D. B. (2008). A Review on Steganography. Kolkata: Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata.

15. T. Morkel, J. E. (2005). A Review of Image Steganography. Pretoria: Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria.
16. U.K. Essays. (2018). Encoding Secret Messages In Text Information Technology Essay. London: U.K. Essays.
17. Steganography, https://en.wikipedia.org/wiki/Steganography accessed on 10 June,2018
18. Shaddad, J. C. (2008). Biometric inspired digital image steganography. 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (pp. 159-168). IEEE.