QR CODE STEGANOGRAPHY RESEARCH MANUAL

Steganography of encrypted messages inside valid QR codes

By Kieran Carroll

C00241073

2021/2022

Y4 Cybercrime & IT Security

Institute of Technology Carlow

Project Supervisor: James Egan

Abstract

As technology rapidly advances the security and confidentiality of information transmitted across the internet remains a fundamental issue. With the development of quantum computers furthering each year this puts the current standards for encryption such as AES at risk. If such cryptographic algorithms are rendered obsolete this would make communication across the internet insecure. This is where steganography can be used to protect the confidentiality of information by hiding the existence of communication. In this paper an analysis of QR codes is presented and overview of steganography is provided, which contains the various types of steganography including image, audio, and video. Several techniques using the various cover mediums are also examined, such as the least significant bit method. The factors that influence the construction of a steganographic system are reviewed and potential attack techniques used in steganalysis to break such systems is outlined. We also briefly discuss the use of chaotic maps in image scrambling. Finally, we review some related work where QR codes and images have been used to perform steganography.

Table of Contents

Introduction

Steganography can be defined as the procedure of hiding a secret message inside a carrier that itself is not secret. Many confuse it with cryptography which involves encrypting a message which renders it uniterable thus providing privacy, while steganography is the art of secrecy and deceit as it hides the message inside of something that appears to be innocent, thus masking the fact that a secret message is present at all (Stanger, 2020). This is especially important in countries where encrypted communication is banned which would make using steganography an ideal method of communication. Typically, cryptography is used in conjunction with steganography when trying to create a robust steganographic system. The word Steganography originates form the Greek word "steganos" which means "secret" or "covered" and graphy which means "drawing" or "writing", these words combined define it as "secret writing". Steganography isn't a modern invention and has been used for centuries, with the initial steganography method being developed in Greece at around 440 B.C. Histaeus a Greek ruler used Steganography to secretly communicate with his recipients, his method involved shaving the head of a slave, tattooing the message onto the slave's bald head, and then waiting for their hair to grow back to hide the secret message. The slave was then sent to the recipient where their hair would be shaved to uncover the secret message. Other methods of Steganography followed suit over the centuries which involved the carving of messages on the wood of a wax tablet and then coating it wax which was used by the Spartans and invisible ink which was used during time of war such as the American revolution. Therefore, we can say that Steganography has developed throughout the centuries as a means of secret communication through deception as the secret message is embedded in an innocent looking object thus not arising suspicions. In today's digital age steganography has developed immensely to use the various file types that are widely shared across the internet to embed data. QR codes have emerged as a popular method of storing data and can be manipulated using steganography to embed secret data.

Analysis of QR Codes

The History of QR Codes & Its Use Cases

Quick Response (QR) codes were created by Denso Wave a Toyota subsidiary in 1994 and initially were used to track inventory during the manufacturing of vehicle parts. They can be described as a two-dimensional matrix barcode that has the capacity to store data (Tiwari, 2016). Nowadays, QR codes have become increasingly popular as their accuracy, reading speed and convenience has proved to be superior to the likes of linear one-dimensional barcodes (Narayanan, 2012). QR codes can hold significantly more data and can be easily scanned with a smartphone. This has prompted business to incorporate them in their marketing strategies, where they can be used to promote the business and supply the customer with additional information on a product or service. The applications of QR codes are numerous and are utilized across multiple industries as they can easily encode a URL, phone number, email address, text, and even give access to a Wi-Fi network.

How QR codes Work

The QR code system is made up of an encoding and decoding procedure. The encoding procedure involves converting text using one of four modes available alphanumeric, numeric, bytes, or kanji into a string of bits (which are 1s and 0s). When the text is encoded using one of the four modes a string of bits is constructed which is broken up into data codewords which are 8 bits in length. Error correction codewords are then generated which are ordered correctly alongside the data codewords and then placed in a specific way in the 2D QR code matrix. Then data masking is utilized to alternate the color of each module from black to white or vice versa to enable scanners to read the QR code easily (modules are the black and white square patterns that make up the QR code). There are 8 mask patterns that are available to be chosen, the most suitable one to be used should be calculated by checking the penalty score each one would have if used and the one with the lowest penalty score should be selected (Garg, 2015). The version and format information pixels are then appended to the QR code in the areas that are not taken up by the data modules.

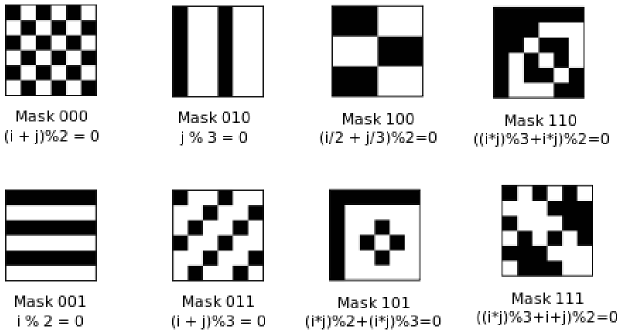


Figure 1 - Masking patterns. (Assaad, 2019)

When the QR code is scanned their arrangement translates back into the original form of data, this is the decoding process (Scott, 2020). This occurs by the scanner analyzing the white and black modules as a 2D array that is made up of bits of 1s and 0s. The version and format information are determined and then the masking pattern is released. The error correction and data codewords are restored and any errors are corrected using the error correction codewords. Finally, the data is decoded using the mode that was used in the beginning to encode the data.

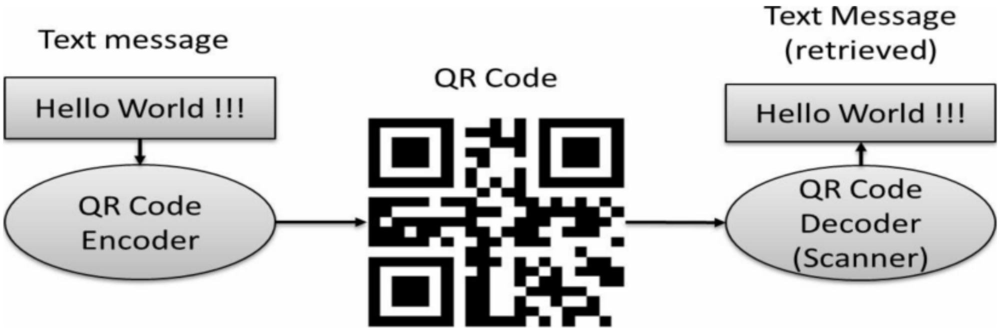


Figure 2 - QR Code Encoding and Decoding. (Tiwari, 2016)

The Structure of QR Codes

The structure of a QR code includes:

1. A timing pattern – Allows the decoder to determine the width of a singular data module.
2. A quiet zone – This is the empty space that surrounds the QR code which allows it to be identified from its surroundings.
3. An alignment pattern – This patter allows the QR code to be decoded from all angles, this is achieved by correcting the distortion of the QR code. Version 1 QR codes do not have an alignment pattern.
4. A position pattern – There are 3 position patterns located on QR codes that help decoders indicate the correct direction of the QR code.
5. Data and error correction - Stores the information of the QR code and the error correction codewords.
6. A version pattern – This pattern identifies the version of the QR code.
7. Format – This pattern holds information about error correction and data mask.
8. Separators – This is an area of whitespace that separates the position pattern from the encoding region. The encoding region being the area that contains the format information, version, and data.

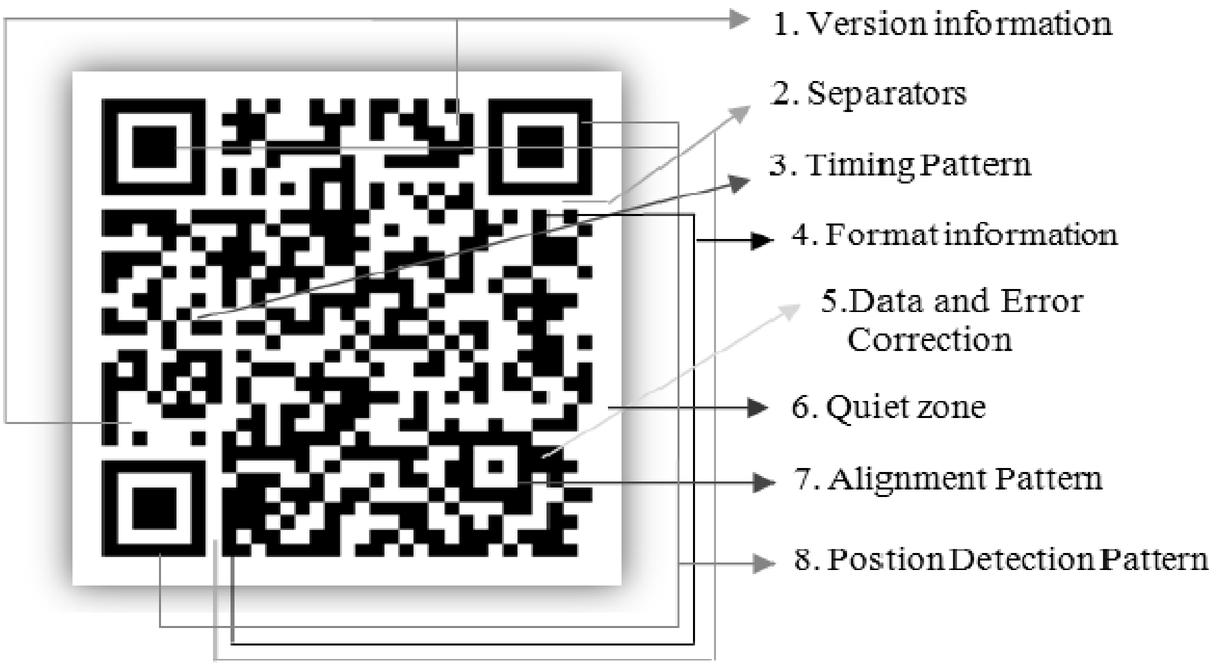


Figure 3 - The Structure of a QR code. (Waleed, 2015)

QR Code Sizes

The size of a QR code varies as there are different versions available that can be created. These versions range from 1 to 40. Each of these versions have a contrasting number of modules. Versions 1 consist of 21 rows of pixels by 21 columns of pixels while the largest possible QR code is version 40 which consists of 177 rows of pixels by 177 columns of pixels. With the largest possible QR code consisting of 177x177 modules, this means that it can have up to 31,329 squares which can encode 3kb of data. This gives each mode a max number of possible characters that can be encoded as displayed in the table below.

Mode	Maximum Characters	Values
Numeric	7,089	0-9
Alphanumeric	4,269	0-9, Uppercase letters A-Z, symbols $, %, *, +, -, ., /, : , and a space
Bytes	2,953	ISO-8859-1
Kanji/Kana	1,817	Shift JIS (2 bytes used for encoding each character)

Table 1 - Max characters for each mode. (Kanji uses two bytes to encode mainly Japanese characters but can also encode some Chinese, Russian and English).

The higher the version of QR code the more data it can store. Therefore, if a significant amount of data is needed to be encoded the larger the QR code will have to be. There is an obvious preference to keeping QR code small as having a larger QR code could slow down the scanning process, one can keep their generated QR code small by lowering the amount of data encoded and lowering the amount the error correction used (Scott, 2020).

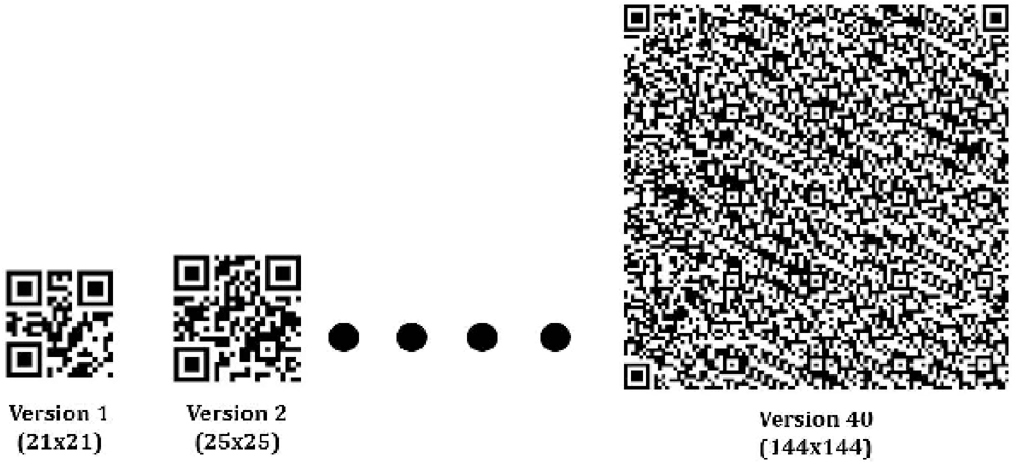


Figure 4 - QR code versions. (Tiwari, 2016)

Error Correction

QR codes contain an error correction feature that enables them to be read even if the QR code is damaged or dirty. The bits of data we encode are used to create error correction codewords. This is achieved by using Reed-Solomon codes, which are algebraic codes which perform forward error correction. Blocks of digital data are taken by a Reed-Solomon encoder added together with extra bits. Every block is processed by the Reed-Solomon decoder and an attempt is made to retrieve the original data and make any corrections to errors found. The category and number of errors it attempts to correct is based on the properties of the Reed-Solomon code used (Anon., 2012). There are 4 different levels of error correction levels that QR codes can use.

Number	Level of Error Correction	Amount of error correction needed
1	L	7%
2	M	15%
3	Q	25%
4	H	30%

Table 2 - Error Correction levels

Each level adds a separate amount of backup data depending on how much damage the QR code is expected to endure. The higher the percentage of error correction used the larger the QR code becomes as more rows and columns are added to support the addition the backup data (admin, 2011). Generally, 15% of error correction is used, while 30% would be used in areas or industries where the QR code is expected to be damaged or become dirty and 7% would be used when an insignificant amount of damage is expected to be undertook.

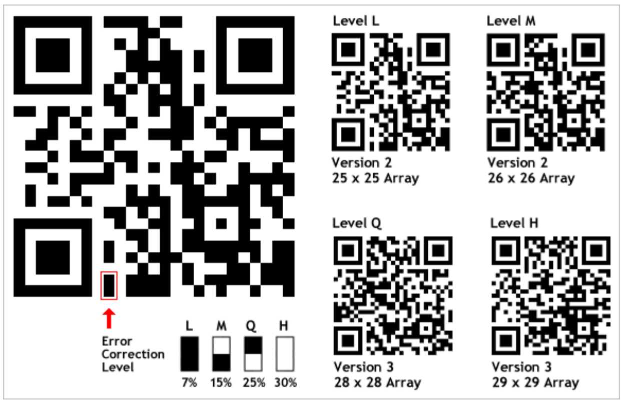


Figure 5 - Error correction levels. (admin, 2011)

Types of QR Codes

There are 5 types of QR codes that can be constructed (Mathuria, 2017).

1. QR Code Model 1 & Model 2 – The original QR code is model 1, with its largest version being 73 x 73 modules. While model 2 is the updated version of model 1 which is what is used today with its largest version possessing 177 x 177 modules.
2. Micro QR Code – This QR code only has a single position pattern which makes it significantly smaller than other QR codes with its max version being only 17x17 modules, which makes it suitable to be printed on small spaces.
3. SQRC – A secure quick response code appears as a normal QR code but possesses the functionality to store confidential information securely from whatever device is used to scan the QR code.
4. iQR Code – Is significantly larger than any other type of QR code which can hold a lot more data than any other type of QR code. It can use square or rectangular data modules.
5. Frame QR – This type of QR code has a canvas area at its center which can be used for marketing and promotion purposes as designs and data can be placed in this area (Anon., 2019).

An Overview of Steganography

Types of Steganography

When performing steganography, a message and a carrier is used. The message is the data that will be hidden, the carrier is what the message will be hidden inside of, and the resulting image is usually called a "stego object". Nowadays digital steganography has developed to provide numerous stenographic containers that can be utilized to embed the message into. This includes text, image, audio, video, and protocol (Nosrati, et al., 2011).

1. Text steganography

Text steganography is considered the hardest form of steganography to perform as it has the least amount of inessential information which is present in image, audio, or video file. With text steganography one can potentially change the words in an existing piece of text, change the formatting, construct random character sequences, or make use of context-free grammars to create legible texts. However, unlike other forms of steganography minuscule changes can easily spotted therefore it is best to make alterations to the structure of the text rather than changing the output. There are 3 categories of text steganography:

1.1. **Format Based Methods**: This method involves modifying the existing text to embed the steganographic text. This can be performed by inserting intentional misspellings allocated throughout the text, inserting spaces, and changing the size of fonts. This form of text steganography can be quite easily detected as the reader could visibly spot the differences easily if they obtained the original text and even without it, suspicions would be raised (L & B, 2008).

1.2. **Random and Statistical Generation**: This method employs the use of character and word sequences by creating cover texts. The information is embedded in these character sequences to make it seem as if it has been arranged in an arbitrary sequence of characters. It can also take the approach of analyzing the texts letter frequency and word length to form words that look to have the same statistical properties as words (Monika, 2013).

1.3. **Linguistic Steganography**: In this method the secret message is embedded by changing the cover document and not altering its initial definition. It can be divided into two subcategories, syntactic and semantic approaches. The semantic approach involves swapping one word with another while syntactic alters the layout of the cover document while avoiding replacing its meaning (R, et al., 2017).

2. Image Steganography

This form of steganography is the most popular as images are the perfect medium for hiding information because out of all the other forms of steganography, they have the most significant amount of redundancy. This high level of redundancy can be harnessed to easily alter the image to hide information in such a way that it is not easily detected that any changes have been made (Bhayani, 2020). To understand image steganography, we must understand how images work. A computer analyzes an image as a collection of bits (1s and 0s). These bits form pixels which are represented as points on a grid. The pixels are laid out horizontally row by row on a rectangular map and contain a color and their location. The bit depth is the number of bits used for each pixel; this is the color scheme. The lowest bit depth is 8 for each pixel which greyscale and monochrome images use, this amounts to 256 different shades of grey. While colored images generally are stored in 24-bit pixel depth which uses the RGB color model. The RGB model stands for red, green, and blue which all the color variants are obtained from for the pixels in a 24-bit image. Therefore, in one pixel there is a possibility of more than 16 million combinations of red, green, and blue.

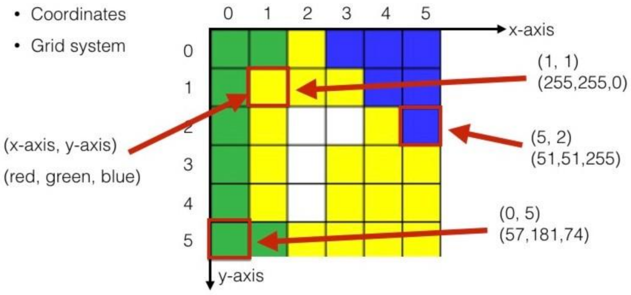


Figure 6 - The Pixel Grid. (Anon., n.d.)

Image compression is another aspect of images that should be understood before trying to perform image steganography, as it comes into play when trying to select which steganographic algorithm to use. Image compression is required when working with high resolution images that prove difficult to transfer across the internet. There are two forms of image compression lossless and lossy (Sha, 2017). Lossless image compression involves reducing the size of an image without having any impact on the original quality. On the other hand, lossy image compression reduces the image size and removes some data from the original image file (Orlandi, 2017). Since the image size is reduced when using lossy compression this rises the chance of some of the inserted payload becoming lost as some image data is removed. Steganographic algorithms using both methods of compression have been developed and can be split into two sections.

2.1. **Spatial Domain**: Using the spatial domain techniques, the pixels in the image are directly manipulated, they are changed to achieve the desired output (Sharma & Kumar, 2013). These techniques are usually dependent on the lossless image format as they implement the insertion of bits and the manipulation of noise, therefore it would not be suitable for the inserted bits to be partially lost if lossy compression was used.

- **Least Significant Bit (LSB**): This form of image steganography is a favored and conventional method used as it provides the capability to hide large amounts of information without significantly altering the original image. As the name suggest this method works by changing the least significant bit of random or selected pixels in a given image. Let’s say we are using a 24- bit image one bit of each color red, green and blue can be altered, therefore 3 bits can be stored in each pixel. If we had an image that was 800x600 pixels, then we could store 1,440,000 bits of altered data (Waykule, 2015). For example, we have a grid of three pixels that are part of a 24-bit image. Highlighted in green is the least significant bits in each byte.

Red	**Green**	**Blue**
00101101	00011100	11011100
10100110	11000100	00001100
11010010	10101101	01100011

Table 3 - A Pixel before the bits are embedded.

When we embed the number 200 (the binary representation is 1100100) into the least significant bits of this specific portion of the image then we get the result:

Red	**Green**	**Blue**
00101101	00011101	11011100
10100110	11000101	00001100
11010010	10101100	01100011

Table 4 - A Pixel after the bits are embedded.

Only the 3 bits highlighted in yellow were required to be changed as per the message we embedded. It has been noted that on average only fifty percent of the bits in an image need to be altered to embed a secret message when utilizing the maximum cover size (Waykule, 2015). With 256 possibilities of each of the RGB colors then the modification of the least significant bits in a pixel are not easily observed by the naked eye, thus successfully hiding the payload. When the secret message needs to be extracted from the image then, then the LSB bits are taken out and rearranged to form the secret message. Below is the current algorithm used to perform LSB steganography.

1. A carrier image is selected.
2. A pixel selection filter is used to find the most suitable areas in the image to embed the secret message.
3. The secret message is then inserted into the LSB of every pixel using the filter.
4. The Bit replacement method is then used.

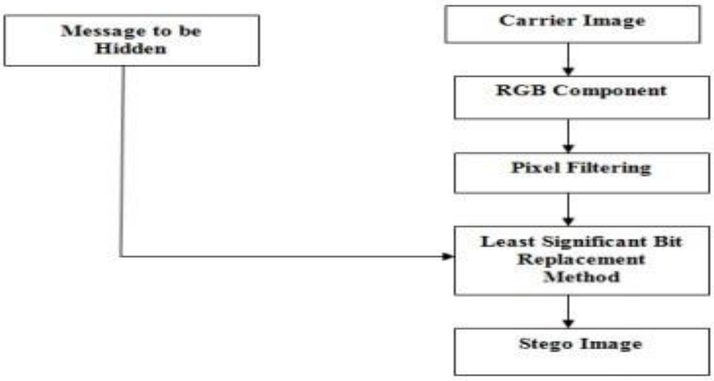


Figure 7 - Least Significant Bit Algorithm (Gupta, et al., 2012)

The use of a pixel filter selector mitigates the issue of an individual easily plucking out the secret message by taking out the LSB bits from pixel 0 up until the nth number thus piecing the embedded message together. If more data was needed to be embedded into the image, then this would be dependent on the image as the bit storage could be extended from just 1 to x number of least significant bits. However, this could lead to image distortion, but a well-chosen image would mitigate this issue. There are several image files formats that use lossless image compression that can be used to perform steganography, some examples are BMP, GIF, PNG. Each of these image file formats provide both their own advantages and disadvantages when used as a container. BMP images prove simple to use for LSB as they have the capability of storing a significant amount of data. However, BMP images are no longer widely used on the internet, thus this would arise suspicions and would go against the whole objective of steganography which is deception and secrecy. While graphics interchange format (GIF) images possess only an 8-bit depth, they can have a maximum of 256 colors. As a result, the amount of data that can be embedded is less when compared to BMP images. GIF images are palette based which means that a color lookup table is used to record the color that each pixel uses. This brings about an issue when trying to perform image steganography as if we were to change the LSB of a pixel it would end up possibly changing the color of the pixel because the index in the lookup table would be altered and thus point to a different color, making the changes apparent. We can work around this by sorting the palette or adding new colors to it. Sorting the palette involves ordering the palette by colors, this will help as the LSB steganography modifies the value in the table by +- 1 which means it would always point to a value beside it in the table, therefore when sorted by color it will always point to a color that is like the original. Portable network graphics (PNG) images were devised to upgrade upon GIF images and replace them. Nowadays PNG images are a popular image format that are widely shared across the internet thus this makes them a suitable container for steganography. Like BMP images PNGs can embed a significant amount of data, they are most suitable when the focus is on the transferal of large amounts of data rather than entirely ensuring the transmission of data is kept as discrete as possible (Anon., n.d.).

2.2. **Transform Domain:** The transform domain techniques (also known as the frequency domain) involve transforming the image first then inserting the secret message (Kumar & Yadav, 2014), in contrast to the spatial domain where the image is dealt with as it is. These transform domain techniques have shown to be more robust when compared to the spatial domain techniques as they hide data in the parts of the cover image that have a less chance of being subject to cropping, compression, and processing. However, they are also more complicated and require more of a mathematical understanding. The Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and the Discrete Fourier Transform (DFT) are some of the traditional transforms used. The use of DFT techniques establishes round-off errors which renders them inappropriate for steganography. While DCT techniques offer a small capacity for embedding a message and possess artifact issues. This leaves us with DWT techniques which have the capability of embedding a large message and are much greater at withstanding noise and signal processing attacks (Kumar & Kumar, 2017). Although the rest are still used the DWT transform proves to the most suitable for image steganography. Joint photographic experts' group (JPEG) is a popular image format that is widely used today which uses the DCT transform and lossy compression. Due to their use of lossy compression, it was originally thought that LSB steganography could not be performed using this image format. However, it has since been proved through the JPEG encoding process that LSB steganography using a JPEG is possible. The JPEG encoding procedure consists of two sections, the first stage uses lossy compression and the second lossless, thus we can perform LSB steganography in between these two sections. In the first section an image is compressed to the

JPEG format and the original RGB pixels are transformed into the YCbCr model (Jokay & Moravcik, 2010). Y represents the brightness and CbCr represents the color channels. The image is then split up into 8x8 blocks of pixels and then transformed using the DCT transform. These pixel blocks are made into 64 DCT coefficients and then the quantization of these coefficients takes place. In the second section Huffman coding is used which lowers a significant amount of memory without affecting the image detail (Dias, 2017).

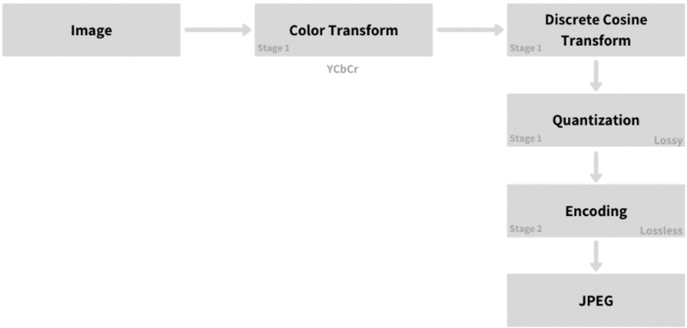


Figure 8 - The JPEG Encoding Process. (Bhayani, 2020)

2.3. **Other techniques**: While LSB remains the most popular form of image steganography other techniques are also used.

- **Spread Spectrum** – This technique involves the embedding of data all throughout the cover image thus rendering it more difficult to detect. Its process includes spreading the bandwidth of a narrowband signal over a broad range of frequencies. This technique is particularly mathematical as it requires one to modify the narrowband signal with a wideband signal, an example being white noise. Once this is completed the energy of the narrowband signal in the selected frequency band is little thus making it difficult to spot. The secret message is then inserted in noise and then merged with cover image to create the stego image.
- **Patchwork** – This technique can be described as a statistical technique that makes use of redundant pattern encoding for the purpose of embedding of a message in an image. Redundancy is applied to the secret message and is spread out across the image. A pseudorandom generator is then utilized to pick two regions of the image called patch A and patch B. The pixels in patch A are lightened while those in patch B are darkened. Only one bit is encoded in the patch subset which makes any alteration to the contrast small. Only one bit is embedded but more can be embedded by separating the image into sub-images and then embedding the bits into them. The technique has its advantages as it can survive the

transformation between lossy and lossless compression, (Mishra, 2013) but its disadvantage is that the message size must be small.

Below is a table comparing the various image steganography techniques that have been discussed (Anon., n.d.).

	LSB in BMP	LSB in GIF	JPEG compression	Spread Spectrum	Patchwork
Invisibility	High**	Medium**	High	High	High
Payload capacity	High	Medium	Medium	Medium	Low
Independent of file format	Low	Low	Low	High	High
Robustness against image manipulation	Low	Low	Medium	Medium	High
Robustness against statistical attacks	Low	Low	Medium	High	High
Unsuspicious files	Low	Low	High	High	High

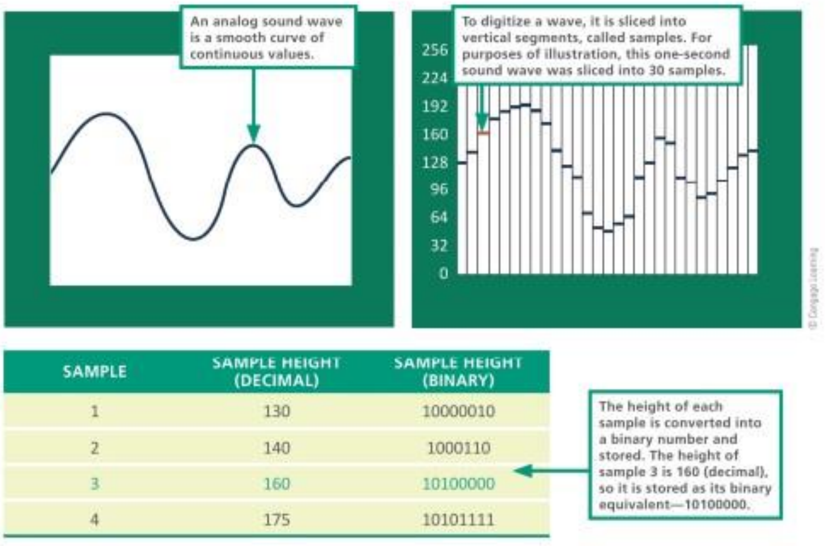
** - This relies on the image used.

Table 5 - A comparison of image steganography techniques.

Overall, there are numerous image steganography techniques involving different methods for different image formats. It's imperative that one must analyze each method and choose one that best suits intended approach as each method brings both their own advantages and disadvantage. For example, one method could be weak in its robustness while being strong its payload size and another method could have the complete opposite strength and weakness thus picking a method that aligns with your objective is key.

3. Audio Steganography

This form of steganography uses an audio file as the container. The message is hidden in frequencies and noise in which humans cannot hear. It proves to be a difficult form of steganography as the human auditory system (HAS) is sensitive and has a wide range. There are numerous approaches that can be used to implement data hiding using an audio file as the cover. To be able to perform audio steganography one must understand how a computer recognizes audio. Digital audio can be described as speech, music and other sounds which are presented in binary form to be utilized by digital devices. An analog signal is a constant signal that represents real world measurements, for example the human voice (Anon., n.d.). This analog signal is digitally represented by samples which are recorded sound waves that are stored as binary data in an audio file. An analog-to-digital converter is used to sample sound waves numerous times per second and a digital-to-analog converter translates the numeric data into analog sound waves (Anon., n.d.). The bit depth of audio file refers to the amount of amplitude units that can be recorded per sample. 16-bit, 24-bit, and 32-bit are popular audio bit depths. As the bit depth increases then the higher the resolution as more values can be recorded. Amplitude is the level of energy the sound wave carries. The audio sample rate is the rate at which the measurements are recorded in kilohertz (Brown, 2021). There are numerous techniques that audio steganography utilizes as it attempts to exploit the failings of the HAS.



An analog sound wave is a smooth curve of continuous values.

To digitize a wave, it is sliced into vertical segments, called samples. For purposes of illustration, this one-second sound wave was sliced into 30 samples.

SAMPLE	SAMPLE HEIGHT (DECIMAL)	SAMPLE HEIGHT (BINARY)
1	130	10000010
2	140	1000110
3	160	10100000
4	175	10101111

The height of each sample is converted into a binary number and stored. The height of sample 3 is 160 (decimal), so it is stored as its binary equivalent—10100000.

Figure 9 - How Digital Audio is Created. (Anon., n.d.)

3.1. Least Significant Bit – This form of audio steganography is performed like LSB image steganography whereby the least significant bit is altered to a bit of the message that is to be embedded. Altering the LSBs of a sample will produce some level of noise however if it doesn't reach a certain threshold then this method can be utilized for audio steganography as it provides a high capacity. The more bits that are changed the higher the capacity which lowers the secrecy, while the less bits altered the lower the capacity and the higher the level of secrecy (Brown, 2021).

3.2. Echo Hiding – Using this approach the secret message is inserted into the audio file by placing an echo into the signal. This technique allows us to avoid the sensitivity that the HAS possesses as an echo is merely reverberation appended to the host audio. The message is hidden in the audio by altering 3 distinct echo variables: the offset, decay rate and the initial amplitude. This ensures that the echo won’t be noticed. These variables are assigned to values that cannot be heard by the HAS and a delay of up until 1ms the echo unnoticeable. However, this form of audio steganography does not have substantial security and thus not many audio steganographic systems have been developed using this technique (Djebbar, et al., 2011).

3.3. **Phase Coding** – This technique uses the phase characteristics of sound which isn’t as audible to the HAS as noise is. The method is executed by exchanging the phase of the audio with a reference phase that incorporates the data. The phase of an audio is the sound waves.

3.4. **Parity Coding –** This method utilizes parity bits to insert each bit of the message into after the signal in broken up into different samples. Parity bits are used to inspect for errors when a piece of data in transmitted or stored, as some bits of data can alert from either 1 or 0 or vice versa, thus parity bits are used as an error checking mechanism to flip those altered bits back what they were originally by counting the number of 1s to see if it’s even which would make the parity bit a 0 and if it was odd the parity bit would be 1 (Hope, 2017). The parity bit is used in this method to ensure it matches with the bit of secret data that is to be embedded, without a match then the least significant bit of one of the areas in a section is inverted. This grants us a choice when embedding the secret bit (Singh, 2016).

4. Video Steganography

This form of steganography uses a video file as the cover, which has proved to be a more secure method due to its capability to embed a large amount of data and overall is difficulty to detect. Video files contain audio, images, and other pieces of information. A video signal possesses several attributes including frames which are the collection of still image that make up the whole video, each frame has its own pixel dimension. Frame rate refers to the pace at which the frames are displayed or captured. The bit rate is an important attribute of a video file as it represents the magnitude of the data stream, it essentially represents the lowest capability the internet connection or hard drive must have to keep the video going without buffering. While Codecs are software found in the operating system or a specific program that create the video and audio data. There are various video container types available for example MOV, MP4, and AVI, each one having a difference in their attributes, type of codec used and compression type (either lossy or lossless) (Harrington & Krogh, 2015). Video steganography techniques can be separated in 3 different group, which is determined by the embedding method (Yunxia , et al., 2019). Video steganography is essentially the combination of audio steganography and image steganography, as video is a combination of imagery and audio. Therefore, the same techniques are used, although new novel techniques exclusive to video steganography can be found in the literature.

Steganalysis

Steganalysis is used to detect and defeat steganography by extracting, detecting, or demolishing the secret data (Paladion, 2005). Steganalysis aims to beat steganography's central goal of secrecy and deceit and has found its place in computer forensics, cyber warfare, monitoring criminal activities online and assembling evidence for use in an investigation (Chanu, et al., 2012). Even if the embedded data is not extracted, merely detecting that steganography has been used is enough to defeat its whole purpose. We can classify the type of attack based on how much information the attacker has:

1. Known stego attack – The steganographic algorithm that was used is recognized and the cover object is known.

2. Stego only attack – The stego object alone is available to be assessed.

3. Known cover attack – The cover and resulting stego object are known.

4. Chosen stego attack – The stego object and the algorithm used are recognized.

5. Chosen message attack – Example stego objects are constructed from various stenographic tool available for a selected message. The resulting stego object is examined alongside an actual suspected stego object and attempt is made to determine the algorithm used.

6. Known message attack – If the message is known and can be examined in a stego object then it can be used to break other similar steganographic systems (Kumar & Reddy, 2007).

There are different methods that can be used to perform steganalysis which can split up in to four central categories: visual, learning, structural and statistical. Visual steganalysis utilizes the human visual system which possesses the ability to observe and process the data within natural images to make comparisons between the cover and stego object to discover any discrepancies (Kumar & Reddy, 2007). Structural steganalysis observes any suspicious signs of changes in the media format, as steganography usually alters the format during the embedding process (Jung, 2019). Using this method duplicate patterns and other signatures can be observed to reveal that steganography has been used. Statistical steganalysis assesses the statistics of a cover object which can be used to find the embedded data. This method can be further subdivided into the specific statistical steganalysis and universal statistical steganalysis. Specific statistical steganalysis examines the embedding process, which is used to discover distinct statistics, and requires knowledge of the embedding process. While learning steganalysis (blind steganalysis) is a universal statistical steganalysis approach that attempts to discover steganography without having any knowledge of the steganographic algorithm, cover file and the inserted message (Anon., n.d.). Overall, steganalysis is used to break steganographic systems and is an area of research that is constantly evolving as there is no one method of steganography. Therefore, it's important that ways to detect these various methods of steganography are developed for use in cases where steganography is used maliciously by terrorist organizations and criminals.

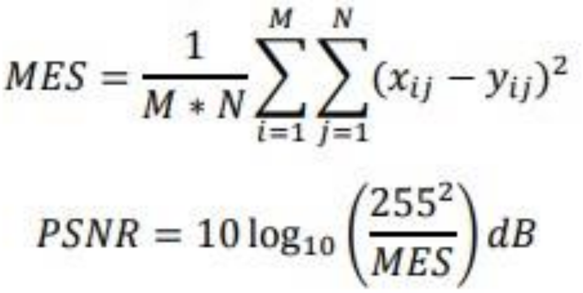
Factors that influence the success of a QR code steganographic system

There are numerous factors that should be considered when implementing steganography. This includes imperceptibility, robustness and embedding capacity. Imperceptibility refers to how well method of steganography hides the data in the cover media while avoiding deteriorating the data as it is put through the procedures used for embedding. The embedded data should not be visually observed or heard thus reducing suspicion that a secret message has been inserted. When constructing a steganographic system it essential that noise is limited as it influences imperceptibility. Noise can be defined as undesirable arbitrary changes that can occur when performing steganography (Imani & Rezaei, 2018). In the case of using QR codes there are two classifications of noise:

1. The noise of the QR code itself, it could be at the incorrect reading position or bending.

2. The noise of the message.

The alignment, position, and timing patterns on QR codes are used to correct the noise of the QR code. While Reed-Solomon codes are used to make corrections to the noise in the message. Robustness is used to measure the systems strength against steganalysis attacks and against alterations that could occur during the embedding and extraction procedures, thus it is important to test a steganographic system against intentional or unintentional attacks. The algorithm used is considered robust when if the secret message can be successfully extracted without it being destroyed (Buchanan, 2004). The embedding capacity refers to the amount of possible data that can be embedded in the cover media. As the embedding capacity increases the chance of introducing noise and distortion also increases. There are several metrics used to measure the efficiency of a steganographic system, one of the most important is peak signal to noise ratio (PSNR) and mean square error (MSE) which are used determine quality of a stego image. If the PSNR is greater that indicates that the quality is better, while lower means it is a poor-quality image. PSNR is recorded in decibels (dB). M and N are the vertical and horizontal pixel dimensions of the given stego image, while xij and yij are the pixel values in the stego and cover image (Anon., n.d.).



$$MES = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2$$

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MES} \right) dB$$

Figure 10 - PSNR & MES Equations. (Anon., n.d.)

Image Scrambling

Image scrambling is a technique used to render an image imperceptible to the naked eye. This is achieved through rearranging the pixels in an image in an arbitrary fashion, without changing the content of the pixel values. Many of the encryption algorithms in this space have two stages, confusion and diffusion. A scrambling procedure is utilized to permutate the pixel positions in the confusion stage, while in the diffusion stage the pixel units are altered. When considering the standard of a scrambling algorithm we look at the entropy, computation length and correlation coefficient (Mondal, 2019). One particular section of image scrambling that has gained traction in recent years is image scrambling using chaotic maps. Chaos is studied under the field of chaos theory in mathematics, where it examines the behavior and condition of dynamic systems which are very sensitive to initial condition. Chaos can be defined by its 3 properties of deterministic, nonlinear and sensitive dependence. Chaos is deterministic meaning it can be explained by a mathematical model that is demonstrated as a simple equation. This equation can be returned as either a discrete equation or differential equation. The tent map is an example of a discrete equation, otherwise known as a chaotic map.

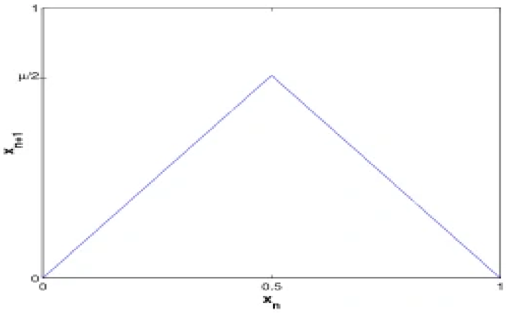


Figure 11 - Tent Map (Tom, 2013)

Nonlinearity refers to the indirect relationship between the input and the output. As we can see above the graph display a nonlinear plot. This property makes chaos suitable for cryptography. In the tent map equation, we have two parameters one is the control parameter, the other is the initial condition. The final property that describes chaos is sensitive dependence, this means a small change in the initial condition will have a significant effect on the outcome (Shelke & Metkar, 2016).

Related Work

There have been numerous applications of steganography using QR codes as the cover that have been recorded in the literature. Some of these applications combine various technologies with steganography to construct a robust system for secret communication. In a paper published in January 2019 a robust steganography method using QR codes for crossing domains is proposed and is dubbed as "EasyStego". Cross-domain steganography is defined as utilizing carriers which can be extracted in many domains to secretly store a message, file, image etc. (Luo, et al., 2019). The method focuses on preventing the disclosure of sensitive information in the physical domain (the physical world), as more attention is paid to the cyber domain (the world of binary data), leaving the physical neglected. Examples of information leakages in the physical domain come from packages, letters (e.g., from banks or hospitals) which if intercepted easily reveal sensitive information as they are printed in plaintext and don't require the use of any complex technology. An individual could easily root through a rubbish bin and discover important information that's printed on a piece of paper, thus it's imperative that protecting sensitive information in the physical domain be paid attention to. QR codes were chosen as the ideal container as they are not as affected physical distortion, have capability to cross domains and cannot visually be read by a person. Not only that, their popularity and widespread use means that they would not easily be detected that a secret message is being carried. The procedure of embedding the message using this method is split into several steps. It uses AES encryption to encrypt the data, dynamic Huffman encoding to compress the ciphertext, Reed-Solomon codes to compute error-correction codes and other mathematical equations to successfully embed the secret message in the QR code. The extraction process involves stitching the elements outlined in the embedding process back together, the data is then decompressed and finally the ciphertext is decrypted using the key that was initially used to encrypt the message which reveals the plaintext that is hidden in the QR code. The proposed system is then put to a series of tests to calculate its usefulness. The tests performed included a test to perform how well it crosses domains, its capacity, difference, and robustness.

The paper also provides a scenario where EasyStego could be used in the real world. Alice who resides in city A intends to send a package to Bob, who is in city B. Alice utilizes EasyStego to embed and encrypt the data that is required to send the package. The keys used for the encryption are then distributed by the cloud. The QR code is decrypted with the key3 by the postman in city A, this reveals the destination city of the package. Key2 is used by the postman in city B to decrypt the QR code which reveals the information of where the recipient lives. Upon receiving the package Bob can decrypt the QR code using key1 to reveal the information of who sent the package. Due to the QR codes error correction capability even if the QR code was to become damaged or dirty, the information would still be able to be read. During transmission individuals that do not have keys assigned to them cannot obtain the sender or recipients information thus providing confidentiality. Therefore, we can say the objectives of steganography have been adequately met. Overall, this paper focuses on preventing the leakage of information in both domains and proposes a robust system that can supersede some of the other common approaches to steganography.

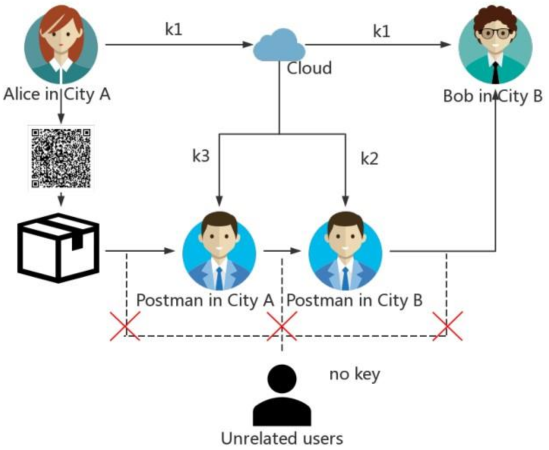


Figure 12 - A Real-World Usage Example for EasyStego. (Luo, et al., 2019)

(Sahu & Swain, 2019) proposed a technique that is based on pixel value differencing and modulus function (PVDMF). Using this technique, it increases the PSNR and payload capacity. Their approach is split into two versions, PVDMF 1 and PVDMF 2. These two versions utilize the distinction between succeeding pixels to embed the secret message this depends on an adaptive range table. It was found that using PVDMF 1 resulted in the PSNR increasing while using PVDMF 2 made the embedding capacity increase.

A new method to "secure updating and sharing of COVID-19 data in decentralized hospitals intelligence architecture" was proposed by (Mohsin, et al., n.d.) in 2021. Their proposed method attempts to solve two particular issues that occur when sharing significant amounts of healthcare data which includes ensuring the integrity and confidentiality of the data and the availability of the data due to failure of the network failure. Their method uses image steganography based in the spatial domain, alongside blockchain technology and the particle swarm optimization (PSO) algorithm. They describe their method in 3 distinct stages, pre-hiding, secret data hiding and transmission stages. The pre-hiding stage consists of locating the best location in the host image for hiding the data, its noted that grey scale images are used. The image is separated into four parts, the image is scanned and the PSO particles are determined. In the hiding stage the secret data is embedded into the image using the indicators that were outlined in the pre hiding stage, hashing is also used. Finally in the transmission stage blockchain technology is used to provide a secure channel for transmission of the stego images. The decentralized nature of blockchain technology means that there is no one central point that certifies the transactions between nodes, in this case the nodes are the hospitals. All hospitals in the network can retrieve the data in an instant without the need for approval by a third party, as all transactions are validated by at the very least 50% of the nodes in the network, which as a result renders the malicious altering of the transaction difficult.

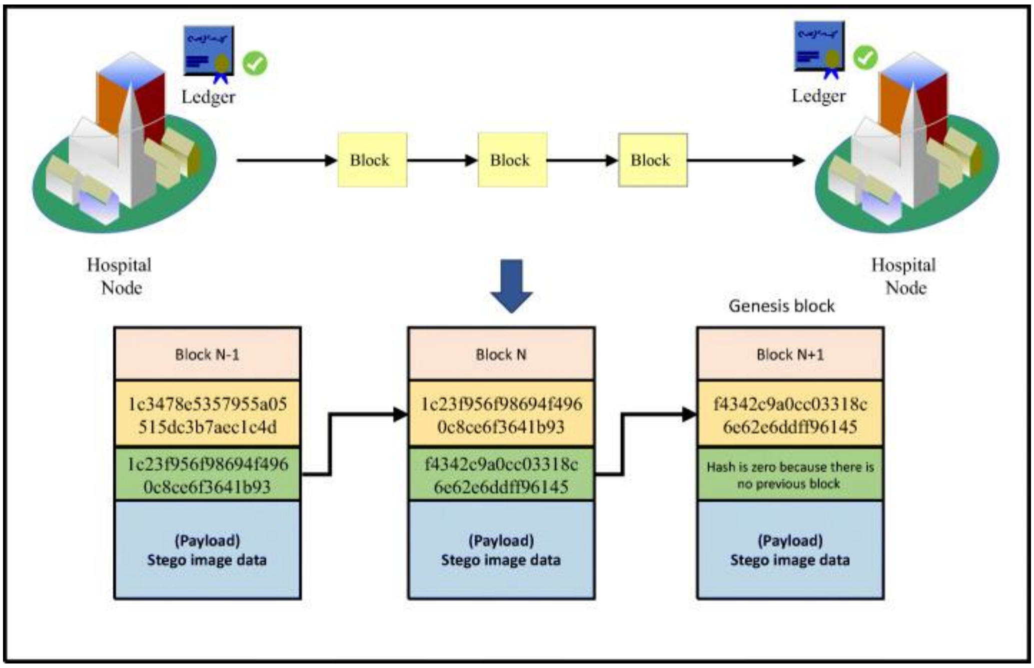

Ledger
Ledger
Block
Block
Block
Hospital Node
Hospital Node
Genesis block
Block N-1
1c3478e5357955a05 515dc3b7aec1c4d
1c23f956f98694f496 0c8ce6f3641b93
(Payload) Stego image data
Block N
1c23f956f98694f496 0c8ce6f3641b93
f4342c9a0cc03318c 6e62c6ddff96145
(Payload) Stego image data
Block N+1
f4342c9a0cc03318c 6e62c6ddff96145
Hash is zero because there is no previous block
(Payload) Stego image data

Figure 13 - The peer-to-peer transmission of the payload (Mohsin, et al., n.d.).

(Muhammad, et al., 2014) proposed a method that is based on stego-key directed adaptive least significant bit (SKA-LSB) substitution method and multi-level cryptography. Their technique focuses on providing a superior equilibrium between the quality of the image after embedding and security. The encryption key is encrypted using a two-level encryption algorithm (TLEA), and the secret message is encrypted using a multi-level encryption algorithm (MLEA). The result of this is then inserted into the image using an adaptive LSB technique. Their tests show that they are still able to attain a reasonable a decent sized payload when using this method and is not as complex to perform in comparison to other techniques out there.

(Zhou, et al., 2015) presented a novel image steganography method to limit the success of steganalysis by no longer using a cover image to embed the message. The method works by first gathering images to create a database, these images are indexed relation to their hash. It's noted that these images already have secret data embedded inside of them. A bit string is then created from the secret data and then separated into segments. To hide the data the images with the same hash sequence as the segment are selected from the database, these are the stego-images. Traces of changes to a cover image when embedding can be detected thus they showed through testing this method that this technique can withstand the current steganalysis tools.

(Darbani, et al., n.d.) published a paper in 2019 outlining a new method for embedding messages in JPEG images. JPEG images are a popular image format and are suitable for transmission due to their small size. Their proposed approach is separated in two sections, in the first section the image is divided into either smooth or hard blocks. The second section involves inserting the embedded message into a block. Two least significant bits of the pixels are utilized for embedding the message, this is completed in the JPEG compression prior to encoding. Their results display a higher capacity achievement in comparison to traditional techniques.

(Lin, et al., 2022) put forward an approach to ensure information privacy for data stored in QR codes through altering the data modules in the QR Code. They argue that current steganography techniques do not suit QR codes applications as they are pixel-orientated, while QR codes are module-orientated. Their system combines 3 modules into a category/group and alters these modules through the use of the error correction mechanism that QR codes have. Two bits of the secret data can be embedded into by changing one QR module. The information can only be accessed by a user with the secret key. The generated QR code is still able to be read by a scanner and does not affect the error correction mechanism.

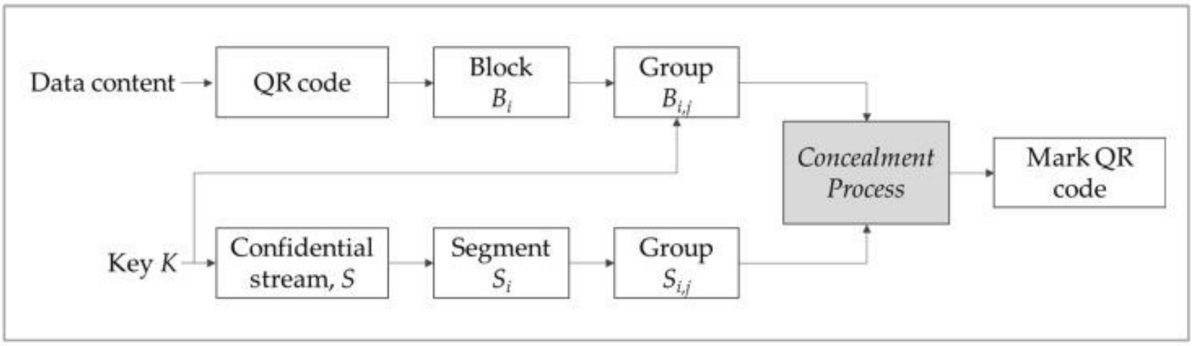


Figure 14 - The proposed approach (Lin, et al., 2022)

(Hassaballah, et al., 2021) published a paper that outlined a method called Harris hawks optimization-integer wavelet transform (HHO-IWT). This technique is based on image steganography and is used to ensure the security of data in an IoT environment. They embed secret message by using the HHO algorithm to pick the pixels that the data will be hidden inside of the integer wavelet transforms. The results of their tests present a method that provides a significant level of security and is difficult to detect with steganalysis.

Conclusion

It's clear the area of steganography is an ever-evolving essential part of information security that should continue to be studied as it offers a means for secret communication which can be useful in countries where digital communication is monitored and restricted. Its continued research presents multiple techniques that can be utilized to create a steganographic system that achieves Imperceptibility, robustness and provides an adequate embedding capacity for the secret message. QR codes are 2D barcodes that can be found on the internet and in the physical world which possess characteristics such as error correction which makes them an ideal cover medium for steganography. Through using techniques such as least significant bit steganography one can successfully embed a piece of data in a QR code using various tools and technologies available. Steganalysis on the other hand attempts to detect the use of steganography in a stego object, using various approaches such as statistical and visual techniques. Overall, there is no one technique used to perform steganography as there are numerous distinct approaches that have been recorded in the literature, some attempting to use steganography to solve real world problems.

Bibliography

1. admin, 2011. *QR Code Error Correction.* [Online]
   Available at: https://blog.qrstuff.com/2011/12/14/qr-code-error-correction

2. Anon., 2012. *Reed-Solomon Codes.* [Online]
   Available at: https://www.techopedia.com/definition/25798/reed-solomon-codes

3. Anon., 2019. *Types of QR Code.* [Online]
   Available at: https://www.qrcode.com/en/codes/

4. Anon., n.d. [Online]
   Available at:
   https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.418.9743&rep=rep1&type=pdf#:~:text=Since%20BMP%20uses%20lossless%20compression,to%20have%20less%20web%20applications.

5. Anon., n.d. [Online]
   Available at: https://d1wqtxts1xzle7.cloudfront.net/30900669/stegoverview-with-cover-page-v2.pdf?Expires=1635940450&Signature=NzP5Xl6rFNEhBBoSvHEU~uc1CxNuQNoSIQoC~IX1XQaesz2cHye6AksXS-CZADhMyroMMKoRhbRluHPLvkVCTS42AkMzjieS85Vq~009uqs3vRALTaeTHvP2Tx3vLeMT4qwfKtIQ~T9LOZc

6. Anon., n.d. [Online]
   Available at:
   http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.641.9370&rep=rep1&type=pdf#:~:text=Steganalysis%20can%20be%20broadly%20classified,in%20images%20embedded%20using%20steganography.

7. Anon., n.d. [Online]
   Available at:
   http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.740.3133&rep=rep1&type=pdf

8. Anon., n.d. [Online]
   Available at:
   http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.740.3133&rep=rep1&type=pdf

9. Anon., n.d. *Digital Image Data Representation.* [Online]
   Available at: https://knowthecode.io/labs/basics-of-digitizing-data/episode-14

10. Anon., n.d. *Introduction to Computers and Their Applications.* [Online]
    Available at: https://home.adelphi.edu/~siegfried/cs170/170l2.pdf

11. Anon., n.d. *Sample.* [Online]
    Available at: https://techterms.com/definition/sample

12. Assaad, A., 2019. *What's inside The QR code?.* [Online]
    Available at: https://medium.com/analytics-vidhya/whats-inside-the-qr-code-bf8a465378fd

13. Bhayani, A., 2020. *Everything that you need to know about Image Steganography.* [Online]
    Available at: https://www.codementor.io/@arpitbhayani/internals-of-image-steganography-12qsxcxjsh

14. Bhayani, A., 2020. *Everything that you need to know about Image Steganography | Codementor..* [Online]
    Available at: https://www.codementor.io/@arpitbhayani/internals-of-image-steganography-12qsxcxjsh

15. Brown, G., 2021. *Digital Audio Basics: Audio Sample Rate and Bit Depth.* [Online]
    Available at: https://www.izotope.com/en/learn/digital-audio-basics-sample-rate-and-bit-depth.html

16. Buchanan, J. M., 2004. *Creating A Robust Form of Steganography.* [Online]
    Available at:
    https://wakespace.lib.wfu.edu/bitstream/handle/10339/14775/Buchanan_STEM04.pdf

17. Chanu, Y. J., Tuithung, T. & Singh, K. M., 2012. *A short survey on image steganography and steganalysis techniques.* [Online]
    Available at:

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6203297&casa_token=D227gzKG34sAAAAA:1ztpmVv2mMI3viibY_ezxVeO5QpY2C6dQnnWyNuhpCnEbxk8I6N88ZxuLrVPon06NxQhcXvRLXIk&tag=1

18. Darbani, A., AlyanNezhadi & Forghani, M., n.d. *A New Steganography Method for Embedding Message in JPEG Images.* [Online].

19. Dias, D., 2017. *JPEG Compression Algorithm.* [Online]
Available at: https://medium.com/breaktheloop/jpeg-compression-algorithm-969af03773da

20. Djebbar, F., Ayad, B., Hamam, H. & Abed-Meraim, K., 2011. *A view on latest audio steganography techniques.* [Online]
Available at: https://ieeexplore.ieee.org/document/5893859

21. Garg, G., 2015. *How QR Codes work: Everything you need to know and more..* [Online]
Available at: https://scanova.io/blog/blog/2015/02/19/how-qr-codes-work/

22. Gupta, S., Gujral, G. & Aggarwal, N., 2012. *Enhanced Least Significant Bit algorithm For Image Steganography..* [Online]
Available at: http://www.ijcem.org/papers072012/ijcem_072012_08.pdf

23. Harrington, R. & Krogh, P., 2015. *Video File Format Overview.* [Online]
Available at: https://www.dpbestflow.org/video_format_overview

24. Hassaballah, M., Hameed, M. A., Awad, A. I. & Muhammad, K., 2021. *A Novel Image Steganography Method for Industrial Internet of Things Security.* [Online]
Available at: https://ieeexplore.ieee.org/document/9334425

25. Hope, C., 2017. *Parity bit.* [Online]
Available at: https://www.computerhope.com/jargon/p/paritybi.htm

26. Imani, H. & Rezaei, M., 2018. *Impact of Noise and Complexity on Targeted Image Steganalysis.* [Online]
Available at: https://ieeexplore.ieee.org/document/8457345

27. Jokay, M. & Moravcik, T., 2010. *Image-Based JPEG Steganography.* [Online]
Available at: https://www.sav.sk/journals/uploads/0317153109jo-mo.pdf

28. Jung, K.-H., 2019. *A Study on Machine Learning for Steganalysis.* [Online]
Available at:
https://www.researchgate.net/publication/332933805_A_Study_on_Machine_Learning_for_Steganalysis

29. Kumar, M. & Yadav, M., 2014. *Image Steganography Using Frequency Domain.* [Online]
Available at: https://www.ijstr.org/final-print/sep2014/Image-Steganography-Using-Frequency-Domain.pdf

30. Kumar, S. & Reddy, P., 2007. *Steganalysis Techniques: A Comparative Study.* [Online]
Available at: https://scholarworks.uno.edu/cgi/viewcontent.cgi?article=1562&context=td

31. Kumar, V. & Kumar, D., 2017. *Performance Evaluation of Modified Color Image Steganography Using Discrete Wavelet Transform.* [Online]
Available at: https://www.degruyter.com/document/doi/10.1515/jisys-2017-0134/html

32. Lin, P.-Y., Lan, W.-S., Chen, Y.-H. & Wu, W.-C., 2022. *A Confidential QR Code Approach with Higher Information Privacy.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8871438/

33. L, P. & B, D., 2008. *Information Hiding: A New Approach in Text Steganography..* [Online]
Available at: http://www.wseas.us/e-library/conferences/2008/hangzhou/acacos/116-586-634.pdf

34. Luo, Z. et al., 2019. *EasyStego: Robust Steganography Based on.* [Online]
Available at: https://www.mdpi.com/2073-8994/11/2/222/pdf

35. Mathuria, M., 2017. *A Review on QR Codes.* [Online]
Available at: https://www.researchgate.net/profile/Manish-Mathuria/publication/316177848_A_Review_on_QR_Code/links/5d4832e592851cd046a2d5df/A-Review-on-QR-Code.pdf

36. Mishra, M., 2013. *A Survey on Digital Image Steganography and Steganalysis.* [Online]
Available at:
https://www.researchgate.net/publication/303940864_A_Survey_on_Digital_Image_Steganography_and_Steganalysis

37. Mohsin, A. H., Zaidan, A. A., Zaidan, B. B. & al, e., n.d. *PSO–Blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture.* [Online]
Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7821848/

38. Mondal, B., 2019. *Cryptographic image Scrambling techniques.* [Online]
Available at:
https://www.researchgate.net/publication/331064749_Cryptographic_image_Scrambling_techniques#:~:text=Image%20scrambling%20is%20the%20method,encryption%20algorithms%20were%20being%20proposed.

39. Monika, A., 2013. *Text Steganographic Approaches: A Comparison.* [Online]
Available at:
https://www.researchgate.net/publication/235438740_Text_Steganographic_Approaches_A_Comparison

40. Muhammad, K. et al., 2014. *CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method.* [Online]
Available at: https://d1wqtxts1xzle7.cloudfront.net/51390517/CISSKA-LSB_MTAP-with-cover-page-v2.pdf?Expires=1650742962&Signature=NSbXq2QnHvRG4QgPFiqXBx7prPN-vXlQXJv4jOU68Dd6t9h~6ielMue8gNM0B9FVznxhCkpS~pBvU4lMxIM~4e5TNyueGNaOeXyEBlpU-hmy9cWNQ8YmfTZ98dg5fZWROGRBYoe7iUAG

41. Narayanan, S., 2012. *QR Codes and Security Solutions.* [Online]
Available at: https://www.ijcst.org/Volume3/Issue7/p13_3_7.pdf

42. Nosrati, M., Karimi, R. & Hariri, M., 2011. *An introduction to steganography methods.* [Online]
Available at:
https://www.researchgate.net/publication/308646775_An_introduction_to_steganography_methods

43. Orlandi, V., 2017. *Imagify.* [Online]
Available at: https://imagify.io/blog/lossless-vs-lossy-image-compression/

44. Paladion, 2005. *Stegananalysis.* [Online]
Available at: https://www.paladion.net/blogs/steganalysis

45. R, B. K., Prasanth, K. T. & M, S. B., 2017. *An overview of text steganography..* [Online]
Available at: https://ieeexplore.ieee.org/document/8085643

46. Sahu, A. K. & Swain, G., 2019. *An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function.* [Online]
Available at: https://www.researchgate.net/profile/Aditya-Kumar-Sahu/publication/332570871_An_Optimal_Information_Hiding_Approach_Based_on_Pixel_Value_Differencing_and_Modulus_Function/links/5eedeeb492851ce9e7f49e67/An-Optimal-Information-Hiding-Approach-Based-on-Pixel

47. Scott, 2020. *How Do QR Codes Work? QR Code Technical Basics..* [Online]
Available at: https://www.sproutqr.com/blog/how-do-qr-codes-work

48. Scott, 2020. *QR Code Minimum Size: How Small Can a QR Code Be?.* [Online]
Available at: https://www.sproutqr.com/blog/qr-code-minimum-size

49. Sha, L., 2017. *Image Compression.* [Online]
Available at: https://link.springer.com/referenceworkentry/10.1007%2F978-3-319-17885-1_584

50. Sharma, S. & Kumar, U., 2013. *Review of Transform Domain Techniques for Image Steganography.* [Online]
Available at:
https://www.researchgate.net/publication/287210148_Review_of_Transform_Domain_Techniques_for_Image_Steganography

51. Shelke, R. & Metkar, S., 2016. *Image scrambling methods for digital image encryption.* [Online]
Available at: https://ieeexplore.ieee.org/document/7857449

52. Singh, P., 2016. *A Comparative Study of Audio Steganography Techniques.* [Online]
Available at: https://www.irjet.net/archives/V3/i4/IRJET-V3I4117.pdf

53. Stanger, J., 2020. *The Ancient Practice of Steganography: What Is It, How Is It Used and Why Do Cybersecurity Pros Need to Understand It..* [Online]
Available at: https://www.comptia.org/blog/what-is-steganography

54. Tiwari, S., 2016. *An Introduction to QR Code Technology.* [Online]
Available at: https://ieeexplore.ieee.org/document/7966807

55. Tom, 2013. *CHAOS THEORY: TENT MAP (PART 1).* [Online]
Available at: https://theworldismysterious.wordpress.com/2013/10/11/chaos-theory-tent-map-part-1/

56. Waleed, J., 2015. *Structure of QR-Code.* [Online]
Available at: https://www.researchgate.net/figure/Structure-of-QR-Code_fig1_275650586

57. Waykule, J., 2015. *ARM Controller Based Image Steganography Using LSB Algorithm.* [Online]
Available at:

https://www.researchgate.net/publication/288630141_ARM_Controller_Based_Image_Steganography_Using_LSB_Algorithm

58. Yunxia , L. et al., 2019. *Video steganography: A review.* [Online]
Available at:
https://www.sciencedirect.com/science/article/pii/S0925231218312608?casa_token=nZEeNC9eoRUAAAAA:OafeRjh3IbKJDlAmP_jg1px3l-bgjc24bSEovqHwK8luREMY_VzV54AV4tkO_pA4a13DPf-tNQ

59. Zhou, Z. et al., 2015. *Coverless Image Steganography.* [Online]
Available at:
https://d1wqtxts1xzle7.cloudfront.net/59373533/Cloud_Computing_and_Security20190523-36641-xrsqvh-with-cover-page-v2.pdf?Expires=1650744399&Signature=LJJWIBiMVBRiItOBgfXhJW7LVIc-5BOHBe2ZVwUvpAdItF11Tao0I2ThFO0X9UYXFlPhaOteyE-XbpABwTQB6tkb0HF0okCcRZZiPmE3ib

Table of Figures and Tables