

Steganography in digital media

Pricope Stefan-Cristian
psir2384@scs.ubbcluj.ro

Dr. Suciu Mihai
mihai-suciu@cs.ubbcluj.ro

Abstract

Steganography is the science of concealing a piece of information within another piece of information without affecting the latter in a noticeable way and therefore alerting any intruders of the existence of the former. This paper presents both existing and new ways of embedding computer files and data into different digital multimedia formats as covert as possible while still allowing the encoded information to be retrieved at a later time without any significant losses.

Contents

1	Introduction to computer steganography	3
2	Steganography methods	4
2.1	Least Significant Bit(LSB) Insertion	4
2.1.1	Sequential	4
2.1.2	Scrambling	5
2.2	Metadata encoding	6
2.3	Unused space embedding	7
3	Image file formats and steganography techniques	9
3.1	Introduction	9
3.2	BitMap Picture (BMP)	10
3.2.1	Image sub-block scrambling using the BMP format	11
3.3	Portable Network Graphics (PNG)	16
4	Audio file formats and steganography techniques	17
4.1	Introduction	17
4.2	Additional techniques used in audio steganography	17
4.2.1	Embedding within certain frequencies	17
4.3	The MPEG-1/2 Audio Layer III (MP3)	17
4.4	Waveform Audio (WAV)	17
5	The Steganos Project	18
5.1	Used technologies	18
5.1.1	C++	18
5.1.2	CMake	18
5.1.3	CXXOpts	19
5.1.4	Lodepng	19
5.1.5	MMSSTV Engine for Windows	20
5.1.6	Robot36 for *NIX based systems	20
5.2	Application architecture	20
5.3	Benchmarks	20
5.4	Further work	20
6	Conclusion	21
	Bibliography	22

Chapter 1

Introduction to computer steganography

The practice of hiding and securing information and messages between different parties has played a major part alongside human history, especially during times of war when it was vital that the enemy didn't intercept the strategies and even if they did, they would have no idea what to do with them and would have to dedicate a lot of time, money and personnel to decode the communications. Two of the most famous manifestations of this practice are cryptography and steganography[?].

Trying to differentiate between cryptography and steganography is not difficult, the only thing they have in common is their end goal - making sure that a piece of information sent from one place to another is secured and that only the right recipient will be able to read and understand the received information. The difference lies in the methods they use and the time it takes to reach that goal.

Cryptography focuses on altering the information itself, encrypting it using a key only known by the receiver and sender¹, making it harder for any possible meddlers to alter the meaning of the message or even just understand it. Steganography is more concerned on hiding the fact that there even is any information being transmitted usually by embedding it in something else (hereby referred to as a cover), thus if any interlopers were to actually look at the cover, they wouldn't even be aware of the fact that it contained secrets.

In other words, both methods are meant to be used over an open and unsafe environment, and

while cryptography tries to hide the contents of the message but not the fact that there is a message being sent, steganography tries to hide the communication altogether. The main advantage of these 2 methods is that they are not exclusive, they can be used together for maximum safety of the information.²

With the evolution of the Internet and the increasing usage of personal computers in day to day activities we needed to secure the data sent over the network between the users. The efforts were lead by cryptographers who developed thousands of algorithms for encrypting the information and the very few remarkable ones are still being used³. But that doesn't mean steganography was left behind, researchers developed plenty of new algorithms for hiding information using digital files as a cover and the Internet as the transmission environment.

In theory all types of digital files can be used as cover - shared libraries and executables can be edited to include the hidden data and then be re-compiled/rebuilt, text files and documents could be modified to enclose the information in secret places/paragraphs, and multimedia such as images, music and video files can be changed to carry the digital data into their metadata, pixels, audio frequencies, motion vectors and much more. This paper will go into details about some of the most popular formats used for multimedia files and showcase their internal structure and document techniques used in steganography.

¹This is only true in symmetric cryptography and is a gross oversimplification of cryptography as a science, but it is just meant to get a point across and help differentiate between the 2.

²The speed of encoding/decoding the information is greatly decreased when these 2 are combined which is the reason that nobody merges them, preferring to just use encryption to keep the information safe.

³The reason cryptography is in the spotlight is because it is much faster, mathematically proven, and it hides all the data without leaving anything in plain sight (like steganography does with the cover).

Chapter 2

Steganography methods

2.1 Least Significant Bit(LSB) Insertion

2.1.1 Sequential

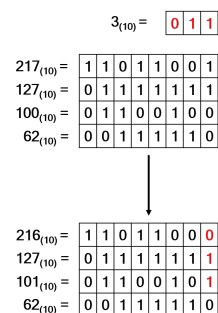


Figure 2.1: How the sequential Least Significant Bit change works

Least Significant Bit or LSB is by far the most used method when talking about any type of steganography. Given that the smallest unit a computer can understand and process is usually a byte, altering only the least significant bit will not change the transmitted information in a noticeable way to any external parties. It is much easier to showcase what a byte contains and what the LSB change implies and how it works. A byte contains 8 bits, so this means that the values a byte can take range anywhere from 0 to 255 (inclusive)¹. Let's assume that we have an array of 4 random values in consecutive memory : 217, 127, 100, 62 (all values are in decimal), each stored on exactly one byte, and that we want to hide our grade in Numerical Analysis from our parents (in this case a 3) using a LSB substitution. The process would be something like this :

¹This is the case for unsigned bytes, but given that we are talking about a method that only deals with the least significant bit, we can safely ignore the most significant bit, also known as the sign bit.

²Steganalysis is the study of steganographic methods, including but not limited to : differences in file sizes or in color histograms, secret message redundancy, embedding capacity and performance etc.

As we can see from Figure 2.1, we have successfully altered the least significant bit of the first 3 bytes of the stream in order to hide our grade : 217 became 216 when we changed the last bit from 1 to 0, 127 was unchanged because it already had the last bit set, and the third byte became 101 after toggling the final bit. Furthermore, the rest of the stream (the fourth byte, 62) was not affected because we already hid the entirety of our secret message. While this is great because we only hide exactly as much as we need and not a byte more, we have a high risk of corrupting the hidden message in case our cover image gets compressed or loses even a single byte when sent over a network. Basically, we are trading data redundancy in order to get simplicity and efficiency.

Sequential LSB insertion is the simplest and most common way of embedding any kind of in-

formation into a byte stream that is then shared. It has been thoroughly discussed by a great deal of researchers and has been the subject of many papers where it was analyzed and benchmarked[?][?] . Being the most popular technique also means that any flaws the method has are widely documented and showcased. Steganalysis² performed on outputs created using this algorithm has shown that it is unreliable to stay undetected if an outside party intercepted the message containing the cover file[?]. Furthermore, doing a simple reverse engineering on the algorithm reveals even more issues with this naive encoding : if a single bit that is part of the secret message was flipped from the cover file byte stream, the message would become corrupted and the original secret would be lost forever. This means that sequential LSB insertion is not resistant at all to any form of lossy compression where some of the original data may be lost in order to reduce the used disk space because it would lose most, if not all, of the embedded file information.

Furthermore, it is extremely easy to compute the carrier storage, i.e. how many bytes we are able to hide into the cover file or in other words, the maximum size of the secret message that we can successfully embed without losing anything while still keeping a covert profile. Assuming *CDS* or Cover Data Size (how many bytes are actually used to store the pixel information, no metadata information or chunk headers or anything like that), then the *MMS* or Maximum Message Size would be equal to

$$MMS = [CDS / 8] \text{ bytes}$$

or the integer part of CDS divided by 8. This should come as no surprise since sequential LSB is altering 1/8 (an eighth) of each byte when embedding a bit of the secret information so the maximum capacity makes sense to also be 1/8.

2.1.2 Scrambling

As documented earlier, sequential LSB insertion algorithm has a decent number of flaws so it was needed to develop some new techniques that are not relying as much on the cover file not losing a few bytes or undergoing a compression algorithm. In other words, it needed to introduce a few redundancies to ensure that the secret message wouldn't be lost as easily and that the message was not written in a sequential and direct order. They achieved this

by not just changing the least significant bit in a sequential order, but by writing in an apparently random order (in simpler terms, scrambled) that could be reproduced by having the right key or by using the same algorithm in order to retrieve the embedded information. In this subsection we will discuss a few of the most common scrambling techniques and introduce a new one as well.

The most popular methods used for scrambling secret messages into various covers usually choose to simply ignore the entire data stream and only focus on a specific subsection and choose that as the carrier environment. After a smaller subsection is chosen (it can still be the entire actual data part of the cover, it's not an actual rule), we will have to generate the order in which we will write the message information. As mentioned before, this is derived using a key known only to the sender and the receiver that can be shared between the 2 parties using another transmission environment, preferably one that is encrypted and safe. The main logic is to use that passkey as a seed in a valid pseudo random engine when generating the order so that there are no collisions and that only the right key will produce the right order.

There is also an option for when there is no safe method of transmitting a key and that is to scramble the secret message within a certain order that is not sequential. But as long as the receiver and transmitter have no way of communicating the algorithm used in embedding the message (can also assume this because they have no way of sharing the key), this option is useless but is still interesting to look into because they are a variation of the other mentioned option. Having no key to generate the order makes this option easier to showcase(since we don't have to also simulate a pseudo-random engine and a seed). Let's assume we have a byte stream of random data³ and we want to again hide a grade from our parents, in this case a 6 (or 110 in binary). Instead of hiding the grade sequentially, the bits will be hidden into the last bit of every third byte and it will end up looking something like this :

³Now the actual data meaning can be safely ignored because we only work on the LSB and we have seen in the previous chapter it does not alter the data in a significant way such that an intruder might notice something is wrong.

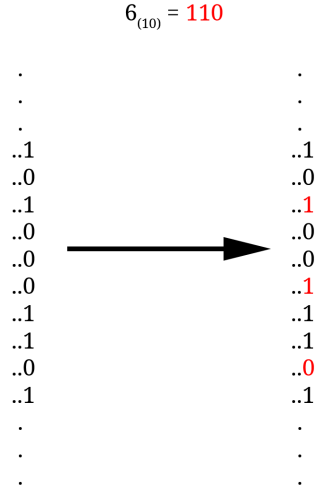


Figure 2.2: An example of scrambling LSB insertion

The key difference from sequential LSB insertion is that as long as the sender and receiver are aware of the used algorithm, any external parties will not be aware of the secret embedded message. Furthermore, this method has proven very useful because there are infinite ways of scrambling a message into the cover file without alerting any possible intruders and it ends up being an extremely hard guessing game for the attackers in their goal to extract the information.

The carrier capacity appears initially to be the same, but it is very important to remember that the scrambling algorithm used will usually work on a subset of the cover data bytes, not the entirety of it (just like in figure 2.2 we used only each third byte to store the information). Using the same notations as in the previous chapter we get that

$$MMS \leq [CDS / 8] \text{ bytes}$$

so in most cases, the scrambled MMS will be smaller than the sequential MMS. However it is very important to note that this decrease in size comes with a great increase in data security and message safety.

This paper also introduces a new type of scrambling algorithm created by the authors that only works on lossless image formats that do not use any kind of interlacing when rendering the picture. It relies on scrambling the secret message into the image sub-blocks in a specific order that can only be deduced by having the right passkey. More information on this method is presented in chapter 3.2.1 after the introduction of image basics.

2.2 Metadata encoding

The word metadata was formed from combining the word "data" with the prefix "meta-" and is used to describe a special type of data that has information about other types of data[?]. In simpler terms, it means "data about data" and it keeps the same meaning in the digital world. It is much easier to visualize and understand the concept of metadata using a simple example : let's take a picture stored on a computer.

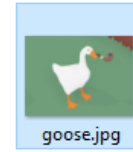


Figure 2.3: A simple image file

As noted in the introductory chapter, every file can be seen as a byte stream. However it is very important to keep in mind that those bytes don't represent only the image data, the pixels seen on the screen, they are much more. They also contain information about the camera used to take the photo, the location where it was taken, when the file was created, when it was modified, etc. All of the aforementioned information forms the metadata. It varies from file format to file format where they store this information in the byte stream, how many bytes are allocated for each piece of information or if it even has any effects on the actual file data. Most of the time metadata fields are only parsed by the renderer software and are mostly hidden to the user, but there are a few ways of viewing the information:

- using a hex editor to view the raw bytes of the file and then mapping those bytes to the publicly available file format specifier - an international approved paper which specifies the meaning of the bytes in the file binary stream
- using the operating system to view more properties about the file, not just the actual data interpreted and displayed to the end user
- using a third party tool which already knows the mapping and meaning of each sequence of bytes in the file binary stream and can successfully parse the metadata

```

sleshwave>exiftool goose.jpg
ExifTool Version Number      : 10.80
File Name                    : goose.jpg
Directory                   : .
File Size                    : 16 kB
File Modification Date/Time   : 2020:04:21 19:44:09+03:00
File Access Date/Time        : 2020:04:21 19:44:09+03:00
File Inode Change Date/Time   : 2020:04:21 19:44:09+03:00
File Permissions              : rwxrwxrwx
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit               : inches
X Resolution                  : 72
Y Resolution                  : 72
Image Width                   : 1000
Image Height                  : 750
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1000x750
Megapixels                   : 0.750

```

Figure 2.4: Example of using a tool to read file metadata

The focus of this sub-chapter will be on the metadata fields that don't necessarily have any important effect on the data representation and theoretically could be altered, such as any comments from the author or any contact information. In the case of an image, changing important metadata fields such as the width or height of the picture are not very covert methods of embedding any information at all, proving that not all fields are equally important. We are left with the more *useless* metadata fields, but the good news is that most file formats allow these fields to have a variable size which is perfect for any steganographic purposes because it removes the size constraint of the secret message. While in theory this allows for ∞ MMS, there are a few limitations in place that significantly reduce that number:

- computers have a limited amount of storage space, in most modern day computers that would be about one terabyte. This means that the MMS will certainly be smaller than that.
- most file formats that allow metadata fields to be embedded in the byte stream of the file by an external party also have a sequence of bytes that indicates how long that metadata field is (how many bytes it contains). In most cases that sequence is 4 bytes long so this usually results in a MMS of $2^{4*8} = 2^{32} \approx 4.29 \text{ gigabytes}$.
- in the pursuit of keeping the existence of a secret inside the cover file as covert as possible, the MMS is again limited by the CDS. This happens because the size of the cover file is

almost always displayed to any parties without any interactions and it needs to not raise any suspicions or attract unwanted attention to the actual contents of the file. To give an example, it would be very weird to see a simple image in FULL HD resolution have a size of two gigabytes and will almost certainly alert any intruders. It is extremely hard to say an exact MMS based on this limitation because it depends on the original cover file size and it should be relative to that number. It is recommended that $MMS \leq 50\% * CDS$.

In the end it is important to note that metadata secret encoding is the most trivial method of embedding secret information into different kinds of cover files. However, this method comes with a great cost: almost every single tool that specializes in extracting metadata will be able to detect and identify our message without too much hassle because the final cover file still has to respect the format specification.

```

sleshwave>exiftool -s -Comment goose.jpg
Comment                        : Meet me tonight at 10PM

```

Figure 2.5: Example of message hidden in a file in the metadata section

2.3 Unused space embedding

Usually most file formats and even internationally approved and used protocols such as the TCP/IP have unused bits or bytes in their composition, either for future proofing the format in the form of reserved space or simply to serve as padding space mainly present to help the associated parsers.

One well known example of this is found in the BMP file format which appears only in the cases where the width of the image is not a multiple of 4. The standards specify that in this situation there needs to be added the right amount of bytes to fill so that the width will be divisible by 4. So if an image has a resolution of 1920x1080 (the width is the first number), there won't be a need for any padding bytes because

$$1920\%4 = 0$$

On the other hand, if the image had a resolution of 125x100, we would instead have

$$125\%4 \neq 0 \implies 4 - (125\%4) = 4 - 1 = 3 \text{ bytes}$$

to serve as a padding for each pixel line, ending up in a total of $100 * 3 = 300$ bytes of simple, raw,

unused space that most BMP parsers will ignore because they know that data is meaningless.

Another very good example is in the case of the IPv4 packet header which has a reserved bit in the flags subsection, or to be more precise, the 49th bit. According to RFC3514[?] it is meant to be a security bit representing the true intent of the packet (GOOD or EVIL), however it is important to note that it was an April Fools informational memo and it is most likely that altering this bit will still go undetected by any kind of firewall or intrusion prevention system.

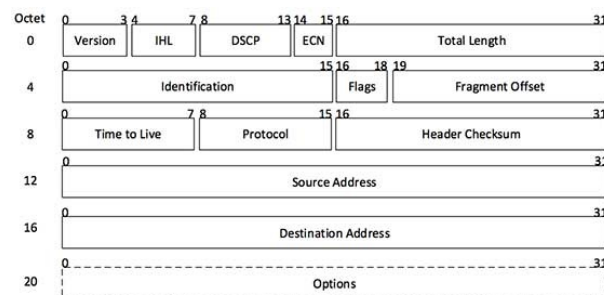


Figure 2.6: The structure of an IP packet

Given the IP packet header specifier represented in Figure 2.6 it becomes trivial to alter the first bit of the flags section to the current bit of a secret and then over multiple sent packets to actually send the message in one of the most covert ways possible. Furthermore, it is very important to note the contribution done by Kamran Ahsan and Deepa Kundur in their 2002 article entitled "Practical Data Hiding in TCP/IP"[?] because they also achieve the ability to send covert information by taking it one step further: using IP packet headers that may actually even be in use and by using Chaos Theory in the values of the Identification field sent over.

However, there is still one very important spot left in a file's byte stream where the secret message could easily be hidden: at the end of it. Most file formats either have specially crafted headers that announce the end of the file⁴ or have a few bytes reserved at the beginning of the file that mark the length of the data⁵. It is important to note that both of these methods basically produce the same result technically speaking: a superior margin, a maximum amount of bytes that are to be read and interpreted by the parsers that contain the data relevant to the

current file. After that region has ended, it is a free-for-all memory territory for secrets to be embedded. The same limitations from the previous chapter still stand, it is recommended that $MMS \leq 50\% * CDS$ in order to remain as covert as possible while still exfiltrating data.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
0009B8A0 ED C2 FF FB C5 F8 C5 A3 C8 B9 8D 98 32 A8 FA DC iÄÿuAøÅÆÈ¹."2"úÜ
0009B8B0 D2 28 41 38 C7 52 D0 15 3A 3B F4 8B E1 A2 B3 4E Ò(A8ÇRÐ.;;ó<á<³N
0009B8C0 A2 B3 A3 17 9B B0 60 93 51 8A 73 D9 73 47 9D ED <³£.;>°""Q&SûsG.í
0009B8D0 3F 5E F5 E2 47 F4 1C 0C F0 39 5C FF 24 37 3E EB ?^ôaGö..ô9\y$7>ë
0009B8E0 17 FD 9B 37 C4 59 D9 E8 A7 78 15 91 40 8C F0 06 .ý>7ÄYÜè$×.`@æð.
0009B8F0 A2 D3 FF 03 D4 FE E5 11 BA A8 95 1C 00 00 00 00 <öÿ.Ôpá.°".....
0009B900 49 45 4E 44 AE 42 60 82 68 65 6C 6C 6F 20 77 6F IENDËB`hello wo
0009B910 72 6C 64 rld
```

Figure 2.7: Simple example of hiding a note after a file has ended

⁴One good example is the PNG format which has an IEND header and a couple of other information to mark that the image data has ended and that there is nothing left that is relevant to the parser. More information regarding this format is available in chapter 3.2.

⁵This method is found in BMP or WAV file formats usually, it is very simple and easy to work with for parsers. More details in later chapters.

Chapter 3

Image file formats and steganography techniques

3.1 Introduction

An image is a two-dimensional representation depicting any possible subject conceivable by human imagination, captured using an optical device (such as a camera or a telescope) or a natural object (human eyes). The image can then be rendered and displayed for other people to see either manually (by painting, carving etc.) or automatically (by using a computer). In this chapter we will focus on images captured using digital optical devices that are rendered automatically. The correct term for them is digital images, but throughout the rest of the paper they will be referred to as images for convenience.

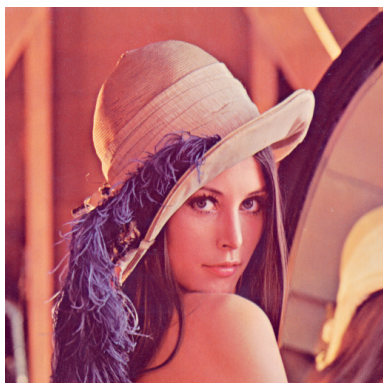


Figure 3.1: Lenna - Classic example of a digital image

Computers are programmed to do operations in a clear sequential way and this rule doesn't change when working with pictures. In order for a com-

puter to be able to render an image, it needs to know some general metadata information about the photo, such as the width and height, as well as the data bytes of the image. These bytes are the actual representation of the picture which compose the two-dimensional pixel map¹. A pixel is the smallest unit that a computer monitor can read and display. The pixel color is the result of merging the different color channels which compose the picture (such as RGB, YUV, YCbCr etc.). Here is an example of the entire process - let's assume that from the image data bytes the first 3 bytes have the decimal values 20, 127, 250 and that it uses the RGB color model. This means that when the computer will have to render the image, the first pixel will have the red component equal to 20 (0x14), the green equal to 127 (0x7F), and the blue equal to 250 (0xFA), in what will finally be interpreted as #147FFA by the monitor (variation of light blue).

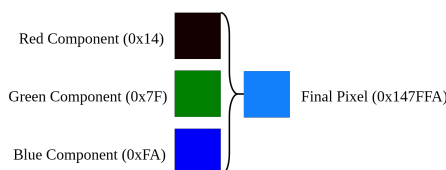


Figure 3.2: How 3 colors channels build the pixel

By merging multiple pixels over a two-dimensional space, they will eventually start to resemble an image that can be stored on a disk as a byte stream and can be rendered anytime by parsing

¹This is true for a lossless format, where each pixel is stored in memory. It is not exactly the case for lossy formats such as JPEG where the image goes through processing before being rendered. More information later in the chapter.

the aforementioned stream. Each pixel can be represented as a point in that space with coordinates that are part of the unsigned integer domain. An entire row of pixels, i.e. pixels that have the same ordinate value, is sometimes also referred to as a scanline because in the earlier days of modern computing, computers would be given the width of the image and based on that value they would read a precise amount of bytes and render it on the screen before moving on to the next scanline, repeating this process until there would be no more information.

It is important to note that most of these developments have been done in a time where the maximum storage was extremely limited and not very fast, very different from what it is today. In order to save some space they looked into different compression algorithms to apply to the byte streams and today they fall into two distinct categories: the lossless algorithms are the ones that compress all the original information without destroying any of it, while on the other hand there are the lossy algorithms which are able to identify which information is useless and delete it accordingly. This concept also applies to file formats and we will see in later chapters more concrete examples.

With all of this information in mind, we can now proceed to discussing the most commonly formats commonly used in today's.

3.2 BitMap Picture (BMP)

The BMP file format, also known as the device independent bitmap file format (DIB), bitmap image file or just bitmap, is a lossless² image file format originally designed by Microsoft back in 1986 in order to store two-dimensional digital images on their Windows operating system. Over the years it has developed plenty of variations and extensions that were based on the original specification but this paper will focus only on the most common available ones, no extended versions that are looking to improve the format since they do not add anything interesting or new to the way the format stores the data thus affecting the steganography algorithms.

As with almost every file format, the final BMP byte stream can be seen as a result of the merge between the BMP header which contains metadata about the file and the BMP data which is the actual pixel information. As we can see from table 3.1, the BMP header stores a lot of important information about the image that is useful for any rendering software while making sure to allocate enough memory to be able to display the picture on the screen and other essential steps. It is also important to note that all the structures seen in the BMP header use the little-endian format for representation and are usually more troublesome on the systems that have the default set as big-endian.

Information	Size	Offset	Description
Signature	2 bytes	0x00	Two chars, 'B' and 'M'
File size	4 bytes	0x02	Total file size in bytes
Reserved	4 bytes	0x06	Unused space
Data offset	4 bytes	0x0A	Offset to get to the actual BMP data
Size	4 bytes	0x0E	Size of the left header information
Width	4 bytes	0x12	Horizontal size of the image
Height	4 bytes	0x16	Vertical size of the image
Planes	2 bytes	0x1A	Amount of image planes
Bits Per Pixel	2 bytes	0x1C	How many bits are used to represent each pixel
Compression	4 bytes	0x1E	Indicates the type of compression used
Image size	4 bytes	0x22	The size of the compressed image, can be 0
X pixels per Meter	4 bytes	0x26	Horizontal resolution in pixels/meter
Y pixels Per Meter	4 bytes	0x2A	Vertical resolution in pixels/meter
Colors Used	4 bytes	0x2E	Number of actually used colors (based on Bits Per Pixel)
Important Colors	4 bytes	0x32	Number of important colors (usually all)

Analyzing the obligatory BMP header fields we realise that most of them are useless for any steganographic purposes mainly because they can't be altered without having major consequences on the

renderer software but there are still a few interesting ones left:

- The 4 bytes that are reserved and unused

²It is true that the format specification standards supports compression but further research reveals that currently it only supports lossless types of compression, such as the Huffman or Run Length Encoding algorithms.

could be very well put to use by using the methods presented in chapter 2.3, so we can use either this space to send parts of a message over multiple BMP files, or we can store the secret message size in these 4 bytes and write the secret after the actual image data has ended.

- Data offset could be useful because some renderers use this field to indicate the offset of the actual image data and just skip any other irrelevant metadata information, allowing us to hide information in those fields.
- The width and the height of the image usually are altered to hide bottom parts of the image that may contain hidden information or by masking the result of the merge of two images and just showing the top one. Let's take for example this image of the sun that is obviously missing a part for demonstration purposes.

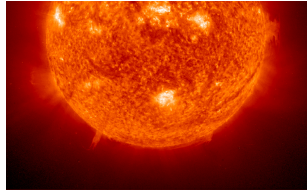


Figure 3.3: Incomplete sun image

However if we adjust by trial and error the height of the image to see if there is any more bytes to render, we would notice that there really is a message hidden with those bytes that some steganalysis softwares would detect but any renderer software such as the Windows Media Viewer would always miss. In other words, we have tricked the software to not display more scanlines than we wanted it to display, even though the information is there, not corrupted in any way.



Figure 3.4: Complete sun including the hidden message

Moving on from the metadata block of the BMP format to the actual data byte stream, we find additional interesting information about how the pixel data is actually stored. Most images use the Red, Green and Blue also known as RGB values to compose the final pixel color, but for an unknown reason the creators of the bitmap format decided to store the information in the reverse order in the data stream as Blue, Green, Red or BGR. However this is not the only change they made from the other common image formats available at the time: rather than storing the scanlines from a top to down order, BMP decided to store them bottom-up.

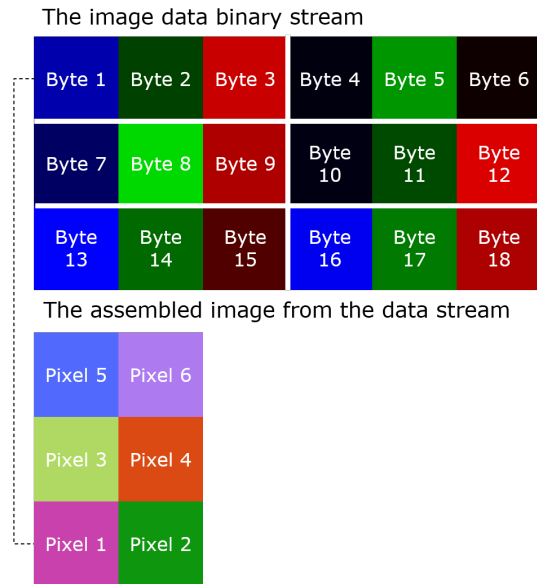


Figure 3.5: How the BMP image is rendered

This behaviour can be noticed in figures 3.3 and 3.4 where the top part is cropped in order to hide a message and we can now understand why it is only that part that can be made redundant in the steganography process: because the last bytes of the image data binary stream are actually responsible for the rendering of the top section of the picture. Seeing and understanding how the carrier format works is the first and most important step in embedding messages in a covert way.

3.2.1 Image sub-block scrambling using the BMP format

Sub-block scrambling is a type of scrambling algorithm, like those introduced in chapter 2.1.2, that can be applied to images stored in the BMP format. It was created by the author of this thesis based on

the idea of the JPEG format and the algorithm it uses during compression that is applied only on sub-blocks of 8x8 size. We mentioned in chapter 2.1.2 that most scrambling algorithms have

$$MMS \leq [CDS / 8] \text{ bytes}$$

but the target was to design and implement an algorithm which can make use of all the bytes available in the cover, and we ended up with this method which has

$$MMS = [CDS / 8] \text{ bytes} \quad (3.1)$$

making it similar in storage capacity to a sequential algorithm. That performance was achieved following a simple procedure:

- Separate the image into multiple blocks of BLOCK_SIZE (this is a global constant value

which is usually equal to 8 but can be higher or lower). It doesn't matter if the width or height of the image are not a multiple of BLOCK_SIZE, the algorithm also works with non-square blocks.

- The algorithm needs a password to work with in order to use it as a seed when generating a permutation. Each block calls a helper method to obtain the given permutation for itself based on its own width and height. That permutation is the order in which the data will be written.
- The first block is reserved for writing the meta-data about the message (such as the length of the secret) and the other blocks are for writing the actual contents of the message.

```

global constant BLOCK_SIZE;

procedure embed_subblock(secret , subblock , random_engine)
  #Generate a permutation from 0 to subblock.width * subblock.height
  #using the random_engine given. That permutation will be the order
  #used when writing the secret data into the subblock data.
  writing_order ← random_permutation(0, subblock.width * subblock.height , random_engine);

  for each byte_index in writing_order do
    #Getting the absolute index of the subblock rows and
    #columns where we need to write the secret information.
    subblock_row ← subblock.starting_line_index + byte_index / subblock.width;
    subblock_column ← subblock.starting_column_index + byte_index % subblock.width;
    set_least_significant_bit(subblock.data[subblock_row][subblock_column], secret);

    #We move to the next bit of the secret information
    advance_to_next_secret_bit(secret);

procedure pseudo_scramble(cover , secret , password)
  #Creating a new pseudo-random engine with a given seed.
  random_engine ← new pseudo_random_engine(password);

  for each subblock of cover with subblock.size ≤ BLOCK_SIZE
    if subblock = cover.first_subblock
      #Used for hiding the size of the secret into
      #the first subblock of the cover in an order
      #given by the pseudo-random engine random_engine.
      embed_subblock(secret.size , subblock , random_engine);
    else
      #If it's not the first subblock of the cover,
      #write the actual secret into the subblock.
      embed_subblock(secret.iterator , subblock , random_engine);

```

Listing 3.1: Pseudocode of the scramble algorithm

It is much easier to explain the algorithm using a simple example, so let's begin with the image represented in figure 3.6. It is BMP image with a resolution of 10x6 pixels (10 pixels wide, 6 pixels tall). Furthermore, let's also create the parameters needed by the algorithm in order to embed a message:

- The secret message we want to hide in the cover file is "Hello World", no quotes.
- Given the aforementioned message, we can calculate its size: 5 characters for the word "Hello", 5 characters for "world" and 1 character for the space inbetween. Total message length is 11 characters or 11 bytes using the ASCII standard.
- The password used for generating the seed is "super_secret.key", no quotes.
- The BLOCK_SIZE used in splitting the original image is equal to 4.

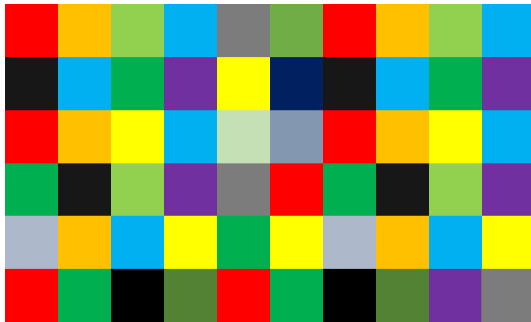


Figure 3.6: Original BMP cover image

Knowing all of this information we can already know if the cover file is going to be able to hold the secret message based on the formula 3.1. We know that the BMP format uses 3 bytes for storing each pixel and that our image is 10 pixels wide and 6 pixels tall, so we have that

$$CDS = 3 * 10 * 6 = 180 \text{ bytes} \xrightarrow{(3.1)} \\ \xrightarrow{(3.1)} MMS = \lceil 180/8 \rceil = 22 \text{ bytes}$$

Since our total message length is smaller than MMS , we know that we will not be running out of cover space during the embedding process. After making these verifications, we can begin by initializing our pseudo-random engine based on the given password meant to be used as a seed and we can also start splitting the original image into sub-blocks, ending up with a result similar to figure 3.7. Since neither the width or height of the image are multiples of the BLOCK_SIZE constant, we have several

smaller blocks (to be more precise, blocks 3, 4, 5 and 6) that are still going to be used for embedding purposes.

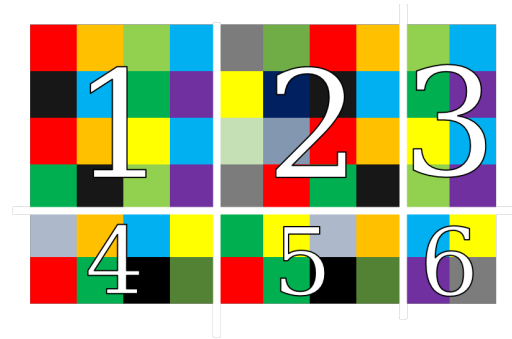


Figure 3.7: Sub-blocks of the original image

We can now begin the actual embedding process. From the pseudocode presented in listing 3.1 we see that the first step is to embed metadata about the secret message, more specifically its length represented as an unsigned integer on 32 bits. But before we can do that, we must ask the pseudo-random engine to generate a permutation between 0 and $subblock.width * subblock.height$, excluding the last value. For this example specifically, we know that

$$subblock.width * subblock.height = 4 * 4 = 16$$

and let's assume that the engine returns us the following permutation:

$$(5, 10, 12, 3, 0, 15, 4, 9, 14, 13, 8, 2, 7, 1, 6, 11)$$

With this order known and with the fact that each BMP pixel is represented on 3 bytes giving us 3 least significant bits for embedding purposes in mind, the process of embedding the message length (11 or 0x0000000B) into the first subblock goes as follows:

1. 5th pixel is the first one, all LSBs are set to 0.
2. 10th pixel, all 3 LSBs are set to 0.
3. 12th pixel, all 3 LSBs are set to 0.
4. 3rd pixel, all 3 LSBs are set to 0.
5. 0th pixel, all 3 LSBs are set to 0.
6. 15th pixel, all 3 LSBs are set to 0.
7. 4th pixel, all 3 LSBs are set to 0.
8. 9th pixel, all 3 LSBs are set to 0.
9. 14th pixel, all 3 LSBs are set to 0.

10. 13th pixel has the Blue channel LSB set to 0, Green channel LSB set to 1, Red channel LSB set to 0.
11. 8th pixel has the Blue channel LSB set to 1, Green channel LSB set to 1, Red channel is unchanged.
12. The rest of the pixels are unchanged.

A visual representation of the order based on the given permutation can be found in figure 3.8. We can also notice that we managed to embed 4 bytes of information into a simple block of 4x4 pixels, or 48 bytes of total data, and we still have 2 bytes of free space based on 3.1(one bit available in 8th pixel and 3 bits in pixels 2,7,1,6,11).

4	13	11	3
6	0	14	12
10	7	1	15
2	9	8	5

Figure 3.8: Order of writing into the first block

After embedding the metadata, we can begin hiding the actual message data into the subblock bytes. The sub-block size is 4*4 pixels total, which means 48 bytes in total space, resulting in exactly 6 bytes we will be able to write into this subblock (and every other block which uses 3 bytes to store a pixel and has 16 pixels in total). We start by converting our secret message in binary and we end up with something like this:

1. H = 01001000
2. e = 01100101
3. l = 01101100
4. l = 01101100
5. o = 01101111
6. (space) = 00100000
7. w = 01110111
8. o = 01101111

$$9. r = 01110010$$

$$10. l = 01101100$$

$$11. d = 01100100$$

By knowing we have 6 bytes available in the first sub-block we will be able to hide the string "Hello", which is impressive because it is already more than half of our total message in an image that is only 4 pixels wide and 4 pixels tall. Before starting the actual embedding process, we must again use the pseudo-random engine to generate a new permutation ranging from 0 to the total amount of pixels in the block. Again for the sake of our example, let's assume that we get this permutation:

$$(10, 4, 12, 6, 1, 15, 9, 3, 0, 8, 13, 5, 2, 14, 7, 11)$$

Using the binary conversion of our message, we begin by taking 3 bits each time from the binary stream and embedding them into each channel of a pixel in the order given by the permutation. We can see what bits we have written into which pixels in figure 3.9 (the first bit is the one written into the Blue channel of the pixel, the middle one is the Green channel and the last bit is encoded into the Red channel).

8 th 011	4 th 010	12 th 111	7 th 100
1 st 010	11 th 110	3 rd 110	14 th 100
9 th 011	6 th 101	0 th 010	15 th 000
2 nd 000	10 th 000	13 th 100	5 th 101

Figure 3.9: Order of writing the actual message into the second block

In the case of the third block the situation is slightly different because the width of the block is not equal to BLOCK_SIZE but this change does not change the behaviour of the algorithm at all. In this case we have a block that is 2 pixels wide and 4 pixels tall, ending up with a total of total 24 bytes needed for storage that can accommodate 3 bytes of secret information, or in our case the letters 'w', 'o' and

'r'. In this case we generate a permutation from 0 to 8, excluding the last value:

(3, 6, 0, 1, 4, 7, 2, 5)

By going through the same process as with the previous block we get the result that can be seen in figure 3.10. This leaves us with the target of hiding only two more characters: 'l' and 'd' in block number 4 which is identical to block 3 in size but was rotated by 90 degrees.

2 nd 110	3 rd 110
6 th 110	0 th 011
4 th 111	7 th 010
1 st 101	5 th 101

Figure 3.10: Order of writing into the third block

For the last time we generate a permutation using the engine in the same interval as above and we obtain:

(5, 3, 0, 7, 4, 2, 6, 1)

And by going again through the steps described above we manage to hide the last two remaining characters and we still have a byte free in the sub-block. The remaining blocks of the image remain unchanged and theoretically could be used for hiding other messages, but there are a few issues that can arise with this, the main one being message separation and identification, how each message is divided etc.

2 nd 000		5 th 0__	1 st 011
4 th 010	0 th 011		3 rd 110

Figure 3.11: Writing the actual message into the fourth block

After the algorithm finishes and the modified cover image is saved, there is absolutely no difference to the human eye between the two pictures.

This is the power of Least Significant Bit insertion when using digital images as the carrier format. The only difference between the two files is at a bit level, making it one of the safest and most covert ways of sending secrets over an untrusted environment.

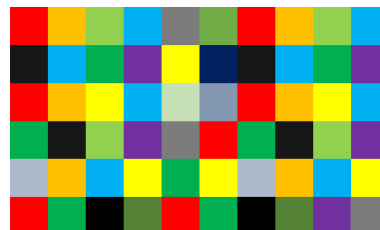


Figure 3.12: The original image

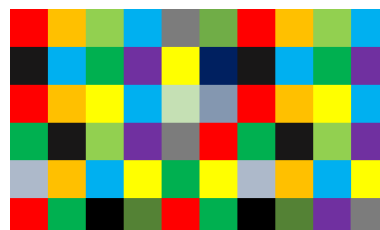


Figure 3.13: The altered image containing the message "Hello world"

Like any other steganography algorithm, this method also has advantages and disadvantages. The main benefits of this algorithm are:

- **Security.** Choosing a BLOCK_SIZE of only 8, each normal sized block will have a total of 64 pixels and there would be $64! = 1.2688693e + 89$ ways available (just for a single block) for the algorithm to write the secret information. Given the fact that each block has its own permutation generated specifically for it based on a pseudo-random engine makes it very hard for any intruders to try and retrieve the secret message without having access to the key. Increasing the size of the BLOCK_SIZE only strengthens the overall security of the method while still keeping the same message capacity.
- **Efficiency.** The algorithm is extremely fast because it performs very few demanding operations and it is taking advantage of bit-wise operations. Furthermore, there is also the option of adding parallelization because there are no conflicts whatsoever between the parties involved, thus ending in an even more efficiency

increase for the entire operation. There could be a small issue regarding the generation of the permutations based on a key in a multi-threaded environment because it may be prone to some implementation language issues with the pseudo-random engine.

However there are quite a few issues with this algorithm, issues that can render the method useless and make it obsolete in a faster than normal timeframe:

- **No data redundancy.** There is absolutely no mechanism in place in order to prevent the loss of data. Most communication environments nowadays usually compress the files before sending them over the wire and that compression may be lossless, but in most cases it is lossy. And even by sending the file in a way that it will not be compressed, there is also the slight change of altering and a small change in a single bit can and it will make the whole secret message corrupted without any method of recovery.
- **Detection via pattern identification.** Working only within small sub-blocks of BLOCK_SIZE means that we also limit the attack surface of any outside parties and allow them to focus on finding any details that can help them identify the key that was used when encoding the secret. For example, it is possible that an attacker will want to focus on the second block of the cover file and try to search for common extensions in the secret embedded file headers. If the intruder finds there is an order to the bytes of the block which produce that header that means that he is much closer to identifying the seed of the pseudo-random engine because he knows the second permutation generated by that seed and based on that information he may be able to deduct further permutations.
- **Limited market.** This algorithm was designed with file formats that are lossless, i.e. bitmaps that store the entire information of the image. While theoretically it could be used for PNGs as well, we will see in later chapters that PNG uses a mechanism called interlacing which makes it harder to work or even identify the sub-blocks of the image. Most modern online platforms have also moved away from BMP since they are far too big in size and the same image quality could be achieved by using other formats that have a much much smaller

size, ending up in almost making the entire BMP format obsolete.

In the end, it is important to note that similar work has been done by a few researchers, the closest one being the work done by Hussein Al-Bahadili[1] in his paper where he chose to focus on scrambling the contents of the secret message using a similar password and seed generation technique before writing it to the carrier file. But while the 2 methods are similar in their goal, the way they reach that goal are different.

3.3 Portable Network Graphics (PNG)

Chapter 4

Audio file formats and steganography techniques

4.1 Introduction

4.2 Additional techniques used in audio steganography

4.2.1 Embedding within certain frequencies

4.3 The MPEG-1/2 Audio Layer III (MP3)

4.4 Waveform Audio (WAV)

Chapter 5

The Steganos Project

Steganos is the name of the application that implements the algorithms enumerated in the earlier chapters of this paper and is the direct result of the work done by the authors. In this chapter I will present what modern technologies and frameworks went into creating the application, how it is structured from an Object Oriented point of view, how fast it is and how I hope it will expand into the future.

5.1 Used technologies

5.1.1 C++

C++ is one of the lowest high-level computer programming languages. Designed by Bjarne Stroustrup, it first appeared in 1985 as a variation of one of the most popular languages at the time, C. It is one of the most efficient modern languages mainly because it has been designed with performance and flexibility in mind, just like its predecessor. C++ has gained a lot of traction from big companies like Intel and Microsoft which needed a programming language that could be used for operations ranging from basic kernel functions to highly specialized Object-Oriented projects with Graphical User Interfaces[2].

Since its conception, C++ has grown substantially by adding support for generic and functional features to ease the development processes and getting standardized by the International Organization for Standardization probably helped as well because it meant no more obscure variations of the language, allowing programmers to follow only one standard, ending up with even more portability and stability of the applications.

In the modern day, it is used almost everywhere: the kernel of various operating systems, the transaction software used by banks, drones and airplanes,

embedded systems such as the Arduino or Raspberry Pi, and now in the Steganos Project as well under the latest approved standard of the language, C++17.

C++ inherited from C the file types: headers and sources. The header files (the files that have a .h or .hpp extension) are where the standard recommends to store the class declarations, function prototypes, constants declarations, no definitions should take place in a header file. There are a few exceptions to this rule, the most common one being a rule that states that all templated functions and functions are to be declared and defined in a header file otherwise it will not work properly when dealing with multiple instances of different types. In the case of the source files (the files that have the .c or .cpp extension) the standard suggests to only be used for the definition of the class methods or other general functions. Following the standard results most of the time in a clean and well defined separation in the code, allowing for high cohesion and low coupling in all projects built using C++.

The reason for choosing C++ as the language for the Steganos project is simple: it allows for the programmer to work on the raw bytes of files in an extremely easy way, reading and parsing them, bitwise operations and writing to file, all the common low-level operations that are highly valued when working in the steganography field. But the high level aspects of the language also permit for dealing with complex tasks, such as modern cryptography algorithms applied to robust byte streams or holding all the information in different data structures.

5.1.2 CMake

CMake is a cross-platform open-source tool designed for managing the build process of software based on the C++ programming language. It has been

created in the year 2000 and ever since then it stayed compiler-independent using simple configuration files that generate the adequate makefiles to be used in the users environment while building the target project[3].

CMake uses files called CMakeLists.txt that contain the commands to be used by the internals of the tool in the building process. It is required that one file is in the root of the project before running the CMake process, with the possibility of adding a .txt file in the subdirectories in order to indicate special cases that require a different approach.

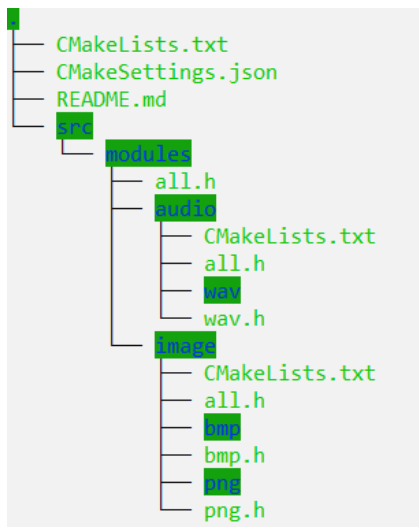


Figure 5.1: Folder structure of a project using CMake

Each command in CMake has the same format: `COMMAND (args..)`. Using this format, users are able to build even the most complex software projects in the form of simple executables, dynamic or static linked libraries, etc. Steganos uses CMake because it is an extremely effective tool in the building process and it allows for separating the logic of the project into distinct modules i.e. the audio module, the image module, the general usage module, and linking them in the end into a simple executable. Most projects use only a small subset of the commands available in CMake, the most common being:

- **CMAKE_MINIMUM_REQUIRED** is used to mark the minimum version of CMake that is required to be installed on a system in order to build the project.
- **SET** is used to assign a value to a CMake variable that is used while building, similar to environment variables found on all operating systems.

- **PROJECT** for naming the project, important step in active Continuous Integration and Continuous Development environments.
- **INCLUDE_DIRECTORIES** for marking the directories containing the header files in order for the compiler to be able to link the source files and header files.
- **ADD_EXECUTABLE** for creating an executable after build the project from the source files given as arguments.
- **ADD_LIBRARY** for creating a library or module with the given source files.
- **TARGET_LINK_LIBRARIES** for linking (pre)defined modules or executables between eachother.

5.1.3 CXXOpts

CXXOpts is an open-source C++ library that is meant to be a lightweight command line option parser[4]. It is meant as the C++11 and beyond alternative to other libraries such as Commons CLI for Java or Argparse for Python. It was initially created by user jarro2783 on Github and nowadays is actively developed by the community using the Git commit and pull request system. CXXOpts is made to replicate the handling of the help argument and the merging of multiple parameters commonly found in *NIX command line binaries, without using any additional dependencies in a header-only file.

5.1.4 Lodepng

Lodepng is an open source C++ library developed by Lode Vandevenne used for image processing for pictures stored under the PNG format [5]. It is very useful for decoding the image data before beginning the steganography process, making it easy to modify the data and to encode it back into a PNG file that follows the standard format. Lodepng works on every version of C++, contains only two files(a source file and a header file) and is rated to be one of the fastest libraries for PNG image processing. Steganos uses Lodepng to parse PNG files and to obtain the image data byte stream from the zlib compressed stream in order to be able to work with the implemented steganographic algorithms.

- 5.1.5 MMSSTV Engine for Windows
- 5.1.6 Robot36 for *NIX based systems
- 5.2 Application architecture
- 5.3 Benchmarks
- 5.4 Further work

Chapter 6

Conclusion

fasfadh

Bibliography

- [1] H. Al-Bahadili. A secure block permutation image steganography algorithm. *International Journal on Cryptography and Information Security*, 3:11–122, 09 2013.
- [2] Bjarne Stroustrup. *The C programming language*. Addison-Wesley, 2018.
- [3] Cmake documentation.
- [4] jarro2783. jarro2783/cxxopts, Feb 2020.
- [5] Lvandeve. lvandeve/lodepng, Mar 2020.