March 2020

VARIABLE VESSEL CAPACITY IN STEGANOGRAPHY OF UNSTRUCTURED DATA

Alex Zverev

VARIABLE VESSEL CAPACITY IN STEGANOGRAPHY OF UNSTRUCTURED DATA

AUTHORS:
Alex Zverev

ABSTRACT

Techniques are described herein for switching between different bases in the numeral system to allow adjustment of the capacity of a vessel file in digital steganography. If the base is low, the change is indistinguishable, while the storage for the hidden payload is minimal. If the base is high, more data may be hidden in the digital vessel, but the change is more noticeable.

DETAILED DESCRIPTION

Steganography is an approach to embedding information into nondescript pieces of information, such as text, digital images, and other multimedia. Whereas cryptography hides the meaning of information, steganography hides the fact that information even exists and is being transmitted. Steganography has existed for centuries, and the modern digital world and technology provide more opportunities for its evolution. Data is already transmitted between government agencies and corporations in a hidden format, but there are still a multitude of problems that require resolution. Historically, the main goal of steganography is to conceal the existence of information. The digital world demands hidden transmission of large volumes of data, including multimedia.

Figure 1 below illustrates an example flow of a steganographic method.

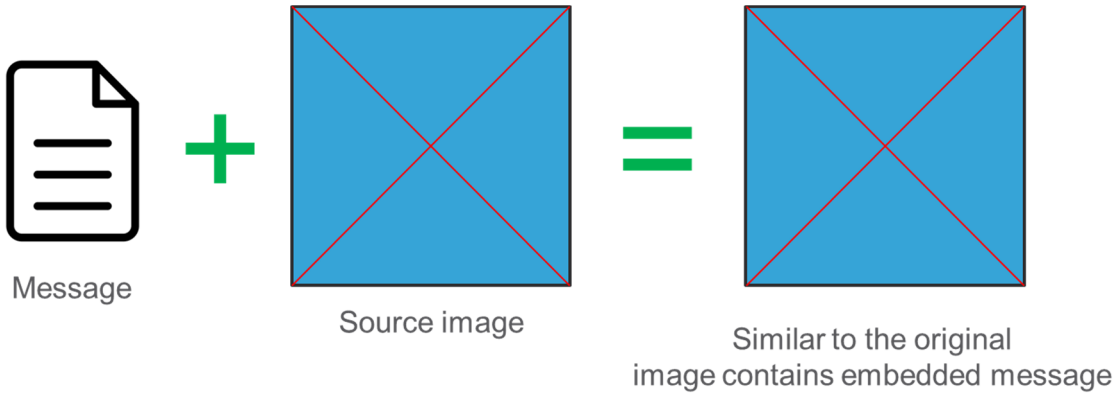

Figure 1

Published by Technical Disclosure Commons, 2020

A vessel is a file that is used to embed a payload thereinto. A vessel can be a digital image, an audio or video file, or anything else that is not severely affected by digital alterations in its content. The payload is a digital message that is inserted (embedded) into the vessel in such a way that a random observer cannot discover the content of the payload, or the fact that the payload was introduced. A payload can be represented by any digital entity, such as text, image, video, audio file, executable file, etc. A slot is a value extracted from the original vessel container. This can be a color channel value in a pixel in a digital image, or a sound wave configuration in an audio file. The slot is normally altered during the operation of injection (or embedding) the payload. The slot value is an integer, and sits in a specific range defined by the standards. For illustrative purposes, digital images are used as an example herein, although the concept may be extrapolated to other types of digital vessels.

As illustrated in Figure 2 below, in an additive color model, several color channels constitute a pixel: Red, Green, and Blue (RGB). Each color is a number. The maximum limit depends on the color depth level. TrueColor is the most common and includes ranges from 0 to 255 (most common), but other ranges are possible. For example, DeepColor includes ranges from 0 to 65536.

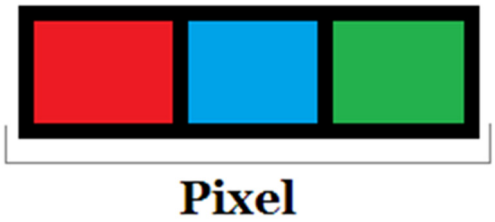

Figure 2

Existing steganography methods for digital vessels typically rely on binary operations, which means that they represent information in 0's and 1's, and all operations are designed to change only one bit of information in order to embed a payload into a vessel. Existing methods assume the vessel's capacity is a static value and do not have an easy way to change it. Such methods are generally interested in the arrangement of the affected bits in order to conceal alteration to the vessel. Thus, there is a tradeoff between the amount of embedded data and the ease of detectability of the alterations.

Techniques are described herein for switching between different bases in a numeral system to allow for adjustment of the capacity of the vessel. First, the base of the positional numeral system is chosen. Almost any positional numeral system can be used (e.g., binary, ternary, decimal, etc.) to encode the payload. The higher the base of the numeral system, the higher the variance rate, the more artifacts may be introduced to the vessel, and the greater the chance of discovery that the image was altered. A higher base corresponds to more carried information. Conversely, the lower the base of the numeral system, the less visual perception is impacted. In particular, the binary and ternary bases are acceptable, but the octal base (base 8) does not significantly visually affect the image, and carries more data in a single pixel than binary.

For every base-N numeral system, the variance will never exceed floor(N/2), except for minimum (e.g., 0) and maximum (e.g., 255) values, in which case it would be N-1 or less. Because floor(N/2) is the maximum variance in most cases, an odd base (e.g., 3, 5, 7, 9, 11, etc.) can carry more data than an even base (e.g., 2, 4, 6, 8, 10, etc.) without introducing many artifacts. As such, the choice of an odd numeral system may be better than an even numeral system. Additional image analysis may be required. Also, if an optimization technique is used, it is possible to use higher bases with little detectability and much higher capacity. Ultimately, the choice of the positional numeral system represents a compromise between payload capacity and ease of intervention detection.

Second, the payload is encoded in this base. The third step may involve extracting as many slots from the vessel as the number of characters in the payload. The more characters in the payload, the more slots will be required. However, if the same payload is encoded into a higher base, it is likely to take less slots, though this will lead to higher variance. Fourth, the modulo (base) operation is applied to each slot value, and the results are recorded.

Fifth, the slots are altered. This may include determining a new slot value that would replace the old slot value in the most efficient way. Two possible numbers may be found: D_{left} and D_{right}. In order to do this, the difference must be calculated. This is an absolute value of the subtraction of the current payload character from the current slot value. If D_{left} or D_{right} are outside of the permitted range, then the other one is the new slot value. This is a rare case, and both are usually inside the permitted range. The modulo base

operation is applied to both of these numbers. Only one of the operation results may match the current payload character. The matching result is the new slot value. This operation may be applied to all slots until they are replaced with the new values.

The following example will help illustrate the techniques described herein. First, the base of the positional numeral system is chosen as 3. Second, the payload "2 1 0 2 2 1" is encoded in this base. Third, as illustrated in Figure 3 below, because there are six characters in the payload, six color channel values (two pixels with three RGB channels each) are extracted from the vessel.

23	50	41	99	250	2

Figure 3

Fourth, as illustrated in Figure 4 below, the modulo (base) operation is applied to each slot. Specifically, because 3 is the base of the chosen numeral system, the value of each extracted color channel value is extracted and divided by 3 to determine the remainder.

23	50	41	99	250	2
		modulo 3			
2	2	2	0	1	2

Figure 4

Fifth, the slots are altered by comparing the payload and the result of the modulo operation. As illustrated in Figure 5 below, the payload character equals the respective remainder value, so no change is required. Otherwise, the color value of the closest result is changed, and it is ensured that the modulo-N operation would yield the payload character. N is the base of the numeral system (e.g., 2 for binary, 8 for octal, etc.), which in this case is 3.

Slots	23	50	41	99	250	2
			modulo 3			
Remainder	2	2	2	0	1	2
Original payload	**2**	**1**	**0**	**2**	**2**	**1**
Action	No action, 2 = **2**	49 mod 3 = **1** 52 mod 3 = **1** 49 is closest to 50	42 mod 3 = **0** 39 mod 3 = **0** 42 is closest to 41	98 mod 3 = **2** 101 mod 3 = **2** 98 is closest to 99	251 mod 3 = **2** 248 mod 3 = **2** 251 is closest to 250	1 mod 3 = **1** 4 mod 3 = **1** 1 is closest to 2

Figure 5

As illustrated in Figure 6 below, the new slot values are obtained and need to be replaced in the vessel. This may be used to generate a new image with the embedded payload.

Slots	23	50	41	99	250	2
New values	23	49	42	98	251	1
Difference	0	1	1	1	1	1

Figure 6

As illustrated in Figure 7 below, in order to decode the payload and extract the original payload from the vessel, the new slot values need to be modified by the base. As shown, the extracted payload matches the original payload.

Slot with embedded data	23	49	42	98	251	1
			modulo 3			
Extracted payload	2	1	0	2	2	1

Figure 7

Techniques described herein challenge the static capacity of digital vessels (e.g., multimedia files such as video, voice, image, etc.) as well as the usage of binary representation in digital steganography. These techniques offer the possibility of altering every bit in sequence/combination. Thus, more data may be carried in a single digital vessel. There are also opportunities for integration with other optimization methods and algorithms to further improve efficiency and increase capacity. These techniques may allow any lossless digital image (e.g., Portable Network Graphics (PNG), Bitmap (BMP), Tagged Image File Format (TIFF), etc.) to carry an arbitrary digital message while storing as much information as possible. The intended recipient, and only that recipient, may know that the image contains information and understand how to read it.

In summary, techniques are described herein for switching between different bases in the numeral system to allow adjustment of the capacity of a vessel file in digital steganography. If the base is low, the change is indistinguishable, while the storage for the hidden payload is minimal. If the base is high, more data may be hidden in the digital vessel, but the change is more noticeable.