Hiding Information in a Picture File: a System Model with Experimental Design

Jakub Siłka[a]

[a]Faculty of Applied Mathematics, Silesian University of Technology Kaszubska 23, 44-100 Gliwice, Poland

Abstract

The format of information is changing with the developments of computer methods and formats. Graphical information can be also used to transfer text. In this paper, I am going to describe the new approach via merged text implemented directly to the image by using alpha channel of the pictures. This kind of encryption can be also used as the opportunity to spread script guidelines, which subsequently enable assuming control of entire computer. The paper presents a discussion and experimental set up of the designed solution.

Keywords

Picture, hiding, Data, Invigilation, Instruction

1. Introduction

Nowadays information processing is possible in various different levels. We can find many systems which proceed information from users to get the knowledge about several aspects. One of the most popular information format is an image. We can have photos from holidays, work, travel or many other occasions. This type of information is easy to read and possible to use in various devices. From images we can have information about objects visible there by analyzing pixels of the image or simply all color channels. In [1] was presented how pixels can formulate shapes of lung diseases for estimation by artificial intelligence. In [2] was discussed that pixels from voice spectra can be recognized as image segments centroids for use verification processes, while [3] presented that comparing colour aspects of pixels from microscopy images will help on detection of bacteria.

Other field of working with the information hidden in images is steganography. This field of computer science is oriented on developments of algorithms for transferring some hidden information in images. In [4] was discussed how permutation on pixels operations can improve security of transferred information. In [5] was given a wide discussion on trends and recent advances in steganography. In [6] a discussion on these innovative aspects was moved to the domain of coverless images, while in [7] the opposite of cover selection was presented. There are many ways to use images as carriers of information, also text which can be visible to computer systems. This possibility gives many ways to use it also in bad way, ie. when the text is a code which can be a virus.

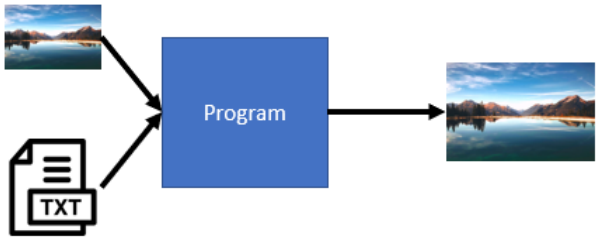

Figure 1: Sample merge scheme when the text code is simply inserted into the image by third program to compose an output file.

This paper presents a system model which can use graphical file as information transmission, both in good and bad way. The idea presented in this paper is to use an alpha channel, which is responsible for the resolution level - the difference between the value of 255 and 254 is imperceptible without special program. The HD picture contains 921600 pixels (1280x720), so if we use all of them we get as many as 112,5 kB place to gather data. Because of that, there is a broad scope of opportunity to implement variety of scripts there. If the program is encoded properly, it will host instructions and send them out with coming pictures. The model presented in this paper shows how to use alpha channel for information buffer. The system is composed to use an input image, merge it with text and forward to second part which decomposes it. In the model are discussed different aspects filtering the image to adjust information in the channel [8, 9].

IVUS 2020: Information Society and University Studies, 23 April 2020, KTU Santaka Valley, Kaunas, Lithuania

kubasilka@gmail.com (J. Siłka)

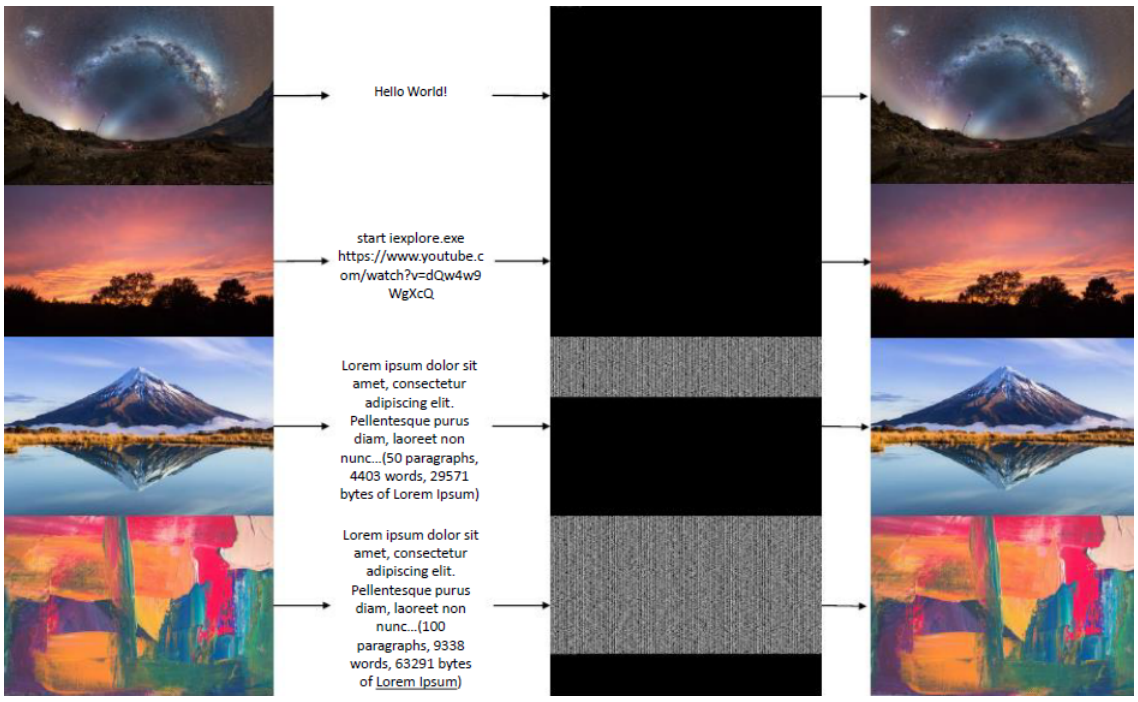

Figure 2: On the left side we can see photos before adding coded message (A) - white pixels stand for the value 254 instead of 255. Below is displayed the message (B), its appearance coded in alpha channel (C) and image after adding the last, modified layer (D).

2. Proposed data processing

Now we can discuss how the idea of code encryption into the graphic files works in practice. The system composed for the research has an experimental set up which is described below.

Transmitter Transmitter is the program that codes guidelines for the receiver, downloads picture and links text file from proper folders and checks whether the pictures have correct format. If not, the program would turn it into the demanded one. Sample scheme is visible in Fig. 1. Afterwards, the predefined statement is encoded, whereby program has already determined format and ending of the instruction. Therefore it is not necessary for the receiver to analyse entire picture to indicate the guideline.

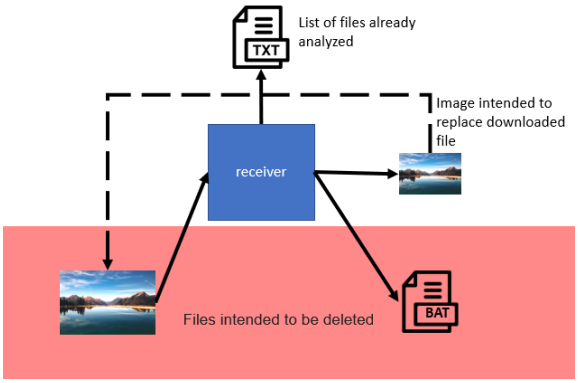

Figure 3: Sample decoding scheme from the receiver side, where the code is reformatted in the file and verified by the program.

Receiver The program is receiving instructions, first checks if the folder name is “downloaded”. Then the history of files is constructed with proper format in order to prevent conducting the same instruction. The system script is getting overwritten by meaningless writing and consecutively deleted, so it would not be possible to regain it. After carrying the instructions out the program overwrites the picture by the new one, which does not contain any guidelines. Sample scheme is visible in Fig. 3. Of course, it is possible to adjust the program in a way that enables it to turn itself from receiver into the transmitter and to encode new instructions for every file with proper format. This type of the structure is also often used in viruses since it can infect solely one computer in the inner network, because it will spread virus to each system that re-

Figure 4: Attached is the picture, in which the original photo is displayed on the left,the determined quantity of bites that were cut off, starting from A) 6 bites, B) 5 next bites, consecutively in C and D are presented on the right.

ceives graphical information from attacked computer, and thus the whole network can be infected easily, at the short period of time.

The system result from input to the output is presented in Fig. 2. On the entire process an information is merged with the initial input to compose a final output. On the way an alpha channel is used to fit within the text format information.

2.1. Message Encoding

In regard to restricted transcript place, it benefits to use certain an approach for data compression. In program, for instance, the Shannon-Fano coding is used through its easy implementation and satisfying level of compression. The Shannon-Fano coding is a type of lossless compression - it finds prefix code for each discreet source.

Example.

a) S={a,b,c,d}

b) p={0.6,0.2,0.15,0.05}

For the sequence a) which corresponds to the probability, i.e. the number of occurrence in the text is coded to the number of all digits b). The situation is visible in Fig. 5. The program is checking itself whether the implementation if dictionary at the beginning of coding would take less time than the message. Thereby, the program optimally exploits place in picture.

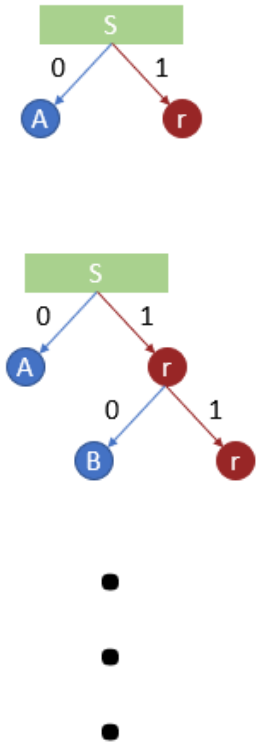

Figure 5: On the left is mark a coded as 0. On the right is mark b coded as 1-0.

2.2. Alternative Use

In regard of increasing surveillance and extended value of high computer performance, casual ways of information protection are becoming steadily unassailable for regular computer user. The real intent of a message can be therefore easily hidden due to innovative method. Let us now think how to use the above system for this. The first pixels of a graphic are changed into the desirable file-format, which entails that the

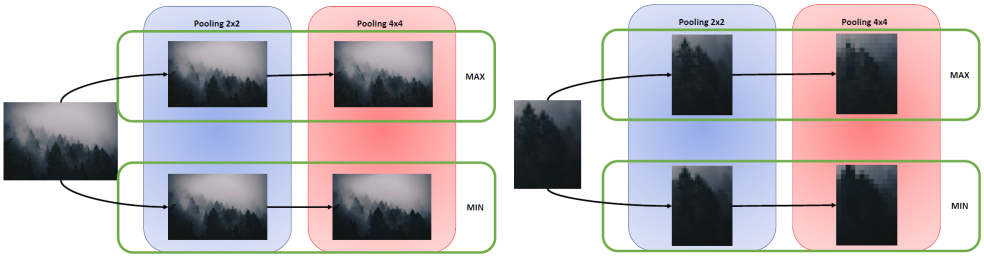

Figure 6: Preview of polling picture on the left and version where one part of the picture is magnified for better view on the right.

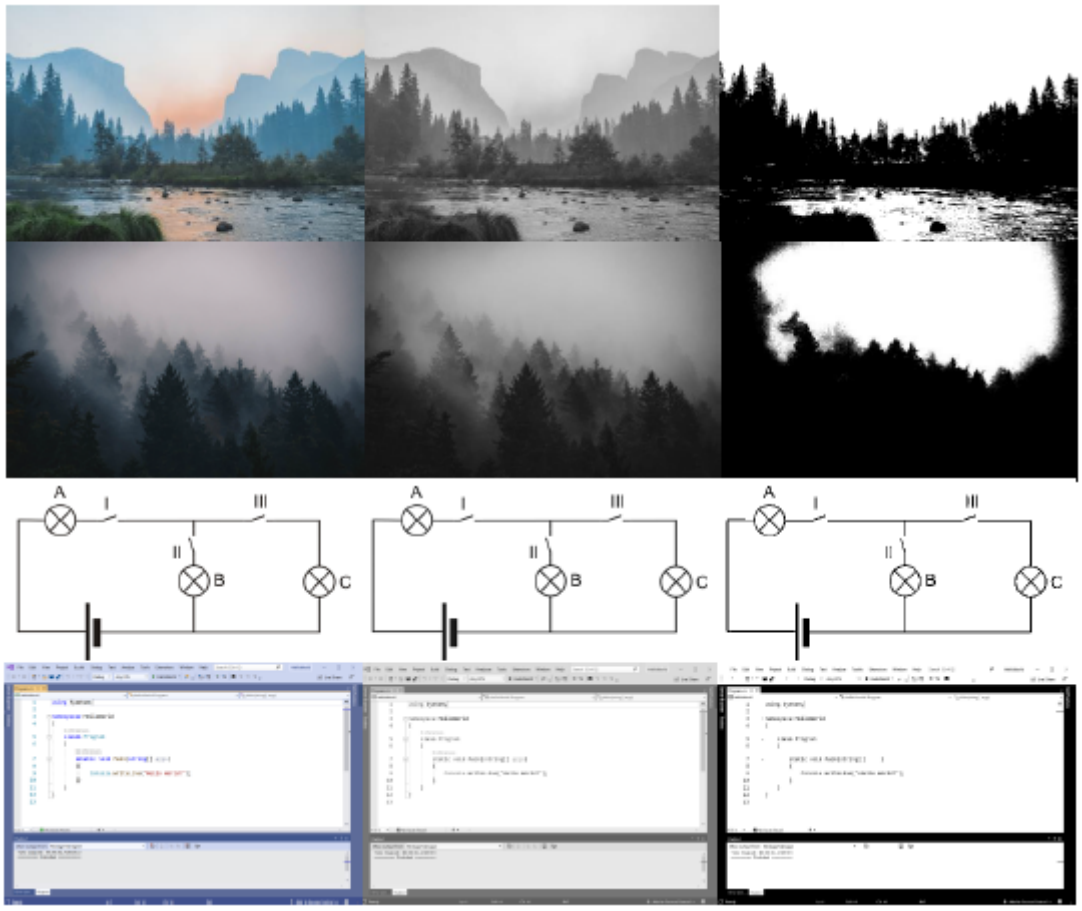

Figure 7: Above on, the accuracy of projecting the highest compression of picture is presented. Left photo is an original source (21 bites = pixel), whereas the next ones show higher compression: 7 bites and 1 bite consecutively.

receiver itself can on an going basis decode messages conveyed by its download. The same approach can be applied to text files. To enable it, the program firstly changes given file into binary system pattern. The scheme requires to use adequate amount of pictures to code the message. The receiver, after getting an information turns it into the desirable format.

2.3. Composed Model of Image Data Encoding

The picture itself contains much more information than simple text, so one should label which starting format is expected. There are three options, hence, it is necessary to decrease the amount of data in the picture.

a) Colours accuracy

Figure 8: Picture shows how the lack of colour changes original file, from left is RGB, RG, GB, RB.

b) Less accuracy of colours projection

c) Amount of colours

The color accuracy relies on the differences between particular colors. It means that value assigned to color does not belong already to the interval (0,255), but instead is one of the lower power of 2, determined by the user. Thereby, once the graphics is decoded, the reduction of pixels will go ahead, which is formed from the formula

$$r = \log_2 Max \tag{1}$$

The interval size is a power of 2, due to the writing ongoing in binary form, so that is is possible to use the whole length of bites

$$f(x) = x * 2^{8-r} \tag{2}$$

Whereas x is value of the pixel and r is square root of the interval size. Sample results from pixels encoding is presented in Fig. 4. In order to not complicate both, coder and decoder, the transition takes place in a distinct program, which also allows the independent action of a program. It is worth stressing, that the coder is adjusted to binary data even though the pixel has spectrum 256 and still operates at maximum values. The difference must be as little as it is possible due to security matter - indeed, once somebody knows the communication pattern, the entire scheme is not adequate anymore.

The precision of colors projection relies on the simplification of the graphics by using polling method. The picture is converted as scantily as possible due to high loss of the details. The maximum polling is used, the blurs phenomena takes place, and thereby the picture loses its sharp edges - and ultimately, everything is mixed together.

In opposite, using the minimum polling reflects in the enhancing the image noises, whereby the transparency undergoes decrease. Thus, is is highly significant to adjust properly polling to picture. Sample schemes of both ways is visible in Fig. 6, while the resulting quality of processing is visible in Fig. 7.

The amount of colours is crucial through each new one is adding another dimension to the picture, that has been already scaled-down. Thereby quantity of photos being required for sending solely one photo is greatly enlarged, i.e. it is possible to establish diversified options of recreating the colour either by using the RGB's values or in the Grayscale, which would save the place. The changes of colour channels for the input image are visible in Fig. 8.

3. Conclusions

There are plenty of risks that occur while one is using an internet, hence, we do not want our private information to get into others control. That is why, the developed scheme for quiet conveying instructions for other computer or sending the graphics and text messages is an important to be considered in common information-protection manners. Moreover, the paper points out the possible, sensible protection of antivirus systems. It is important to notice that the sending graphics process is problematic action, however,

under certain circumstances it seems to be only available approach for sending sensible information-media graphics, for instance under high censorship conditions. The idea will be continuously developed toward optimal encoding. I do believe it is the most optimal approach in case of protecting the data.

References

[1] G. Capizzi, G. L. Sciuto, C. Napoli, D. Polap, M. Woźniak, Small lung nodules detection based on fuzzy-logic and probabilistic neural network with bio-inspired reinforcement learning, IEEE Transactions on Fuzzy Systems (2019).

[2] D. Połap, M. Woźniak, R. Damaševičius, R. Maskeliūnas, Bio-inspired voice evaluation mechanism, Applied Soft Computing 80 (2019) 342–357.

[3] M. Woźniak, D. Połap, L. Kośmider, T. Cłapa, Automated fluorescence microscopy image analysis of pseudomonas aeruginosa bacteria in alive and dead stadium, Engineering Applications of Artificial Intelligence 67 (2018) 100–110.

[4] Y. Wang, L. Kong, Z. Qian, G. Feng, X. Zhang, J. Zheng, Breaking permutation-based mesh steganography and security improvement, IEEE Access 7 (2019) 183300–183310.

[5] I. J. Kadhim, P. Premaratne, P. J. Vial, B. Halloran, Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research, Neurocomputing 335 (2019) 299–326.

[6] J. Qin, Y. Luo, X. Xiang, Y. Tan, H. Huang, Coverless image steganography: A survey, IEEE Access 7 (2019) 171372–171394.

[7] Z. Wang, X. Zhang, Secure cover selection for steganography, IEEE Access 7 (2019) 57857–57867.

[8] F. Bonanno, G. Capizzi, G. L. Sciuto, C. Napoli, Wavelet recurrent neural network with semi-parametric input data preprocessing for micro-wind power forecasting in integrated generation systems, in: 2015 International Conference on Clean Electrical Power (ICCEP), IEEE, 2015, pp. 602–609.

[9] G. Capizzi, S. Coco, G. Sciuto, C. Napoli, A new iterative fir filter design approach using a gaussian approximation, IEEE Signal Processing Letters 25 (2018) 1615–1619.