EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 7/ October 2015

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

A Novel Technique of Image Steganography for sensor information with socket TCP/IP connection

AHMED FAHEM ALBAGHDADI
Almustaqbal University College
Babylon, Iraq

Abstract:

Steganography is the art of hiding information in other information in order to hiding the fact that communication is taking place. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. There are different types of steganography but images are the most popular because of their frequency on the Internet. In this paper a novel way of image steganography is applied to embed information in colors of pixels and alpha (ARGB) using python language in four steps. First step include change all alpha that have 254 in byte to 255 in ARGB pixels. The second step include convert all information to bytes. Third step include select distributed pixels from image in suitable ratio depend on size of image in order to put information in it. Fourth step include put first byte of information instead of byte of blue color and make byte of alpha as 254. The result image is encrypted using base64 encoding techniques in order to send it using proposed TCP/IP socket between Python language and VB.NET language or any other way. The receiver represented by VB.NET program makes same steps in reverse arrangement for extract information. Python language is used in order use in raspberry pi platform to hide information of important sensors.

Key words: Steganography, TCP/IP Python, raspberry pi, Hide information, Sensor information.

1- INTRODUCTION

Due to the large use of internet, it is necessary to develop the security of information by proportional manner with widespread. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to save the message. Unfortunately it is sometimes not enough to keep the message secret, it may also be necessary to keep the existence of the message secret. This technique called steganography. Steganography is the science of invisible communication. This is implemented through hiding information in other information, thus hiding the existence of the communication. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [1]. In digital image steganography the data is hidden exclusively in images. The idea of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histories, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message [2]. there is a different between Steganography and cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [3]. Cryptography and Steganography are both ways to protect information of message from unwanted parties. Network socket is an endpoint of an inter process communication across a computer network of between programing electronic devices. A socket address is the combination of a port number and IP address; much like one end of a telephone connection is the combination of a phone number and a particular extension. Based on this address, internet sockets deliver incoming data packets to the appropriate application process.

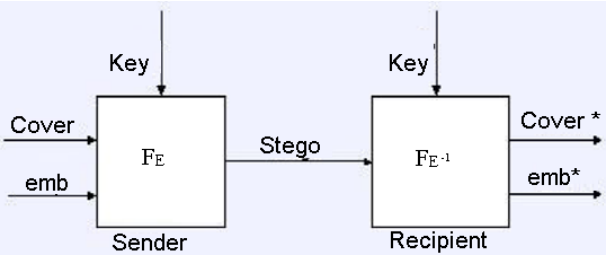

Figure 1 Graphical Version of the Steganographic System

fE : steganographic function "embedding"
fE^{-1} : steganographic function "extracting"
cover: cover data in which *emb* will be hidden
emb: message to be hidden
stego: cover data with the hidden message

2- STEGANOGRAPHY CONCEPTS

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem proposed by Simmons [4], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [5].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [6].

3- DIFFERENT KINDS OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the most suitable formula are those with a many redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [7]. The redundant bits of an object are those bits that can be used for steganography [6].audio and Image files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 2 shows the four main categories of file formats that can be used for steganography.

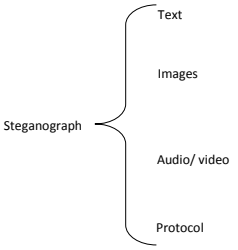

Figure 2: Kind of steganography

In past hiding information in text is most popular method of steganography. An obvious method was to hide a secret message in every nth letter of every word of a text message. Text steganography using digital files is not used very often since text files have a very small amount of redundant data. It is only since the beginning of the Image steganography Protocol [1]. Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital image, digital images are the most popular cover objects for steganography.

This paper will focus on hiding information in images and how to use it practically to hide sensor information.

4- IMAGE DEFINITION

To a computer, an image is a collection of numbers that constitute different light intensities and different colors in different areas of the image [8]. This form is a grid of individual points, referred to as pixels.

Most images on the Internet consist of a rectangular map of the image's pixels. Each pixel has location and its color [9]. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel [16]. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel [10]. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits [8]. Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colors [10].

When working with larger images of greater bit depth, the images be too large to transmit over an Internet. In order to display an image in a reasonable amount of time, Image size must reduce. These techniques make use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. This process called compression [9].

5- USES OF STEGANOGRAPHY

- Steganography can be a solution which makes it possible to send news and information without fear of the messages being intercepted and traced back to us.
- It is also possible use steganography to store information on a location. For example, some military secrets can be stored in a cover source. When we are required to unhide the secret information, we can easily reveal our banking

data and it will be impossible to prove the existence of the military secrets inside.

- Paired with existing communication methods, steganography can be used make hidden exchanges like Governments communications: those that support national security. Digital steganography provides vast potential. Businesses may have similar concerns regarding trade secrets or new product information.
- Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

6- PROPOSED SYSTEM

The most important purpose of this proposed system is to increase the security of an important information come from sensors especially that deal with health care like ECG sensor and a lot of other sensors we want to keep its information hidden. Figure 3 illustrates the main Idea of the proposed system.

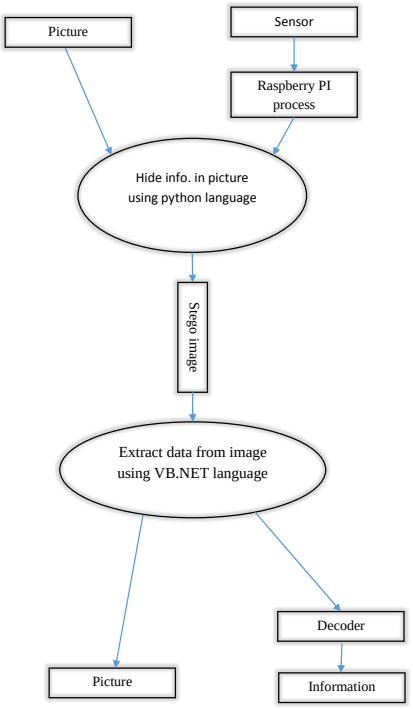

Figure3. Proposed system

I will describe each main part of this proposed system alone in order to provide good understanding of how the system exactly operates.

1. Raspberry PI

The Raspberry Pi shown in figure 4 is a low cost, credit-card sized board that plugs into a TV or computer monitor, and uses a keyboard and mouse. It is a capable little device that enables people of all ages to learn how to program in language like Python. It's capable of doing everything you'd expect a desktop computer to do, from playing high-definition video and browsing the internet, to making spreadsheets, word-processing, and playing games.

Also the Raspberry Pi has the ability to interact with the outside world, and has been used in a wide array of digital maker projects.

Figure 4. Raspberry PI

In this paper, Raspberry PI is responsible for many tasks in different steps. In the first step, Raspberry PI receives the signal from the sensors and makes some processing in order to get the real information from the sensors. In the second step convert this data to ASCII code. In the third step bring any picture from its memory randomly in order to use it in steganography. In the fourth step do search about each pixel in the image has ALPHA equal 254 and change it to 255, the purpose behind this step is to give indication to the receiver about where is information hidden as I will explain. In the fifth step select number of separated pixels equal to the number of bytes in the coded information and put each byte instead of blue byte (as I did) or any other colors. In the sixth step, change the ALPHA of each selected pixels to 254. Now each pixel has ALPHA 254 contain coded data in the byte of blue color. Finally the result image sent via TCP/IP protocol.

All above steps are programed using Python language. The following flowchart in figure 5 illustrates the operation steps of Raspberry PI in this proposed system.

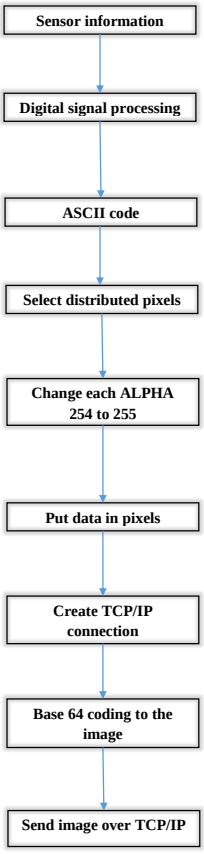

Figure 5. Operation steps of Raspberry PI

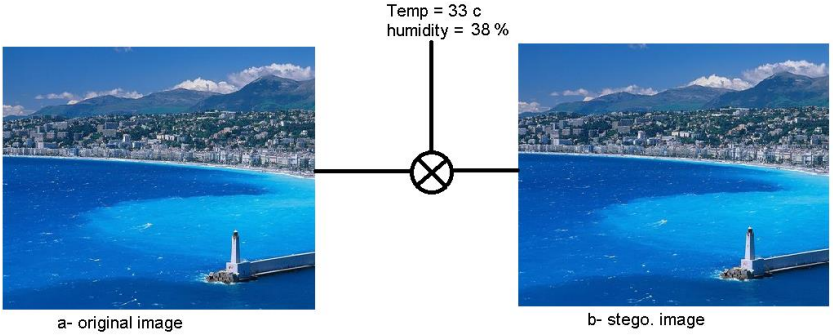

Figure 6. Result (1) of proposed system

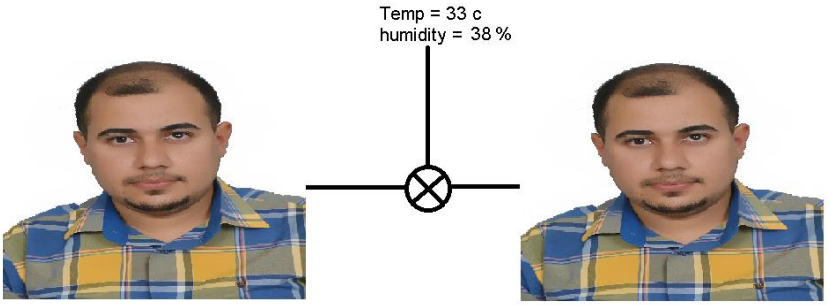

Figure 7. Result (2) of proposed system

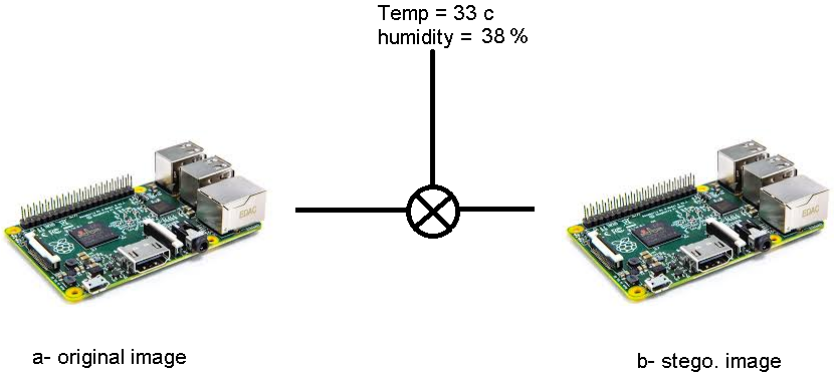

Figure 8. Result (3) of proposed system

In figure 6, figure 7 and figure 8 shows the results of proposed system for different images in size and colors.

2. Extract data from image

In this stage, the same technique of proposed system steganography is used but in inverse arrangement in order to extract information. In the first step receive the stego. image message and process it to get image from base 64 and display it in the program. In the second step select each pixels have ALPHA equal 254 because it has data in it. In third step, get data from selected pixels and display it.

The program responsible for make this tasks is programed by using VB.NET 2013 language. The graphical user interface of program as shown in figure 9.

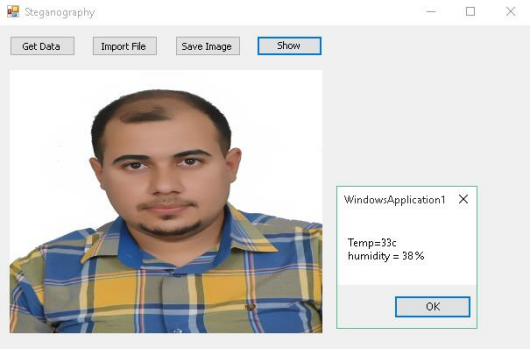

Figure 9. B. Extract data program GUI

As it is clear, the program has four buttons to manage it. The first one is "Get Data". It is responsible for send issue and receive request from Raspberry Pi via TCP/IP. This is mean the information does not transmit all the time but it was the order from the client.

The second button is "Import file". This is responsible for import stego. image from a computer and display it in the image box of the program. This feature provide the ability to receive image from email and other sites not only in the standard method for proposed system

The third button is "Save image". This is responsible for save stego. image in the computer instead of save data this is provide more secure to save information as stego. image

The fourth button is "Show". This is responsible for extract data from stego. image and display it as shown in figure 9.

7- CONCLUSION

- Using steganography to hide sensors information is applicable and provide another level of security
- Raspberry Pi has high processing ability for image especially by using Python language. Also it can programmed to send information via TCP/IP with high level of security.

- Hide information inside image don't alter the visible feature of image. So the information effect on image will be non-visible.
- Select distributed pixels as much as possible decrease the effect on the result image.

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science.

[2] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[3] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[4] Debiprasad Bandyopadhyay, Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain" International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014

[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[7] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996

[8] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998

[9] "Reference guide: Graphics Technical Options and Decisions",

[10] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002.