SECURITY SYSTEM FOR DATA USING STEGANOGRAPHY AND CRYPTOGRAPHY (SSDSC)

Ayman Wazwaz[1], Khalil Abu-haltam[2], Sawan Atawneh[2], Areej Idaes[2], Dalal Salem[2]

[1]Electrical Engineering Department, Palestine Polytechnic University
aymanw@ppu.edu
[2]Electronics and Communications Engineering

ABSTRACT

Security System for Data using Steganography and Cryptography (SSDSC) is a set of hardware and software components that will be used to send secured documents through the internet. Some of the software will be loaded into a microcontrollers in order to increase the complexity and security. The data will be encrypted using the Advanced Encryption Standard (AES) algorithm with a key from the Raspberry PI microcontroller and hide it inside an image using Least Significant Bit (LSB) algorithm, the data will be invisible. The image will be transmitted and received through the internet, the receivers will extract the hidden data from the image and decrypt it to have the original data with the image.

Complicating the steps of hiding and encryption will reduce the possiblity of intrusin of secured documents, and the process will be trasparent to the user to increase security without affecting the normal steps and the behavior in secured documents exchange.

KEYWORDS

Steganography, Cryptography, LSB algorithm, AES algorithm..

1. INTRODUCTION

Steganography is the art and science of concealing communication. The goal of steganography is to hide the existence of information exchange by embedding messages into unsuspicious digital media covers [1]. Cryptography, or secret writing, is the study of the methods of encryption, decryption, and their use in communications protocols [2]. Both techniques manipulate data to ensure the security of information, but the concept of steganography differs from cryptography. Cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. The goal of cryptography is to make data unreadable by a third party, whereas the goal of steganography is to hide the data from a third party. Both techniques have an ancient origin, but the modern field is relatively new. Cryptography and steganography are fundamental components of computer security [1]. In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to

David C. Wyld et al. (Eds) : CSEN, SIPR, NCWC - 2016
pp. 31–38, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61003

transfer data from one end to another across the world. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification.

In this paper, we present a system that is able to encrypt documents, hide it in an image and send it in one side, and then retrieve it in the other side. It uses a graphical interface to facilitate the use of the system and have the ability to transmit and receive through the public internet while keeping documents secured.

2. PROBLEM STATEMENT

The SSDSC can be used in many applications across the world, such applications will include the general secondary exams in Palestine, it will reduce the burden of carrying and distributing exams to hundreds of schools, other beneficiaries of the SSDSC are Banks, between branches and between the bank and its clients. No matter how large or small your company is, you need to ensure the security of your information assets, so you can use this system to protect your information. Other applications of SSDSC is online elections, internet banking, medical-imaging and others.

3. RESEARCH METHODOLOGY & SOLUTION

The SSDSC system consists of software and hardware. The software part will be loaded into a microcontroller attached to the computer at both sides in order to increase its complexity, and to secure the process of extracting data and decryption.

Raspberry Pi is small single-board Linux computer that is used to execute codes instead of computers in some environments. Here, it is used to store keys to be used in data exchange, and codes to implement the encryption and digital steganography.

Figure1 shows the system components and processes that consists of five parts namely: Text, Image, PC, Microcontroller (Raspberry Pi) and internet.

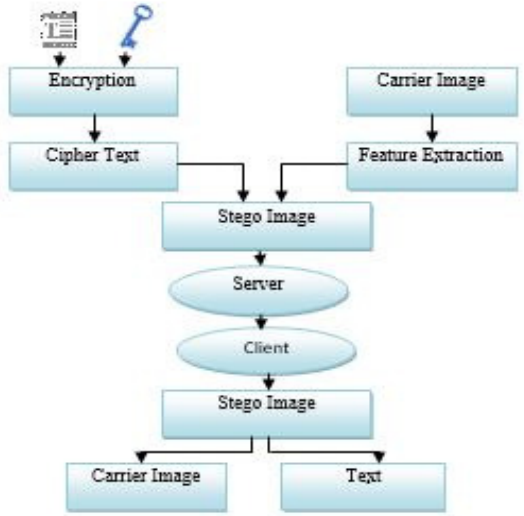

Figure1: SSDSC System Components

The system works according the following steps:

- First step, Insert the text and image to the application.
- Secondly, the text will be encrypted and then hidden within the image.
- Thirdly, connect the microcontroller with the computer, and then the microcontroller work on the text and apply encryption.
- Fourthly, upload the image that contains the information encoded on the server.
- Fifthly, the client access to the server and download the images that contain encoded information.
- Finally, the computer will work on the extraction of encrypted data of the image, then break this encryption to have the original data (file).

4. SOFTWARE AND HARDWARE IMPLEMENTATION

The data will be encrypted on the Raspberry Pi using AES algorithm. The AES stand for Advanced Encryption Standard which is substitution/permutation network cipher. It take 128-bit plaintext and 128, 196 or 256 bit key, depending on the number of rounds [2].

Advanced Encryption Standard, also known as Rijndael is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) [2].

The criteria is defined by NIST for selecting AES falls into three areas: Security, Cost, and Implementation. The AES algorithm is used in this system to encrypt the data which is called the cipher data. The key is 256 bits size, it is generated on the Raspberry Pi.

The cipher data will be hidden in image. The most important method will be lagged the hiding is the implementation of the feature extraction of the images in which algorithms are used to detect and isolate various desired portions or shapes (features) of an image. The selected portion is not important in scene. It is particularly important in the area of recognition. The algorithm is Object detection in a cluttered scene using point feature matching. This process is implemented using Matlab code.

A popular digital steganography technique is so-called least significant bit (LSB).Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [3]. The least significant bit (the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [4].

The object detection algorithm used to extract the features of the image. It is detect the object which is not important in scene .Then the cipher data will be hidden using LSB algorithm in this object.

The system will read the image and convert it into grayscale. The features will be extracted using object detection in a cluttered scene using point feature matching algorithm to determine the parts which is not important in scene. If the capacity of these parts is suite for hiding the cipher data in it, the system will choose the pixel and hide the data. The cipher data will be divided into sub data when the capacity is not enough and testing the condition again. The data will be hidden in the image which is called stego-image .The changes in color of the bits will not able to be notice from the users.

Virtual Private Network is a client server application based on tunneling protocols that are used in making private connection based on public infrastructure like the internet. Here, it is assumed that the sender and the receivers use the internet as an infrastructure, and VPN software is installed to assure privacy.

5. RESULTS

Here, the results of the steps explained earlier to extract the features of the image; object detection algorithm code detected a specific object (Engineering building in Palestine Polytechnic University campus). The ciphered data is hidden in this image.

Figures 2,3,4 and 5 are the results of selecting image and hiding the secured data in specific parts according the features of the selected images.

Figure 2 shows the reference image containing the object of interest (Engineering building) and the target image containing a cluttered scene (image of a different objectives).

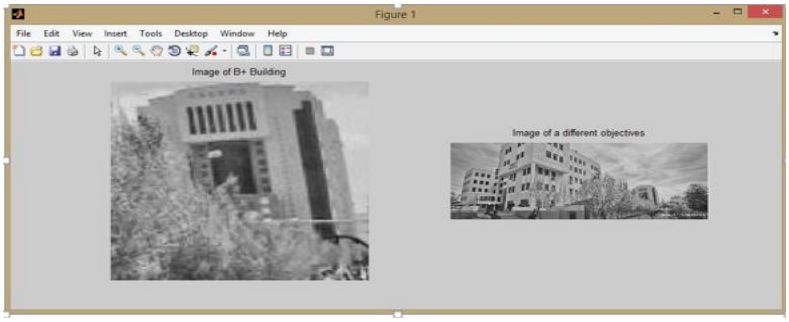

Figure 2 The reference image and the target image

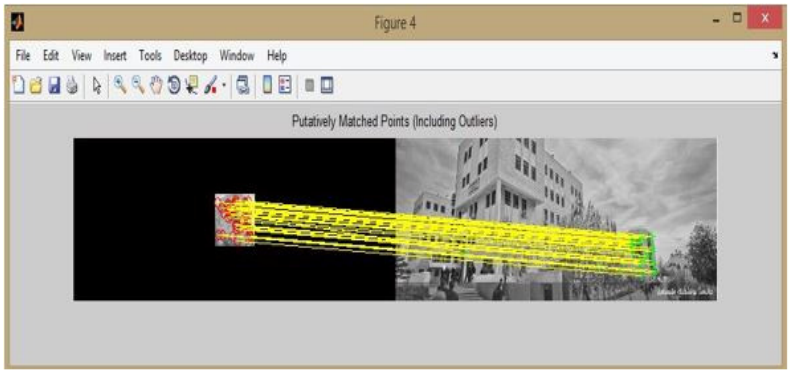

Figure 3: Display matched features

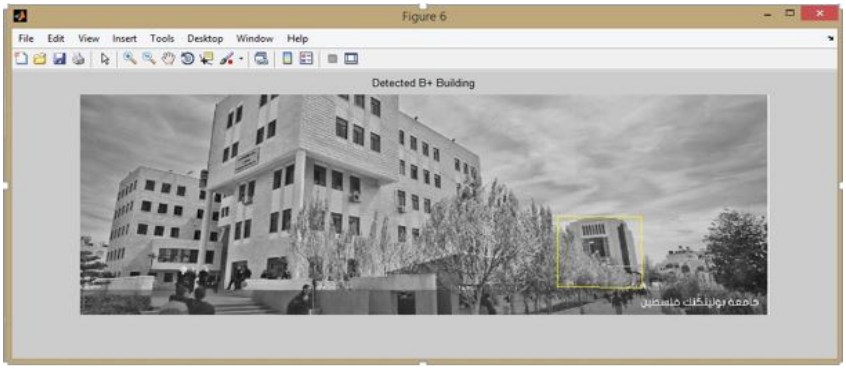

Figure 4: Display the detected object.

Figure 5: Detected object image which is used to hide the data

After implementing the LSB algorithm, we obtained the following results:

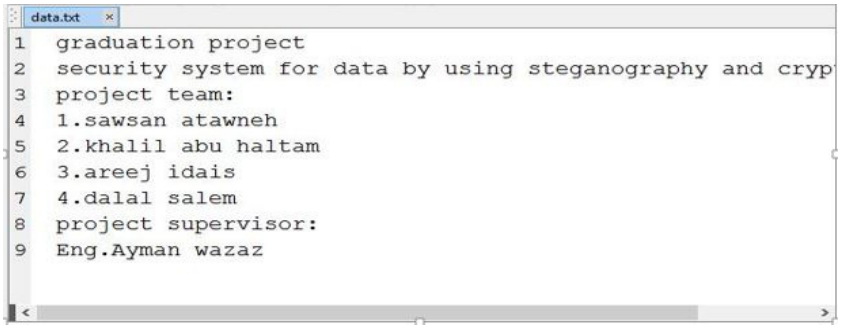

Figure 6: The hidden text.

Figure 7 : Stego-image.

6. TESTS

When the system hided the data, the images before and after the hiding is approximately the same. The difference between the images locate the pixels position of the hidden data.

In image comparison, figures contains the first image (carrier image), the second image (stego-image), and the histogram for the both and result of the test.

A histogram is a graphical representation of the distribution of numerical data. It is an estimate of the probability distribution of a continuous variable (quantitative variable) in an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image [5].

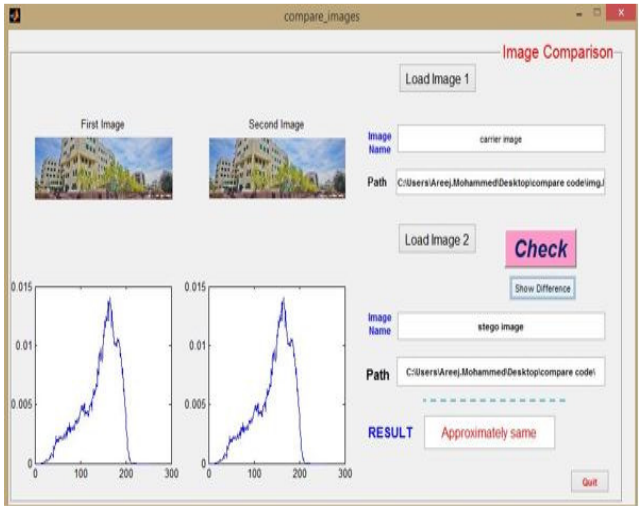

Figure 8: The result of the comparison between the carrier image and stego-image which is approximately the same.

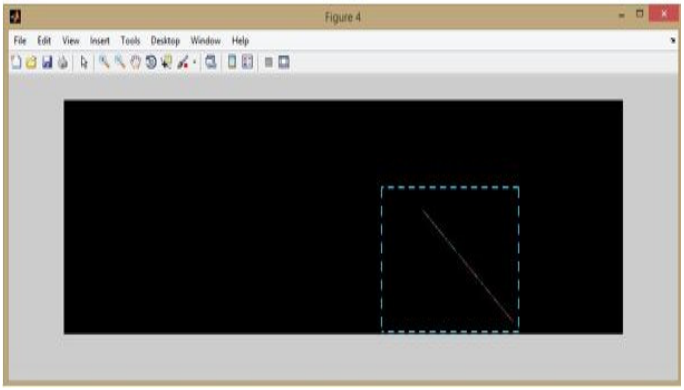

Figure 9: The difference between the carrier image and stego-image.

```
Image File Size  521640
Text  File Size  200
percentage of  differences =textLength/size*100
percentage of  differences 3.834062e-02
percentage of similarity= 99.99961
fx >>
```

Figure 10: The percentage of similarity and differences between the two images.

Figure 9 shows a small sequence of dots resulted from the difference between the two images, and figure 10 shows the number of hidden bytes compared to the image size, and the percentage of similarity between the two images.

A website will be used by the users to upload and download the files. The administrator of the webserver need to login to the website using a username and a password. The files will be added or removed by the administrator who is responsible for the distribution of these files to the other authenticated users. Other users will use the same website to login in and download the documents. Figure 11 shows the login page on the web server.

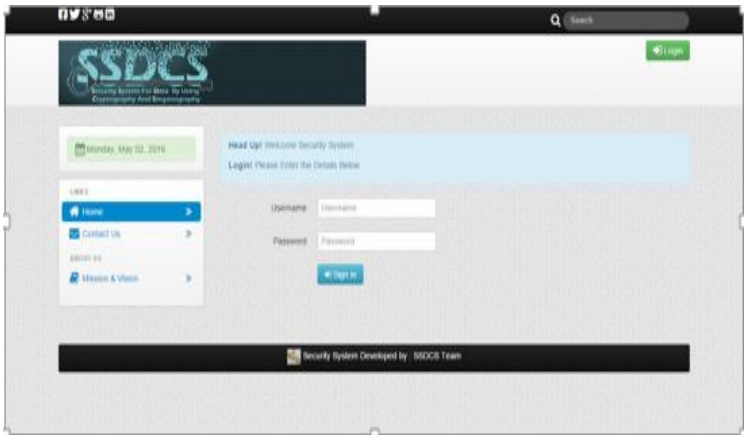

Figure 11: Access to the web server

The security in this system is integrated from different protocols and services:

- Encryption with keys using AES.
- Steganography using images
- Hardware security using microcontrollers.
- Signing in using username and password.
- Virtual Private Network (VPN) to open a private connection using the internet as a public service.

7. CONCLUSION

The "Security System for Data using Steganography and Cryptography" has been designed and tested. The system designed to encrypt the data using AES algorithm, extract the features of the image to detect the places that are suitable to hide the cipher data in. The data will be extracted from the image and retrieve the original data and image.

Adding hardware components made the system more secured because the encryption keys are distributed with hardware itself, this added value will make it difficult for intruders to have a copy of this hardware including the software embedded in the system.

REFERENCES

[1] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information – hiding technology, in H. Nemati (Ed.), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.

[2] Carl H. Meyer and Stephen M. Matyas, Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, New York, 1982.

[3] P.C. Wu, W.H. Tsai, A stenographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (2003) 1613-1626.

[4] R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.

[5] Freedman, David; Diaconis, P. (1981). "On the histogram as a density or: L2 theory".Zeitschrift furWahrscheinlichkeitstheorie und verwandte Gebiete 57 (4): 453–476.Doi:10.1007/BF01025868