International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.06,Issue.07
February-2017,
Pages:1367-1369

www.ijsetr.com

Raspbeery Pi Based Image-Audio Steganography for Data Security

P. SAMATHA[1], K. J ONESIM[2]

[1]PG Scholar, Dept of ECE, Vignana Bharathi Institute of Technology, Hyderabad, TS, India,
E-mail: samatha.potu92@gmail.com.

[2]Associate Professor, Dept of ECE, Vignana Bharathi Institute of Technology, Hyderabad, TS, India,
E-mail: k.onesim@gmail.com.

Abstract: Steganography is the method of hiding secret information like text, password, image and audio behind original cover file. In this paper we proposed an image and audio steganography using raspberry pi. In this system, our aim is to hide message behind the image, audio file. The message can be a text, image or audio. The embedded system will help to secure the message with in the audio and image file. In Embedded system, the message much secure because even though if the unauthorized person succeeds in being able to hack the image, the person will not able to read the message as well as acquire the information in the audio file. Secret data like image and audio is encrypted into cover data by developing the application involved with LSB algorithm on ARM architecture device.

Keywords: Raspberry Pi, LSB Algorithm, Secret Data.

I. INTRODUCTION

The growing possibilities of modem communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. Unauthorized copying is of great problem of especially to the music, film, book and software publishing industries. To overcome this problem, some invisible information can be embedded in the digital media in such a way that it could not be easily extracted without a specialized technique. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and Stenography. All these applications of information hiding are quite diverse.

II. LITERATURE SURVEY

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 transfer data from one end to another end. However, one of the main problems with sending data over the internet is the security. Therefore it becomes very important to take data security into consideration. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: digital watermarking Cryptography and Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

III. EXISTING SYSTEMS

In previous, cryptography and steganography is used for encryption of data and provides data security. Actually term cryptography provides privacy and steganography is the art and science of communicating in an approach which hides the existence of the communication. The steganography hides the message so it cannot be seen; cryptography jumble a message so it cannot be understood. Cryptography systems can be broadly classified in to symmetric-key systems that use a single key that both the sender and the receiver have, and public key systems that use two keys, a public key known to every one and a private key that only the recipient of messages uses

IV. PROPOSED SYSTEM

In existing system, if the “Unauthorized user” is able to access the content of cipher message steganography will fail, to overcome this drawback only steganography is used for sending data like image and audio and make it hidden. Up to now data hiding is done by using Matlab so that it is only used in systems and laptops, now we are implementing this project in raspberry pi kit with Linux operating system. By

this we can use this in mobile phones also. Steganography algorithm is used for embedding the data in to bit map image (.bmp) and joint photographic expert group (.jpg) and audio files like waveform files (.wav).The algorithm implemented in this project is LSB (least significant bit) algorithm This approach is to replace the data of lower bit in a cover audio data and in a cover image file by a secret data. Secret data like image or audio is encrypted and send in another image or audio, the cover image need to be selected carefully and preferably in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colors. We are using raspberry pi for designing predictive model for image and audio steganography system.
The block diagram representation of our project is shown below.

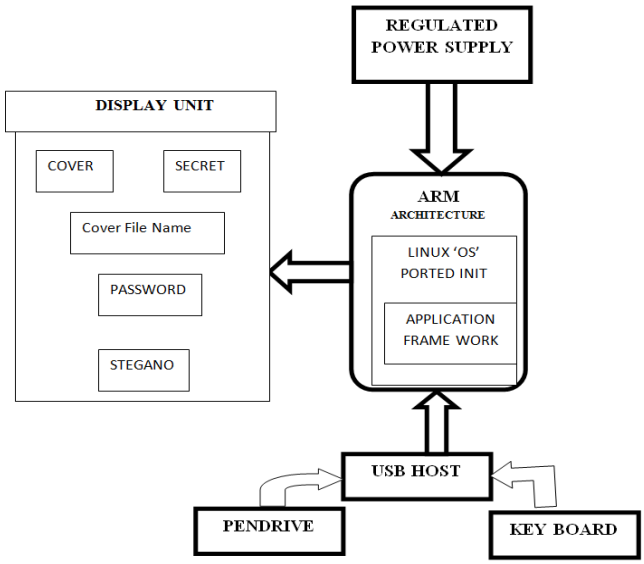


Fig 1. Block Diagram of proposed system.

V. LSB ALGORITHM

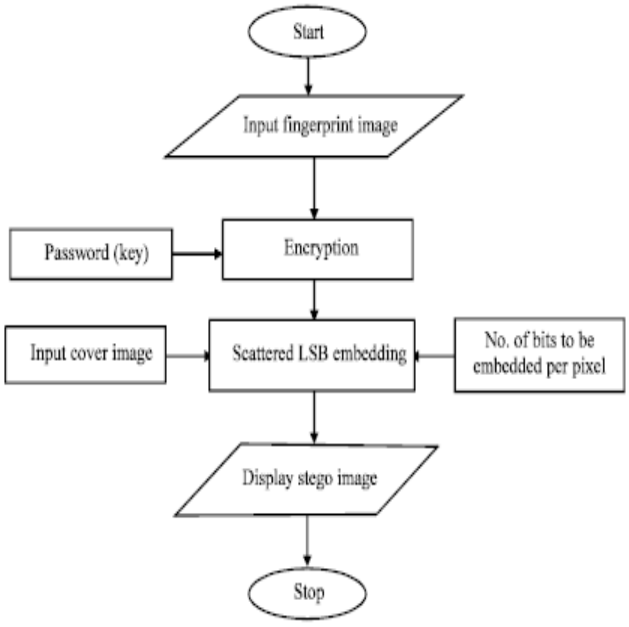


Fig 2. Flow chart for LSB Algorithm.

In this paper we have use the substitution of LSB and LSB+3 bits of the cover file in alternate bytes. The last 300 bytes of the cover file we use for embedding password, size of the secret message file. After that we start to embed the secret message file. We read one byte from encrypted secret message file and convert it into 8 bits and then we take 2 bits of the encrypted secret message and substitute the LSB and LSB+3 bits of the cover file and then leave one byte of the cover file intact. Then again substitute 2 bits. The same process we repeat for all 8 bits of the secret message. Here the change is prominent as we embed in text characters but if we do the same in some image then the changes made here will not be very significant as our eye will not be able to differentiate between two colors.

VI. HARDWARE IMPLEMENTATION

A. RASPBERRY PI BOARD

The Raspberry Pi is a credit-card-sized single-board computer developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools. The Raspberry Pi is manufactured in two board configurations through licensed manufacturing deals with Newark element14 (Premier Farnell), RS Components and Egoman.

These companies sell the Raspberry Pi online. Egoman produces a version for distribution solely in China and Taiwan, which can be distinguished from other Pis by their red coloring and lack of FCC/CE marks. The hardware is the same across all manufacturers. The Raspberry Pi has a Broadcom BCM2835 system on a chip (SoC), which includes an ARM1176JZF-S 700 MHz processor, Video Core IV GPU, and was originally shipped with 256 megabytes of RAM, later upgraded to 512 MB. It does not include a built-in hard disk or solid-state drive, but uses an SD card for booting and persistent storage.

VII. SOFTWARE REQUIRED

A. Linux Operating System:

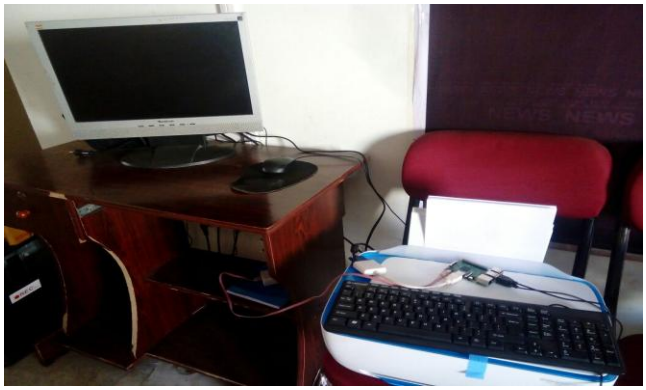
Linux or GNU/Linux is a free and open source software operating system for computers. The operating system is a collection of the basic instructions that tell the electronic parts of the computer what to do and how to work. Free and open source software (FOSS) means that everyone has the freedom to use it, see how it works, and changes it. There is a

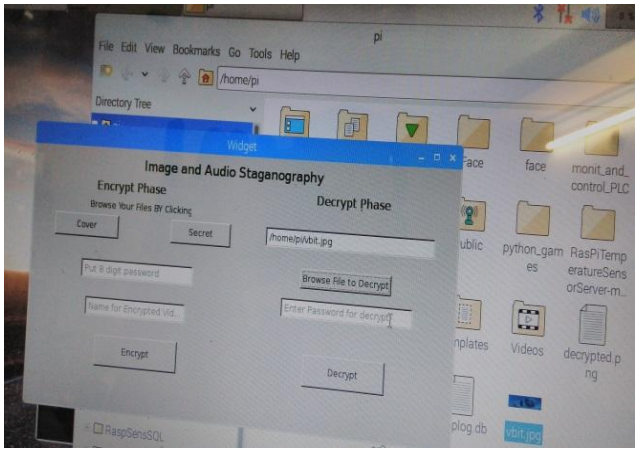
lot of software for Linux, and since Linux is free software it means that none of the software will put any license restrictions on users. This is one of the reasons why many people like to use Linux. A Linux-based system is a modular Unix-like operating system. It derives much of its basic design from principles established in UNIX during the 1970s and 1980s. Such a system uses a monolithic kernel, the Linux kernel, which handles process control, networking, and peripheral and file system access. Device drivers are either integrated directly with the kernel or added as modules loaded while the system is running.

B. Qt for Embedded Linux:

Qt is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as a widget toolkit), and also used for developing non-GUI programs such as command-line tools and consoles for servers. Qt uses standard C++ but makes extensive use of a special code generator (called the Meta Object Compiler, or moc) together with several macros to enrich the language. Qt can also be used in several other programming languages via language bindings. It runs on the major desktop platforms and some of the mobile platforms. Non-GUI features include SQL database access, XML parsing; thread management, network support, and a unified cross-platform application programming interface for file handling. It has extensive internationalization support.

VIII. RESULTS





IX. CONCLUSION AND FUTURE SCOPE

In this project, hiding the secret data like text, image and audio in cover file is successfully implemented and tested. It can be further improved by hiding the secret data in video cover file.

X. REFERENCE

[1] M, Pooyam, A, Delforouzi “LSB based steganography method based on lifting wavelet transform”2007 IEEE International symposium on signal processing and information technology, pp600-603.

[2] SghaierGuizni, NidalNaser,"An Audio/Video Crypto Adaptive Optical stegnography Technique"IEEE 2012.

[3] Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2008) Digital Watermarking and Steganography Second Edition. Elsevier, 2008.

[4] Joan Daemen and Vincent Rijmen, The Design of Rijndael, AES - The Advanced Encryption Standard, Springer-Verlag 2002 (238 pp.).

[5] Empirical analysis on steganography using jsteg, outguess 0.1 and f5 algorithms.