ijecs
open access

www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242

Volume 4 Issue 7 July 2015, Page No. 13072-13075

ARM Based Application Of Data Hiding Process By Using Anti Forensics Technique For Authentication

K. Jaswanthi, J. Amarendra, M.Tech(ph.d)

Department of Electronics and communication Engineering

Audisankara College of Engg & Tech

(Autonomous)

Abstract: In this paper, the system for data hiding in audio-video using anti forensics technique for authentication and data security is designed by using 32-bit ARM controller for image, audio and image steganography. The embedded system will help to secure the message with in the audio and video 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— ARM microcontroller, LSB algorithm, encrypted data, secret data.

I. INTRODUCTION

Steganography means covered writing. Its goal is to hide the fact that communication is taking place. 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. The copyright of digital media such as audio, video and other media available in digital form may lead to large-scale unauthorized copying. This is because the digital formats make it possible to provide high image quality even under multi-copying. 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. In watermarking applications, the message contains information such as owner identification and a digital time stamp, which is usually applied for copyright protection. This adds to copyright information and makes it possible to trace any unauthorized use of the data set. Stenography hides the secret message within the host data set and its presence is imperceptible.

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 across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the „security threat it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

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 SYTEM

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. The subject is that study techniques for decoding cipher messages and detecting hide messages are called cryptanalysis and steganalysis.

Steganography is not the same as cryptography, data hiding techniques have been widely used to broadcast of hiding secret message for long time. Assuring data security is a big dispute for computer users. Even though both methods provide protection, to add multiple layers of security it is always a good practice to use cryptography and stegnography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. In color image (e.g. scanned image) there are 3 color data values for one pixel, that is red, green, and blue. To save storage, there is 24 bit representation for each pixel. So hiding without significant distortions is very difficult for color images. As arbitrarily flipping a pixel in a color image could be easily noticed. So any pixels on the boundary may be modified, and it also needs some constraints.

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 in Mat lab so that it is only used in systems and laptops, now We are implementing this project in raspberry pi kit by this we can use this in mobile phones also. Steganography algorithm is used for embedding the data in to map image (.bmp). This approach is to replace the data of lower bit in a cover audio data by a secret data.

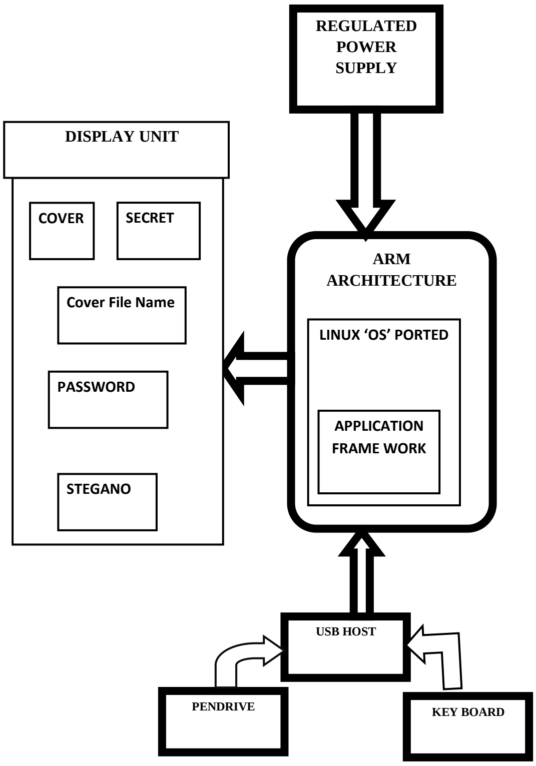


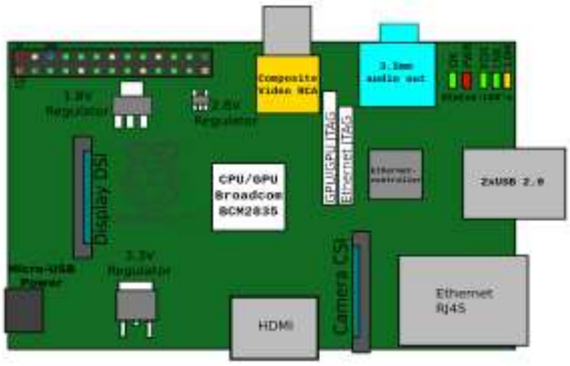
Fig.1: Block Diagram for Proposed system

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 32-bit ARM controllers for designing predictive model for image and audio steganography system. Data is embedded in low level sub-band to avoid compression losses. Human visual systems (HVS) model points out different insensitive among different level sub bands. More data can be embedded without causing notable visual artifacts. For embedding secret message we are skipping 300 bytes from the last byte of the cover file. After that we start to embed bits of the encrypted secret message in to cover file. We will select secret message file less than cover file.

V. HARDWARE IMPLEMENTATION

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.

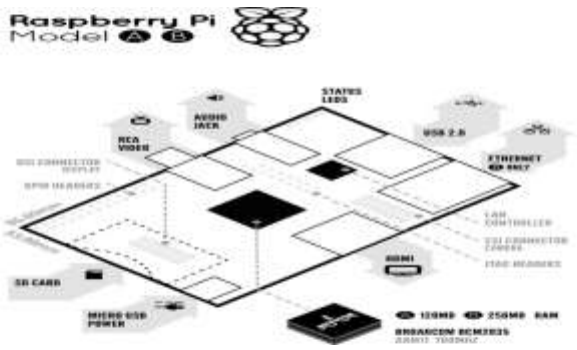


Fig.2: Board features

The Foundation provides Debian and Arch Linux ARM distributions for download. Tools are available for Python as the main programming language, with support for BBC BASIC (via the RISC OS image or the Brandy Basic clone for Linux), C, Java and Perl.

VI. SOFTWARE IMPLEMENTATION

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.

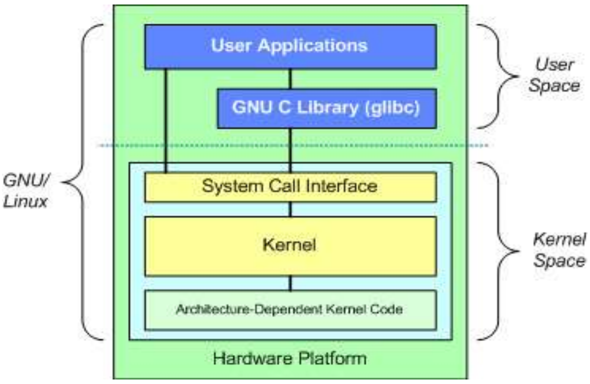
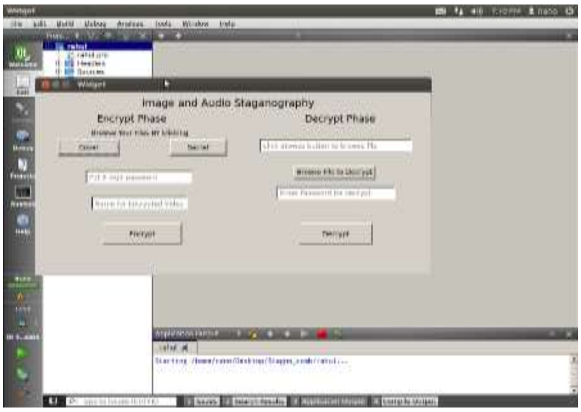


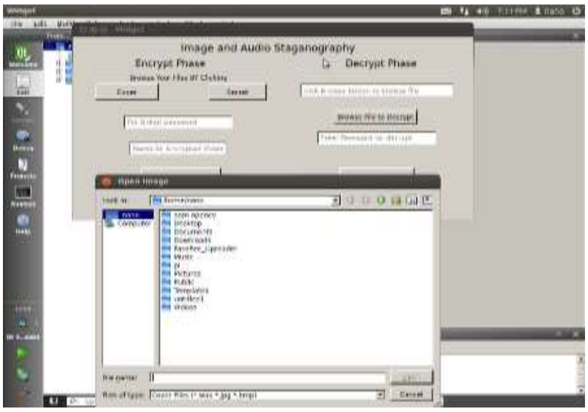
Fig.3: Architecture of Linux Operating System

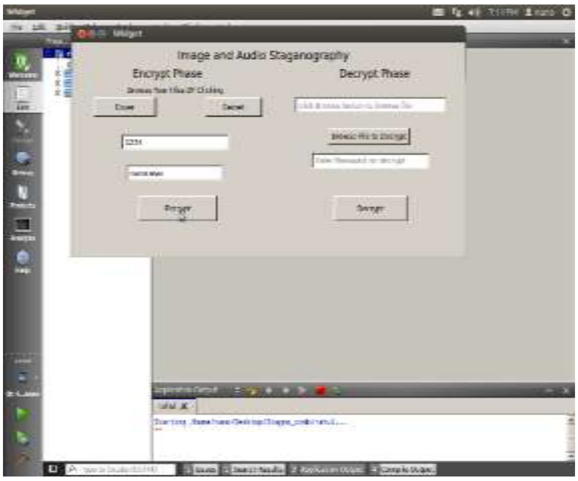
B. *Qt for Embedded linux:*

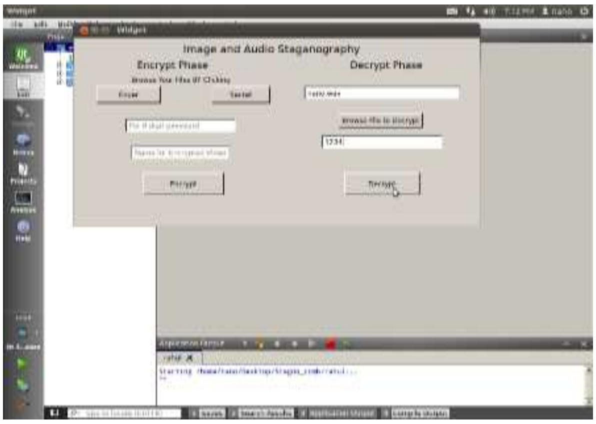
Qt is a cross-platform application framework that is widely used for developing application software with a graphical user interface (GUI) (in which cases Qt is classified as awidget toolkit), and also used for developing non-GUI programs such ascommand-line tools and consoles for servers. Qt uses standard 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 programing interface for file handling.It has extensive internationalization support.

VII. RESULTS









VIII. CONCLUSION

The project titled **"ARM BASED APPLICATION OF DATA HIDING PROCESS BY USING ANTI FORENSICS TECHNIQUE FOR AUTHENTICATION"** has been successfully designed and tested. It has been developed by integrating features of all the hardware components and software used. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced Raspberry pi board and with the help of growing technology the project has been successfully implemented.

REFERENCES:

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

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

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

AUTHORS

K.jaswanthi received her B.TECH degree in Electronics and communication Engineering from KSN Institute of Technology, Kovur, Nellore (Dist), affiliated to JNTU Anantpur. She is currently pursuing M.Tech Embedded systems in Audisankara college of Engineering and Technology(Autonomous), Gudur, Nellore (Dist), affiliated to JNTU Anantpur.

Amarendra Jadda is working as Associate Professor in ECE Dept, ASCET, GUDUR. He has been guiding UG & PG students since five years in this institution. He pursued his M.Tech from JNTUH, Kukatpally Hyderabad. He presented papers in six international journals & six international conferences. His interesting fields are Communications &Signal Processing, Embedded Systems.