I J C T A, 9(32), 2016, pp. 261-269 ISSN: 0974-5572

A Study of Low Power Consumable Frameworks for Hiding Audio signals in Image Container Using Different Steganography techniques Using ARM Controller Devices For Smart Living

P. Sanyasi Naidu* and Jagadish Gurrala**

ABSTRACT

Steganography is a predominant field in the computing world where all kinds of data to be hidden (text, audio) through embedding them into Host image as a carrier act as a container to pass through wireless medium and to retrieve secret data at receiver for extraction. In the few decades many researchers focused on hiding data in original audio using lot of audio steganography techniques so far, for taking more power has been consumed during signal transmission. In this context, Images are a good medium for hiding data (Pan, Chen, and Tseng3) passing through mobiles. There is no such techniques designed to hide audio file into Host image as a container using low power consumable frameworks. Since contemporary technologies, there is a lack of research in the covered writing within image where as limited hiding techniques were found into fixed length host audio media ûle (MP3) through analysis. In the current technology, various frameworks need to develop and find out the implications on digital information of .wav files to stay hidden Between Pixels (BP) in .bmp or .jpeg image data irrespective of any operating systems; however, it takes less time to hide audio chunks into Cover image using DES algorithm for data security and also taken pseudo randomness keys for authentication has been studied and also working on Arduino based 32-bit Advanced RISC Machines (ARM) micro controller used for it . In the paper present framework can provide roadmap of how to apply secure the stego-audio within the image file through Arduino software and logic building to hidden data into it. In Low power consumable devices requires less amount of hidden data to process data and then becomes secure when the person is not able to read the message as well as extract the information from the host image within range of 1KB to 10MB size of address in RAM. In the paper throws a light on placement strategies where to fit the secret data in Cover image using encrypted form of plain text to travel across media using Arduino software involves DES algorithm. In the paper finally attempt to kept audio hiding into the cover image through ARM based DMA- 24xx series succeeded in the maintenance of same quality of camouflage audio include a big enough of secret data and without affecting the quality of sound during transition in host image for mobiles.

Keywords: Steganography, Arduino board ARM controller, DES, mobile devices, Data Security, Authentication, Application framework.

1. INTRODUCTION

Steganography works on covered writing to attain secrecy starting from when the message is ready to departure and when the message being arrived. The aim of steganography is to conceal the any type information like image or audio that camouflage it into host data(meta data) as a container. There is a increase in popularity regarding social media where lot of traffic patterns for examine where actual security needs in social network analysis and auditing area without having a proper hardware and software requirements.. The information security and auditing is fundamental area where all kinds of social network

* Dept. Of CSE, GIT, Gitam University, Bangalore Campus, *Email: snpasala@yahoo.com*

** Dept. Of CSE, Anil Neerukonda Institute of Technology And Sciences, Viskahapatnam, *Email: gjagadish.cse@anits.edu.in.*

traffic is exchanged among routers that spans globally when internet traffic increases. Henceforth lot of study is required during embedding the image or audio inside image to extract actual information during secret data transmission with respect to confidentiality and user authentication of actual data inside original data; however research is biased in particular aspect where unwanted data kept inside original data by attackers in recent years. Audio Information to be kept secret inside image is now played a key role in information security in next coming years is able to protect conceal data is a major task to protect legal information against unauthorized access. This has resulted in an explosive growth in the field of information security domain. The originality of actual authors who written books such as authors text books , water marked images, video broadcasting like ETV or TV9 broadcasting stay the hidden data remains constant otherwise it would lead to tremendous illegal copying in grayscale markets. Nowadays Illegal copying is of big business in gray market especially suffers more in music industry, film industry and distribution of new novels arrivals like JK Rowling's novels like harry potter new series inauguration and software publishing industries like CDROM distribution in public markets where it could not reveal original identity. To overcome illegal copying activities in public market , some information need to be stay hidden using cryptography techniques like DES with 56 keys used to encrypt plain text hidden in the original digital media as a carrier in order to extract required information from stego data .In the paper the authors emphasize on how Information hiding is a part of information security area where lot of research required and need to evolve since 2004, where to acquire suitable knowledge about how to hide audio inside image, which encompasses applications for covered writing process.

All these legal copying applications of image covered writing is having different forms of hiding the actual information inside image. In the real world the concept of audio hiding process is the null visibility to the statistical attacks where not getting hiding formation who were using services along with digital time stamp . For example service provider allow to client where real time image being transmitted through partially hidden information of date and time printed like a DD/MM/YYYY format used in camera captured images in Visakhapatnam port trust by the use of service of video surveillance devices. This adds to real time copyright information and makes it possible to trace any attackers use of the data set on the spot. Several types of Stenography methods have been used to hides the secret message within the host data set and its presence is imperceptible.

2. LITERATURE SURVEY

In recent years, the prerequisite of the digital India is the concept of Prime Minister Mr.Narendra modi conceived the title of Make in India slogan to entrepreneur of all parts of peoples come out the nature of having floating information across several cities[1]-[3] provide wi-fi services to free of cost to public places to transfer heterogeneous types of images from one city to another city across the world for smart living applications. There are many possible ways to transmit images which carries text or audio across wireless medium through e-mails, chats, whatsapp, imo instant video applications through mobile networks. The mobile communication is a part of communication where all types of services through mobile internet over insecure telecommunication network. The big drop out of the using mobile internet is lack of steganography exist in network whereas mobiles are sending Plain data over the internet. Nowadays there is the big gap in the security vulnerability, the mobile possesses i.e. the mobile phone memory contains sensitive information like whatsapp history or phone book directory and storing banking username and password can be stolen [6] in many ways. Since mobile communication taken place a important role in security aspects, where as it is one of the foremost contribution that need attention during the process of hiding data in transit. Information security illustrates the way of protect of inner information from adversaries and providing high level security to prevent stego image modification from unusual traffic.

In fig 1 illustrates regulated power supply is a transmission relay service which supplies power to ARM board which is less power consumable devices where all types of hidden information is to be accepted via

mouse through USB port for getting embedding information and send it as steg image to media and then receive at destination to retrieve original information from stego image . In order to improve the security features in stego image transfers over the internet. In the following sections, the paper organized as a section 2 discuss the idea of implementing hiding audio in image, in section 3 discuss the existing frameworks of hiding information in Image using steganography techniques and next section discuss the proposed idea, and section 5 section discuss the Arduino based ARM Controller processors and final section discuss the summary and future directions of frameworks about hidden audios in image steganography.

2.1. Related Work

In existing system if the "Unauthorized user" is able to access the content of cipher message along with steganography will fail, to overcome this drawback only steganography is used for sending host data like image and then fit the audio bits into it 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 in the paper the new idea to implement this concept is to make use of Arduino Board Microcontroller by any one can use this in mobile phones also. Steganography algorithm is used for fitting secret information into host image where placement strategies are developed in loss less image (.bmp). This approach is to replace the data of lower bit in a cover Image data by a secret audio.

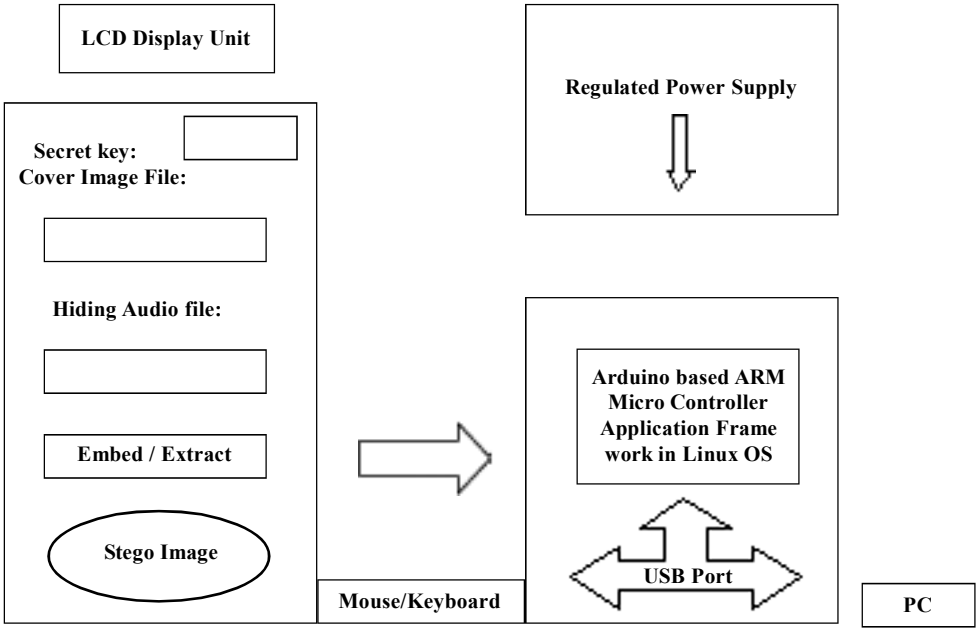

Figure 1: Interface of Arduino based ARM microcontroller to perform steganography on Host Image through Linux

3. EXISTING FRAMEWORKS:

There are few ways to be discussed to hide any data into Host Audio as per records surveyed in the domain[1].

3.1. AUDIO as a METADATA

As explained so far in literature survey need of conduct rigorous research [2] has been surveyed onPersonal computer (PC) to accept stego image where mathematical formulation required to hide actual data into the carrier in order to make undetectable. The Human Auditory System(HAS) is a kind of entropy mechanism to add actual or secret data and host image together to form a stego image there fore any attacker is unable to differentiate original image and stego image. According to the paper [3],the idea contributed the idea about how the color image is spread out the over spectrum range dynamically for identify hue colors of rainbow image. As a result, loud sounds tend to mask out quiet sounds. Additionally, the HAS is unable to perceive absolute phase, only relative phase. This paper produces bad results of data hiding methods to

kick start the idea of next ideas where all types of stego images carries details without affect their quality of image.

There are a couple of advantages as well:

1. The quality of stego data either image or audio files strength is deteriorated while size of the image grows then steganography use to contend the range of sizes where appropriate sizes are allowed to maximum reaching capability in the case of inner details of host image. For example stego data details must be kept in the range of below 10KB size when the host image is the twice of the stego data, i.e 20 KB.
2. The intense contribution of the paper is thinking of better hiding capacity of audio information like mp3 files in Window's VLC media player and made it available to 1 Tera Bytes to 100 Peta Bytes Audio data centers instead of storing less image hiding capacity on host image.

3.2. Actual Image hiding in a Host Image file

From the perspective of hiding image within image, to provide security on covered image . in this context most of steganography deals with Least Significant Bit based hiding process where all pixels information of least significant bits are able to hold another pixels of secret image file to arrange hidden pixels systematically over LSB positions of original image which is described in paper[5] easily to embed actual values of pixels into original values of pixels using spatial domain of steganography rather than frequency domain of steganography.

1. In the paper[1] described earlier that arrangement of pixel values of integer data types can be used rather than ASCII character to eliminate the internal fragmentation of pixel arrangement after loading elements into LSB position using entropy calculation. Entropy means amount of information loaded into color buckets in pixel.
2. In the steganography process[5], the given host image is standardized into specified rows and columns, in which luminance and color information of 8 bit color information allocates values starting from 00000000 to FFFFFFFF in binary representation, 0x00 to 0xff color values ranging from 16 bits to 32 bits. For example 24 –palette color table consists of first least significant bit of color information and most significant bits of pixel values carries luminance part of image which carries stego image over media.Similarly audio files also been stored inside image requires minimum

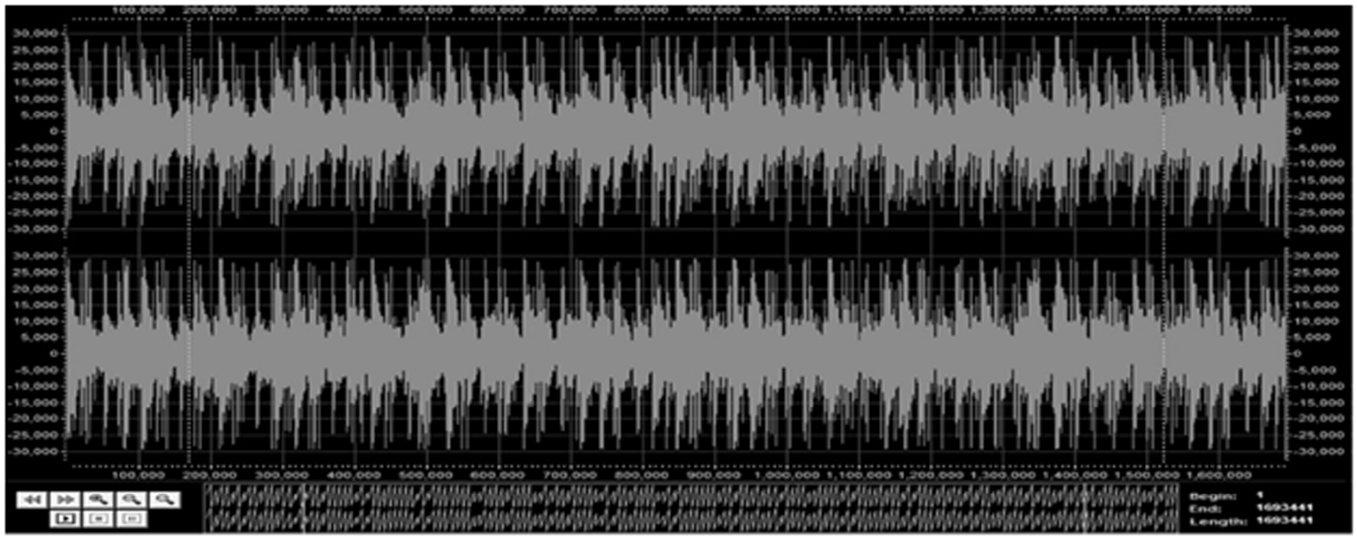

Figure 2: Image File illustrates 8 bit Least significant bits and another 8 bits most significant bits spans over spectrum.

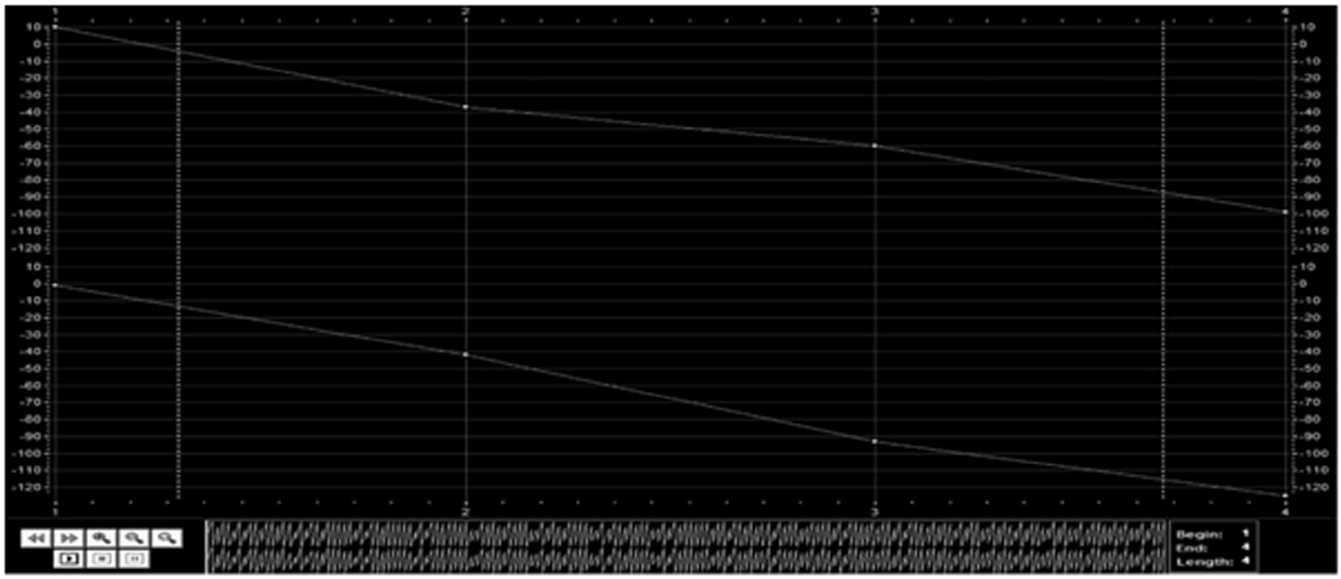

Figure 3: Audio hiding process towards (Top) and Right (Bottom) over insecure Channels about 4 Samples

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	52	49	46	46	28	5C	67	00	57	41	56	45	66	6D	74	20	RIFF(\g WAVEfmt
00000016	10	00	00	00	01	00	02	00	44	AC	00	00	10	B1	02	00	D¬ ±
00000032	04	00	10	00	64	61	74	61	04	5C	67	00	00	00	00	00	data \g
00000048	0A	00	FF	FF	DB	FF	D6	FF	C4	FF	A3	FF	9D	FF	83	FF	ÿÿÛÿÖÿÄÿ£ÿ ÿƒ
00000064	2F	FF	8C	FF	D3	FE	E5	FF	AB	FE	58	00	ED	FE	8D	00	/ÿŒÿÓþåÿ«þX íþ

Sample Wave Original Header and Start of Sample Data Values

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	52	49	46	46	28	5C	67	00	57	41	56	45	66	6D	74	20	RIFF(\g WAVEfmt
00000010	10	00	00	00	01	00	02	00	44	AC	00	00	10	B1	02	00	D¬ ±
00000020	04	00	10	00	64	61	74	61	04	5C	67	00	00	00	00	00	data \g
00000030	0A	00	FE	FF	DA	FF	D6	FF	C4	FF	A3	FF	9D	FF	82	FF	þÿÚÿÖÿÄÿ£ÿ ÿ‚
00000040	2E	FF	8D	FF	D3	FE	E5	FF	AB	FE	58	00	ED	FE	8D	00	.ÿ ÿÓþåÿ«þX íþ

Sample Wave Data Hiding Example Header and Start of Sample Data Values

Figure 4: Analysis of the Host image vs. Hiding data using DES encryption process

number of samples starting from 8 samples to upto 1680 samples embedded into 1MB host image file according to mean and standard deviation of color image table[5].

In the paper authors are illustrates the idea of how audio data is acted as seeing from unseen using DES algorithm to make it imperceptible rather than undetectable. These method are deployed in stay hiding using 56 bit key generation process to encrypt the 64 bit image data to be encapsulated into host image and then decode into actual thing needed to receiver for it.

But it is not used in this paper. It is about hiding audio files into images based on some ideas to be thrown into light.

4. PROPOSED FRAMEWORKS

4.1. Image as a Metadata

Agencies such as the Ministry of Defense academy in India make use of image metadata to trace particular attacker in between routers across smart cities, while sending host images from here and there. If attacker was able to catch the actual image from entire host image for the transfer pictures or post them to indian government websites[5], the metadata stored in the picture could not reveal actual image whenever image was taken into consideration.

There are number of steganography tools for viewing and modifying metadata within pictures. In the paper contributes lot of ideas for embed the .wav bits into .bmp pixel using JStego tool, Steg Torrent tools for extract the actual data into place when image is treated as set of 100 rows and 100 columns

where all audio 9bit tape samples to hold at the LSB positions of pixels of image. In the theoretical point of view the author propose the idea of discuss about how the less size of image of 1.5KB into 2 KB image is not always good. So that actual image to be hidden with 2KB into 4 KB bitmap file.In this way, the host image accommodates locations in which pixel elements are finding out on account of color palette table. In digital india, excess image information can be drawn by attacker when stego image use of 3 KB out of 2.5 KB host image.

Hence, all applications pertain to image as a meta data , when the input image is kept into host image if network bandwidth is limited in order to improve performance of carrying image in to another image. For example 15MB data rate of internet traffic support to transmit less size image of maximum of 100Kilo Bytes of image to be kept into 1000KB file needs correct file representation for storing inside host image. In the section, the image files are categorized into 2 types, one is lossy compressed image file format and another one is lossless compressed image. Most of steganography uses lossless compression images to carry enough size of actual data into it. Where lossy compression, which carry not effective actual data over medium.

Figure 5: Exploring features Propertie in Google's Picasa

4.2. Existing Data Hiding Methods in a .BMP or JPEG files

While adding a audio to the steganography for images, authors suggested to suitable integrated development environment(IDE) for storing audio into pixels of images of .BMP file using Arduino software whenever authors chosen lossless compressed images as a carrier. There are some ideas of changing LSB pixels of given image which paper consider to camouflage audio.In the existing data hiding algorithm describes in two steps: 1. Kept the 1KB audio file into Cover image using Ex-OR operation to mask the inner details. 2. Use the DES algorithm to encrypt the secret key into Pixel positions of Host image.

In the section authors clearly quoted basic representations used in Image as Host image.

4.2.1. Domain in Digital representation in Image

In the section one of the basic domains used in digital audio representations for images. In 2001 spatial domain is frequently used representation in digital image stegnography. After few decades 2006 onwards another field is used in the section where audio samples have been used as a 80 cycles per seconds measure of frequency component. For suppose .wav files are popularly used to represent in frequency domain and .aiff formats are suitable to hold inside image. Another less famous domain is spatial domain where lower quality audio is used as the logarithmically scaled in 8 cycles per second usage. These domains are defined a various combinations of frequency components that supports hiding audio files using Arduino software. The most audio signals are tolerate to upto 1M Hz sizes of file into host image while image as a carrier.

Spatial domain allows the image into 2 important values to hold audio data, one of the value is luminosity value and another value is color value. However, these values are cannot hold the values of audio information into image, while transit. Hence, authors are ready to take challenge to hold audio format in frequency spectrum of image container only where all samples values are ready to positioned into jpeg files happened in frequency domain.

These representations require changes in the statistics of the audio signals. From the contribution of the given section authors chosen some of the measurements of what is defective embedding process in present application and what is good embedding process using following properties.

4.2.2. Present Applications in Image Steganography

The aim of the steganography is to measure of tolerate the hiding of image capacity for host image is a really challenge task in the current applications. Here the current application contributes several ideas to be discussed.

1. Audio steganography when image as metadata: The concept of a digital audio steganography is to tolerate the maximum extent guaranteed transmission over images through where audio samples of 8 bits to be kept inside.
2. Tamper-proofing for audio steganography : the concept tamper proofing is to kept sensitive information how far from attacker and how long to break the key from audio as carrier. In this application, sender and receiver knows only the details of inside information like one time password moved from Service provider to customers where there is no chance of getting the sensitive details to the attackers or intruders. From the discussion, Arduino provide two aspect of running application over medium. First framework runs on low power consumable hardware devices like mobile and second no data except video would be send without affecting the details of audio information inside image.

4.3. Proposed Idea to hide Audio into Image

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 in this paper implement digital envelope concept.

4.3.1. Digital Audio Envelope

In this technique , audio is kept inside image file format. Hence some particular sizes of audio file is put inside image according to the relation between audio size and image size formats. In this application, stego audio required 0 location to n-1 location where n is total number of pixels in the host image.

4.4. Architecture of Arduino based Proposed System:

In the proposed architecture discussed framework using software framework called Arduino software[8], built up with 3 tier architecture. In the Interface through keyboard and display unit is used in it, where LED display is used to display resultant of the given inputs to be implemented. While input audio information is accepted through low power consumber device refered to as Arduino based Processor.

In the application view to perform key generation of key subsets acceptable by arduino configuration made from key values starting from i = 1 to n, where $1< n< 100$ real values to be accepted to encrypt audio file inside image. It also accepting negative values also depends on float range in UBUNTU linux operating system. The audio file is of .wav file extention for better accept the data to be hidden into JPEG file. The

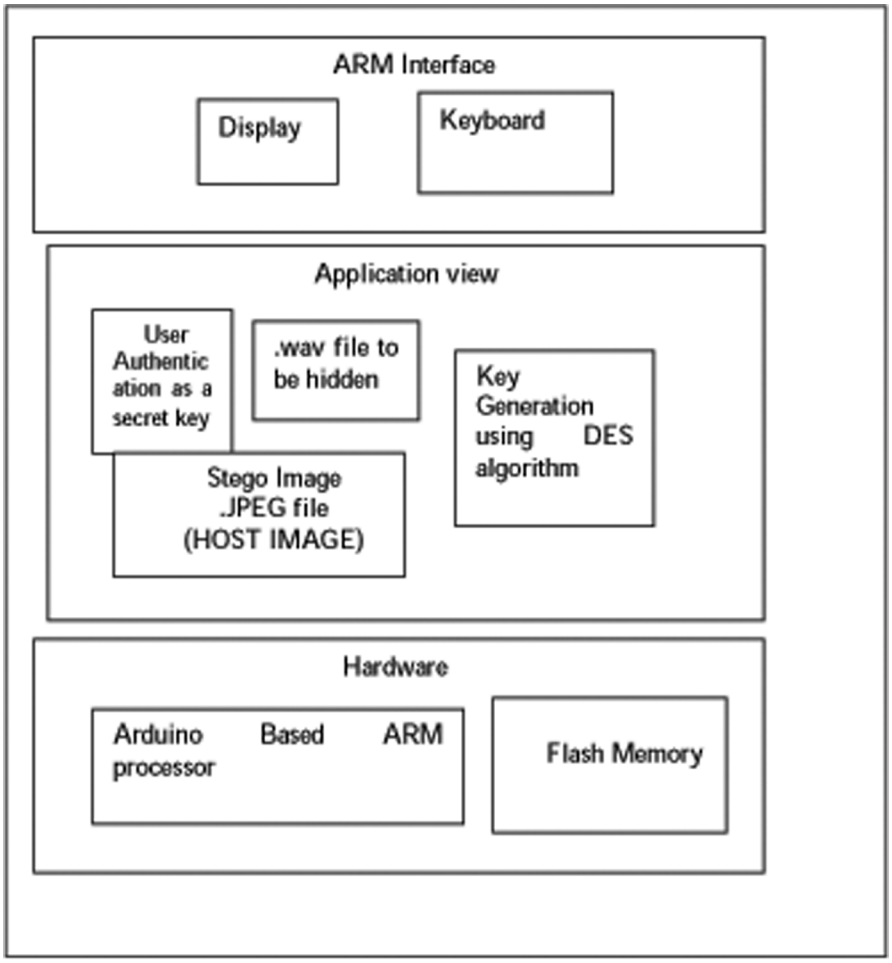

Figure 6: Architecture of the proposed Framework

other part of information is to be processed image signal to be quantized level in frequency domain, where all frequency components to be processed in .JPEG file to place .wav file binary format to be emcoded into image file.

5. SUMMARY

In this section, authors point out several techniques and application to supply audio or image information in host image where researchers specified ranges starting from 1 KB to 10 KB image details to be hidden into host image of 100KB.

As discussed so far, current application focus on how to hide image details into image through steganography methods.

Here lot of research has been done on hiding image into host audio so far. Since tremendous research increase in this area. Hence authors are ready to take challenge of loading .wav file into .jpeg image file as well as maintaining same quality as host image sent and receive at destination without affect the inside image details.

6. CONCLUSION AND FUTURE DIRECTION

In the paper presents an framework for hiding audio file on host image, by integrating ARM controller with Arduino based communication technologies and proposes architecture of software converter of Stego-image to ensure that a .wav file stay hidden in the .jpeg file as a host image that to protected from being

misused even if it is attacked . These updated frameworks might be used in low power devices like Arduino and ARM board [4][6] and produce suitable hiding image to realize smart living application in next 5G generation.

REFERENCES

[1] Michael Raggo, Chet Hosmer.,"Data Hiding- Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols", Published Book in 2013 Elsevier.

[2] Ya-Fen Chang, et al., paper titled., "An intelligent context-aware communication system for one single autonomic region to realize smart living", published in Elsevier, Information Fusion 21 (2015), pp. 57–67.

[3] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal Vol. 35, No. 3&4. MIT Media Lab, pp. 313-336, 1996.

[4] P.Sanyasi Naidu, J Gurrala "Investigation and analysis of Location Based Authentication and Security Services of Wireless LAN's and Mobile Devices", published in IJCA ,Volume 146,Number 8 (ISBN: 973-93-80893-84-7, July2016.

[5] Neil F. Johnson,Sushil Jajodia., "Exploring Steganography: Seeing the Unseen", published in IEEE, 1998, pp 26-43.

[6] L. Scott, D. Denning, "Geo-encryption: Using GPS to Enhance Data Security", GPS World, April 1 2003.

[7] Dorothy E.Denning and Peter F.MacDoran ., "Location based authentication: Grounding Cyberspace for Better Security", Elsevier Science Ltd. Copyright 1996.

[8] http://playground.arduino.cc/Main/InterfacingWithHardware#Communication.