Visvesvaraya Technological University, Belagavi.

PROJECT REPORT

on

"A METHOD OF MOVIE PIRACY REDUCTION USING STEGANOGRAPHY TECHNIQUE"

Project Report submitted in partial fulfillment of the requirement for theaward of the degree of

Bachelor of Engineering

in

Electronics and Communication Engineering

For the academic year 2019-20

Submitted by

1CR15EC221	SurajBabu M
1CR16EC141	Saba Hussain
1CR16EC159	Shivani A
1CR16EC188	Vidhya Judith

Under the guidance of

Mr. Sunil Kumar K H

Assosiate Professor

Department of ECE

CMRIT,Bengaluru

CELEBRATING 25 YEARS CMR INSTITUTE OF TECHNOLOGY

Department of Electronics and Communication Engineering

CMR Institute of Technology, Bengaluru – 560 037

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CMR INSTITUTE OF TECHNOLOGY

CERTIFICATE

This is to Certify that the dissertation work **"A Method of Movie Piracy Reduction using Steganography Technique"**carried out bySurajBabu M, Saba Hussain, Shivani A, Vidhya Judith USN: 1CR15EC221, 1CR16EC141, 1CR16EC159, 1CR16EC188,bonafide students of **CMRIT** in partial fulfillment for the award of**Bachelor of Engineering**in**Electronics and Communication Engineering**of the**Visvesvaraya Technological University, Belagavi,**during the academic year **2019-20**. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the departmental library. Theproject report has been approved as it satisfies the academic requirements in respect of Project work prescribed for the said degree.

Signature of Guide	Signature of HOD	Signature of Principal
Mr Sunil Kumar K H Associate Professor, Dept. of ECE., CMRIT,Bengaluru.	Dr. R. Elumalai Head of the Department, Dept. of ECE., CMRIT,Bengaluru.	Dr. Sanjay Jain Principal, CMRIT, Bengaluru.

External Viva

Name of Examiners — Signature & date

1.

2

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose consistent guidance and encouragement crowned our efforts with success.

We consider it as our privilege to express the gratitude to all those who guided in the completion of the project.

We express our gratitude to Principal, **Dr. Sanjay Jain,** for having provided us the golden opportunity to undertake this project work in their esteemed organization.

We sincerely thank **Dr. R. Elumalai,**HOD**,** Department of Electronics and Communication Engineering, CMR Institute of Technology for the immense support given to us.

We express our gratitude to our project guide**Mr. Sunil Kumar K H**, Associate Professor**,** for his support, guidance and suggestions throughout the project work.

Last but not the least, heartful thanks to our parents and friends for their support.

Above all, we thank the Lord Almighty for His grace on us to succeed in this endeavor.

Table of Contents

CHAPTER 1 1

INTRODUCTION **ERROR! BOOKMARK NOT DEFINED.**

CHAPTER 2 2

LITERATURE SURVEY 2

CHAPTER 3 6

PROBLEM STATEMENT **ERROR! BOOKMARK NOT DEFINED.**

CHAPTER 4 **ERROR! BOOKMARK NOT DEFINED.**

METHODOLOGY **ERROR! BOOKMARK NOT DEFINED.**

CHAPTER 5 11

HARDWARE **ERROR! BOOKMARK NOT DEFINED.**

5.1 Hardware Details 8

5.1.1 Arduino 8

5.1.2 IR LED's 8

5.1.3 GPS 9

5.1.4 GSM 9

5.1.5 Relay 10

5.1.6 ARM-7 Module 10

CHAPTER 6 11

SOFTWARE 11

6.1 Matlab 11

6.2 GUIDE 12

6.3 Video Steganography 13

6.4 Video Steganography using LSB 15

6.5 LSB 17

6.6 Color Detection Algorithm 20

6.7 Masking and Filtering 21

CHAPTER 7 22

FLOWCHARTS 22

7.1 Encryption 22

7.2 Decryption 24

CHAPTER 8 26

RESULTS 26

CHAPTER 9 28

APPLICATIONS AND ADVANTAGES 28

CHAPTER 10 29

CONCLUTION AND SCOPE FOR FUTURE WORK 29

REFERENCES 30

APPENDIX A 31

List of Figures

Figure 5.1 Block Diagram of Movie Piracy System 7

Figure 5.2 LED 9

Figure 6.1 The sender side image steganography system architecture 15

Figure 6.2 The receiver side image steganography system architecture 16Figure 6.3 LSB Video Steganography19Figure 7.1 Encryption Main Module Flowchart 22Figure 7.2 Encryption Function Flowchart 23Figure 7.3 Decryption Main Module Flowchart 24Figure 7.4 Decryption Function Flowchart 25

Figure 8.1 Password authentication 26

Figure 8.2 Error Message27

Chapter1

INTRODUCTION

Cinema is a major entertainment for people in today's life. To entertain people, a lot of investment is put on cinemas by the film makers. Their effort is being destroyed by few people by pirating the cinema content. They do it by capturing the video in mobile camera and upload it to websites or sell it to people and this goes on. India has recently introduced some digital rights management (DRM) provisions to the Indian copyright law with the objective of providing "adequate" protection for copyrighted material in the online digital environment. Film industry was one of the biggest lobbying groups behind the new DRM provisions in India, and the industry has been consistently trying to portray online piracy as a major threat. The Indian film industry also extensively uses John Doe orders from the high court's in India to prevent the access of Internet users to websites suspected to be hosting pirated material. Thus we explore two questions in the context of the new DRM provisions in India: (1) Is online piracy a threat to the Indian film industry? and (2) Are the present measures taken by the film industry the optimal measures for addressing the issue of online piracy? Based on data from an extensive empirical survey conducted in India, the claims of the industry that online piracy is at a substantial level in India. The Internet usage related data in India also support the findings from the empirical survey.

In this study, a technical method is used in order to avoid false recording of video in theaters. Mainly piracy in movies happens by capturing the movie played in theatre with a camera, processing the video and bringing out a better image. To reduce the losses that occur due to piracy, we use infrared radiations, as IR rays have the property of being detected by cameras, but not by human eye. So we use this property of infrared to prevent the camera from capturing the film. As direct infrared is dangerous to human beings, we use near infrared range, in the upper and lower side of the bandwidth. An invisible light is projected from the screen to the whole audience that falls on the camera lens which is sensitive to infra-red light rays which alters the capturing functions of the camera. So while projecting the picture shown in theatres, we send original visible rays that help us see in theatres as movies along with a mix of other invisible light beams. The innovation in our project lies in the design, where we use IR burst transmitter which is inbuilt within the projector which sends high intensity of infrared rays along with the movie projection. This whole infrared blaster and projector acts as one whole system in sync. As we focus on prevention of piracy in cine field, it is highly necessary that the system operates along with the movie played. Hence integrating the IR system with the projector helps us achieve this objective. So in proposed project we are planning to develop an anti-piracy system for film industries using modulo operator based steganography technique in MATLAB and to design an IR based screen to disable mobile recording and also a GSM based immediate alert is sent to concerned authority to alert about piracy position using GPS.Video steganography performs data hiding. The process of encryption and decryption is performed using this concept. Video steganography hides the secret key that is used for password authentication. All the secret data is hidden inside the frames of the video using Matlab software.

Chapter 2

LITERATURE SURVEY

2.1 Movie piracy tracking using temporal psychovisual modulation YuanchunChen ;GuangtaoZhai ; ZhongpaiGao ; KeGu ; Wenjun Zhang ; Menghan Hu ; Jing Liu2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)

This paper presents a new method to defeat camcorder piracy and realize content protection in the theater using a new paradigm of information display technology, called Temporal Psychovisual Modulation (TPVM), which utilizes the differences between the human-eye perception and digital camera image forming to stack an invisible pattern on digital screen and projector. The images formed in human vision are continuous integration of the light field, while discrete sampling is used in digital video acquisition which has "blackout" period in each sampling cycle. Based on this difference, we can decompose a movie into a set of display frames with specific patterns and broadcast them out at high speed so that the audience cannot notice any disturbance, while the video frames captured by camcorder will contain highly objectionable artifacts (i.e., the patterns). The pattern embedded in the movies can also serves as tracking information to reveal the one responsibility for the camcorder piracy.

2.2 Advanced Video Watermarking Approach based on Convolutional Encoding HichamTribak, Youssef Zaz, HouriaKelkoulAbdelmalekEssaadi University, Faculty of science.

In the objective to fight against movies copyright infringement and cinema piracy, this paper proposes, a video frame analysis based treatable system, able to keep track of unpermitted shared multimedia files. The massive expansion of internet network beside the permanent accessibility of online data storage resource has tremendously facilitated fraudsters task in terms of using illegally cinematic productions (Films, documentaries, animation and cartoons). The main idea of our contribution is represented firstly by watermarking technique; each authentic multimedia file is identified by a given ID (which represent information's about the movie, for instance, time and date of projection), This ID is hidden (so as to protect purchaser privacy) using RSA encryption method, secondly, an automatic copyright checker is designated to extract the embedded ID and deduce the authenticity of the queried copy. Since multimedia files undergo video, image and audio

compressions, the evoked ID is exposed to a substantial deterioration. In order to overcome this shortcoming, frame watermarking phase is reinforced by a convolutional encoding procedure. On the other hand, ID extraction is conducted via Viterbi decoding, characterized by its high efficiency in retrieving the original data in case of binary errors.

2.3 DLP based anti-piracy display system ZhongpaiGao ;GuangtaoZhai ; Xiaolin Wu ; Xiongkuo Min ; Cheng Zhi 2014 IEEE Visual Communications and Image Processing Conference

Camcorder piracy has great impact on the movie industry. Although there are many methods to prevent recording in theatre, no recognized technology satisfies the need of defeating camcorder piracy as well as having no effect on the audience. This paper presents a new projector display technique to defeat camcorder piracy in the theatre using a new paradigm of information display technology, called temporal psychovisual modulation (TPVM). TPVM exploits the difference in image formation mechanisms of human eyes and imaging sensors. The images formed in human vision is continuous integration of the light field while discrete sampling is used in digital video acquisition which has "blackout" period in each sampling cycle. Based on this difference, we can decompose a movie into a set of display frames and broadcast them out at high speed so that the audience can not notice any disturbance, while the video frames captured by camcorder will contain highly objectionable artifacts. The proposed prototype system built on the platform of DLP LightCrafter 4500 serves as a proof-of-concept of anti-piracy system.

2.4 Watermarked Movie Soundtrack Finds the Position of the Camcorder in a Theater YutaNakashima ;Ryuki Tachibana ; Noboru BabaguchiIEEE Transactions on Multimedia

In recent years, the problem of camcorder piracy in theaters has become more serious due to technical advances in camcorders. In this paper, as a new deterrent to camcorder piracy, we propose a system for estimating the recording position from which a camcorder recording is made. The system is based on spread-spectrum audio watermarking for the multichannel movie soundtrack. It utilizes a stochastic model of the detection strength, which is calculated in the watermark detection process. Our experimental results show that the system estimates recording positions in an actual theater with a mean estimation error of 0.44 m. The results of our MUSHRA subjective listening tests show the method does not significantly spoil the subjective acoustic quality

of the soundtrack. These results indicate that the proposed system is applicable for practical uses.

2.5 Comparatives study of Various Techniques against Camcorder Piracy in Theater Nilesh Kumar Dubey ; HardikModi 2018 4th International Conference on Computing Communication and Automation (ICCCA)

For the long decay the cinema industries are suffering from camcorder piracy due to that every year cinema industries are losing billions of dollars. Most important cause of piracy is camcorder piracy, in which pirates record the movie during playback in theater. DCI (Digital cinema Initiative) given many rule and regulation to protect from piracy but still it is increasing, reason is there is no concrete technical solution exist. In this paper various techniques that can be opted in future for fighting against the piracy is taken. There are two types of solution exist for the overcoming the piracy problem one is through deterring the pirate and other is not to let it be captured through camera. Watermarking is one way to deter pirates and watermark can be embedded in frames or audio of videos. Modulations techniques can be used to generate flicker that cannot be detected by HVS but create noise in camcorder recorded videos.

2.6 A Survey on Reduction of Movie Piracy using Automated Infrared System

A.K.Veeraraghavan ,S.ShreyasRamachandran ,V.Kaviarasan

In recent times, piracy has been increasing rapidly and only in the last year, it has increased from 65% to 78%. Piracy is a big network.. Hence this yields us a mammoth opportunity to see a resolution for this big a problem and increase the attendance of audience in theatres thus diminishing the losses created. In our project, we use infrared blasters which give IR rays which are easily detectable by digital cameras. These IR blasters are inbuilt within the projector circuit, giving out IR light beams along with the visible rays of the movie projection. It is connected to a microcontroller which helps in altering the radiations frequency and wavelength characteristics. This is mainly done to neglect the use of infrared filters by a person while capturing the film using a camera. As infrared has a large bandwidth, a person would have to use a large number of filters to neglect the effect of IR, which is not feasible or possible.

Chapter 3

PROBLEM STATEMENT

Cinema is a major entertainment for people in today's life. To entertain people a lot of investment is put on cinemas by the film makers. Their effort is being ruined by few people by pirating the cinema content. They do it by capturing the upload it to websites or sell it to people and this goes on.

Film piracy has been the bane of the film industry for about 5 - 10 years now, slowly but surely it is starting to slowly deteriorate the way they sale and make their films. This effect is surely bad, it means a rise in prices, a fall in quality and an abundance of crimes committed by thousands of people.

Technologies like electronic device jammers which jam the operation and functioning of the device itself. This in a way prevents the camera from capturing videos and pictures. However, in places where usages of other devices like cell phones, laptops, etc are necessary, this system fails to give the suitable environment. In recent times, even infrared rays are being used to prevent taking videos. This system uses infrared projectors at 4 corners of the room, releasing IR rays, which prevents capturing of photos and videos.

Chapter 4

METHODOLOGY

In our project, we use the property of light which is not visible to naked eyes, but the one's cameras can pick up, only visible light can be detected by human eyes. But light rays like IR and UV cannot be seen by our eyes, but cameras easily pick images of them. So while projecting the picture shows in theatres, we send original visible rays that help us see in theatres as movies along with a mix of other invisible light beams. The innovation in our project lies in the design, where we use IR burst a transmitter which is inbuilt within the projector which sends high intensity of infrared rays along with the movie projection. This whole infrared blaster and projector acts as one whole system in sync. Thus, unlike the previous case where if the IR system may or may not be operational. As we focus on prevention of piracy in cine field, it is highly necessary that the system operates along with the movie played. Hence integrating the IR system with the projector helps us achieve this objective.

Furthermore, we use LSB video steganography to encrypt a password in the movie before transmitting it to the theatres. The theatre owner has to enter the correct password and the system verifies the password and plays the movie.

There are 3 objectives in proposed model

1. Designing Infra red based Transmitter Screen to avoid mobile recording

2. Steganography Technique to hide secret key to avoid piracy.

3. GSM based immediate alert to concerned authority to alert about Piracy Position using GPS.

Chapter 5

HARDWARE

The block diagram of the movie piracy system using video steganography is shown in the Fig 4.1. ArduinoUno, is the heart of the system. It controls the majority operations of the system using Atmega microcontroller. Arduino is scripted by the Arduino IDE software. Video steganography is done using Matlab software. The system works in the following way.

On switching on the Arduino Uno micro controller the keypad gets activated for the password to be entered. If the password is verified the controller output is given to the driver through the buffer which provides impedance matching between them.

Since the output from the micro controller is low, driver amplifies the signal and actuates the relays to control the IR LEDs. The signals that are transmitted by IR LEDs placed behind and also along the perimeter of the screen are emitted towards the audience. So this invisible light disturbs the acquisition functions of the camera.

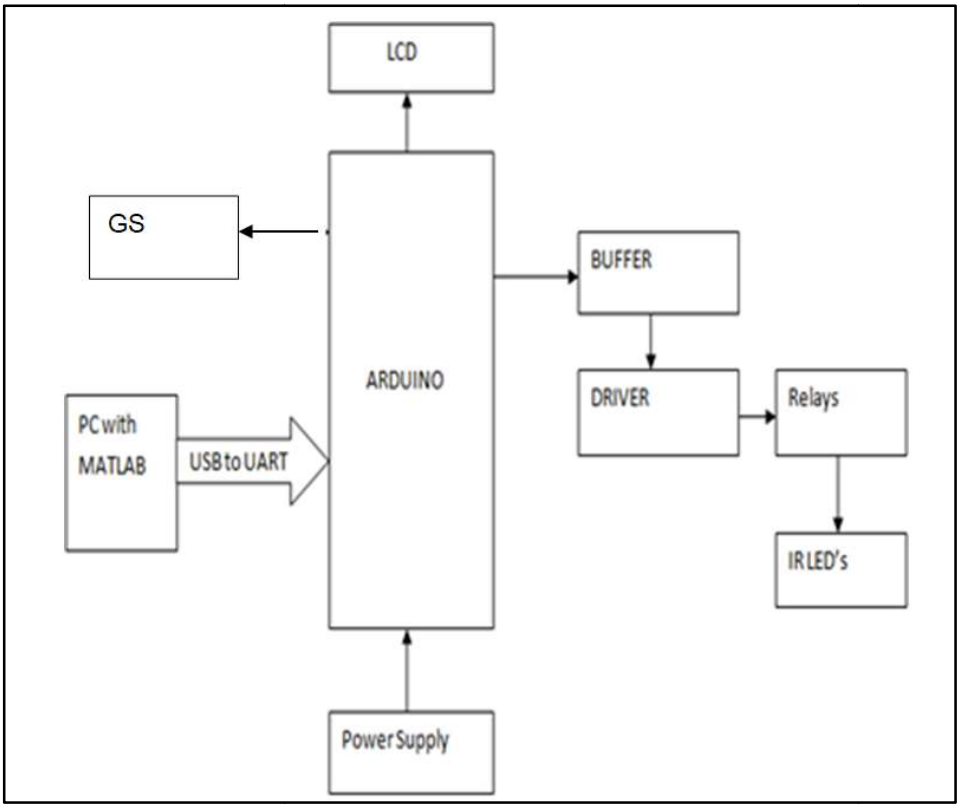

Fig 5.1: Block Diagram of Movie Piracy System

On placing IR LEDs behind and around the screen in the cinema theatre, the video playing on the screen becomes blur or scrambled. Therefore, the audience will be able to watch the movie without any disturbance but since the camcorders are sensitive to IR light the recorded content becomes blur or unfit to watch.

5.1 Hardware Details

The various hardware components used in the project are listed below:

- Arduino
- IR Transmitter
- Power supply components
- LCD
- Relay
- GSM

5.1.1 Arduino

The Arduino Uno is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started. The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB- to-serial converter.

5.1.2 IR LED's

IR Transmitter is used to control any device wireless means remotely. The IR LED & photo transistor both of them have their sensitive area on their tip and their anode lead is longer than the cathode. The IR LED works between 1.6V-3.3V. IR wavelength ranges between 750nm-2500nm.

The purpose of the transmitter is to transform the information we want to send into a signal that can be propagated by the channel. In the case of our wired copper channel, this means we want the information to be transformed into a modulated voltage level,

something like the pulse train. For a wireless channel, however, the transmitter needs to encode the information onto an EM wave that can be easily propagated.

The wavelengths of infrared lights have longer wavelengths than those visible to humans. This range of light is invisible to the human eye .It is very visible however to many times of cameras.

Theatre owners could place small infrared lights on their movie screens as shown in Fig 5.2. The lights would not disturb people watching the movie. It will however distort the recordings made by many types of cameras.

Fig 5.2 LED

5.1.3GPS (Global Positioning System)

A possible to precisely identify locations on earth by measuring distance from the satellites. This system uses MT 3318 GPS Receiver which contains high gain active patch antenna by cirocomm. The GPS receiver interfaced with microcontroller through the UART1 serial communication. The GPS receiver may track upto 51 satellites simultaneously. The GPS receiver is mounted on PCB along with the 3.3V voltage regulator, transmit, receive and power indication LED's. The GPS receiver output data is in the form of NMEA (National Marine Electronics Association) standard format. network of satellites that continuously transmit coded information, which makes it.

5.1.4GSM (Modem Global System for Mobile communication)

A GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. When a GSM modem is connected to a computer, this allows the computer to use the GSM modem to

communicate over the mobile network. While these GSM modems are most frequently used to provide mobile internet connectivity, many of them can also be used for sending and receiving SMS and MMS messages. A GSM modem can be a dedicated modem device with a serial, USB or Bluetooth connection, or it can be a mobile phone that provides GSM modem capabilities.

For the purpose of this document, the term GSM modem is used as a generic term to refer to any modem that supports one or more of the protocols in the GSM evolutionary family, including the 2.5G technologies GPRS and EDGE, as well as the 3G technologies WCDMA, UMTS, HSDPA and HSUPA. A GSM modem exposes an interface that allows applications such as SMS to send and receive messages over the modem interface. The mobile operator charges for this message sending and receiving as if it was performed directly on a mobile phone. To perform these tasks, a GSM modem must support an "extended AT command set" for sending/receiving SMS messages, as defined in the ETSI GSM 07.05 and 3GPP TS27.005 specifications.

5.1.5Relay

Relays are electro mechanical switches which are used to control several IR LEDs. It works on electromagnetic phenomenon. It switches between different loads. It switches between the terminals depending on the potential difference. They can be driven by a low power signal. It takes 12V for its operation.

5.1.6ARM-7 Module

In our system we are using LPC2148. It acts as the major controller unit of the system. Input from various units like IR sensor, Engine switch is given to this unit on which it process according to the programming and gives output to the relay driver circuit, and to GSM module It needs 3.3V to drive the ARM7 module.

Chapter 6

SOFTWARE

6.1 Matlab

The name Matlab stands for MATrixLABoratory. Matlab was written originally to provide easy access to matrix software developed by the LINPACK (linear system package) and EISPACK (Eigen system package) projects.

Matlab is a high-performance language for technical computing. It integrates computation, visualization, and programming environment. Furthermore, Matlab is a modern programming language environment: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming. These factors make Matlab an excellent tool for teaching and research.

It has powerful built-in routines that enable a very wide variety of computations. It also has easy to use graphics commands that make the visualization of results immediately available. Specific applications are collected in packages referred to as toolbox. There are toolboxes for signal processing, symbolic computation, control theory, simulation, optimization, and several other fields of applied science and engineering.

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. It uses the L-shaped membrane logo. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, and FORTRAN. Using MATLAB, we can analyze data, develop algorithms, and create models and applications. The language, tools, and built-in math functions enable us to explore multiple approaches and reach a solution faster than with spreadsheets or traditional programming languages, such as C/C++ or Java™.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics.

We can use MATLAB for a range of applications, including signal processing and communications, image and video processing, control systems, test and measurement, computational finance, and computational biology.

Cleve Moler, the chairman of the computer science department at the University of New Mexico, started developing MATLAB in the late 1970s. He designed it to give his students access to LINPACK and EISPACK without them having to learn Fortran. It soon spread to other universities and found a strong audience within the applied mathematics community. Jack Little, an engineer, was exposed to it during a visit Moler made to Stanford University in 1983. Recognizing its commercial potential, he joined with Moler and Steve Bangert. They rewrote MATLAB in C and founded MathWorks in 1984 to continue its development.

Matlab has many advantages compared to conventional computer languages (e.g., C, Fortran) for solving technical problems. Matlab is an interactive system whose basic data element is an array that does not require dimensioning. The software package has been commercially available since 1984 and is now considered as a standard tool at most universities and industries worldwide.

The MATLAB application is built around the MATLAB language, and most use of MATLAB involves typing MATLAB code into the Command Window (as an interactive mathematical shell), or executing text files containing MATLAB code, including scripts and/or function.

6.2 GUIDE

GUIs (also known as graphical user interfaces or UIs) provide point-and-click control of software applications, eliminating the need to learn a language or type commands in order to run the application.

MATLAB apps are self-contained MATLAB programs with GUI front ends that automate a task or calculation. The GUI typically contains controls such as menus, toolbars, buttons, and sliders. Many MATLAB products, such as Curve Fitting Toolbox, Signal Processing Toolbox, and Control System Toolbox, include apps with custom user interfaces. You can also create your own custom apps, including their corresponding UIs, for others to use.

MATLAB supports developing applications with graphical user interface features. MATLAB includes GUIDE (GUI development environment) for graphically designing GUIs. It also has tightly integrated graph-plotting features. For example the function plot can be used to produce a graph from two vectors x and y.

To create GUI in MATLAB follow the steps listed below.

1. Click on GUIDE button on toolbar in MATLAB launch pad.
2. Make your choice of the type of GUI you need.
3. Make buttons and/or menus from the tools in GUIDE.
4. Double click on menu that is created in grey area of the GUIDE, property manager will open.

6.3 Video Steganography

6.3.1 Embedding of secret data

1) Pre-processing:

- The target string length should be multiple of four otherwise some less used special character is concatenated at the end to make string length as multiple of four.
- For preprocessing each character of target string converted to their corresponding ASCII as well as 7 bit binary.
- Then every 4 bits are cut and converted into hexadecimal digits. Let the string is "Secret" whose length is 6. "`" is added to make its length multiple of four. So the string becomes "Secret``".
- The ASCII of the characters of this target string is 83, 101, 99, and 114 and …, respectively and their corresponding 7 bit binary is 1010011 1100101 1100011 1110010…. After concatenating it becomes 10100111100101110001111110010…
- Then the hexadecimal digits are A 7 9 7 1 F 2 …

2) Embedding using modulo operator:

- Now these hexadecimal digits are embedded into the cover video by adjusting amplitude values of the target samples. The amplitudes of cover video are divided by 16. Then the remainders are compared with the target hexadecimal digits and the amplitudes of the cover video are adjusted in such a way so that the remainder is equal with the target hexadecimal digits.
- The boundary values for amplitudes i.e. 32760 – 32767 and 0 – 8 are treated differently to avoid huge change. Suppose the cover amplitude value is 32764 and we want to insert 1 as target octal digit and if the proposed technique is followed then according to forward difference it becomes 32769 which are not within the range 0 to 32767. So in this case the backward differences are considered. That means if the modified amplitude value is less than 0 or greater than 32767 by either considering forward or backward differences, then the cover amplitude value is replaced by the other difference i.e. backward and forward differences.
- The 16 bits string length of secret string is stored in first 16 samples by using standard LSB technique for extraction at receiver side.

6.3.2 Extraction of secret data:

For extracting the target data from stegovideo at the receiver side first the string length is extracted from first 16 amplitudes by standard LSB extraction technique. Then the following steps are to be followed:

1) Extraction using modulo operator: At the receiver side the affected (where the data is hidden) amplitude values are divided by 16 and the remainders of this division are hidden hexadecimal digits. Now this is send to the post-processing technique to get the original target text.

2) Post-processing: Now the resultant hexadecimal digits are converted to their 4 bit binary equivalent. Each of these 4 bits is concatenated to form a binary string. Then every 7 bits are cut and converted to their corresponding decimal equivalent. The characters of these ASCII values are concatenated as per the string length to get the original target string. Change properties according to requirement and change the code if needed.

6.4 Video Steganography using LSB

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

In all of these methods, the basic principle of steganography is that a secret message is to be embedded in another cover object or cover image as shown in Fig 6.1 which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used. The decryption process is shown in Fig 6.2.

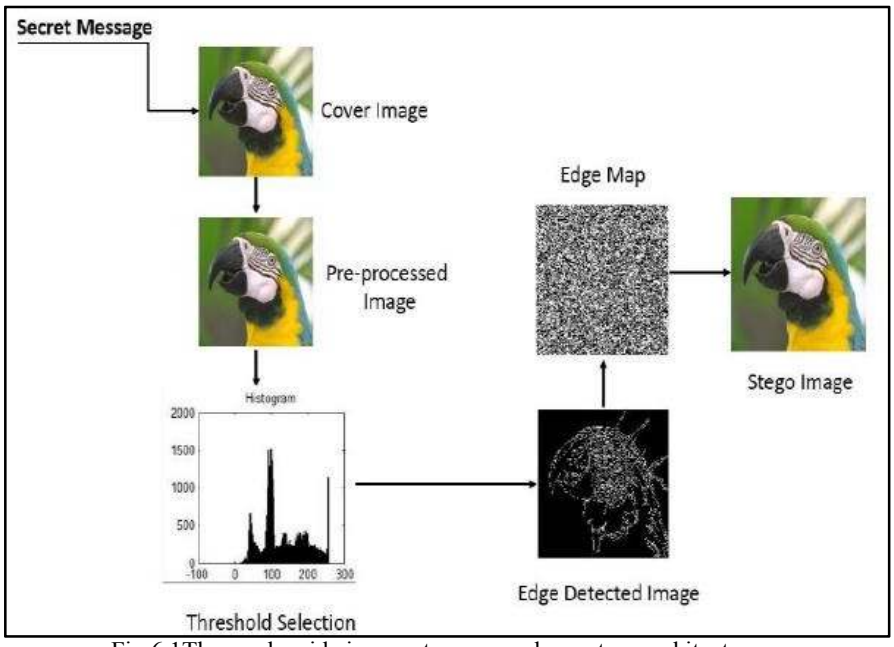

Fig 6.1The sender side image steganography system architecture

Fig 6.1 shows sender side image steganography involving various steps such as:

- Image pre-processing
- Threshold selection
- Secret messagehiding or encoding
- Decoding of the secret message

Each element in the steganography is explained as follows:

- COVER IMAGE: Image in which information is hidden. The information can be of any size. Higher the image quality higher is the amount of information that can be hidden. Cover image is input to the process.
- SECRET MESSAGE: Information which has to be secretly stored for transfer to another person so that third person cannot read it. Length of secret message depends on edge and quality of the image. More the number of edges and quality of the image, more amount of information can be stored.
- PRE-PROCESSING: The process involves conversion of an RGB image to a HIS image.
- THRESHOLD SELECTION: The threshold value is returned by Canny Edge Detection algorithm. It identifies edges in the cover image. Based on the size of secret message, threshold is adjusted. If message is too long then high threshold value is selected so that message can be accomodated in the edges effectively.
- EDGE MAP: Edge map is used to represent vector fields in an image.
- EMBEDDING OF MESSAGE: Most of the steganographic technique uses LSB techniques. This technique is not that much efficient to perform data hiding. Hence 2-bit LSB technique is used to hide data into images efficiently.
- STEGO IMAGE: After embedding the secret information into the image, it is ready for transmission by the receiver. It can be transferred over the internet, e-mail. Stego image is similar to the original image. There is no loss in the quality of the image.

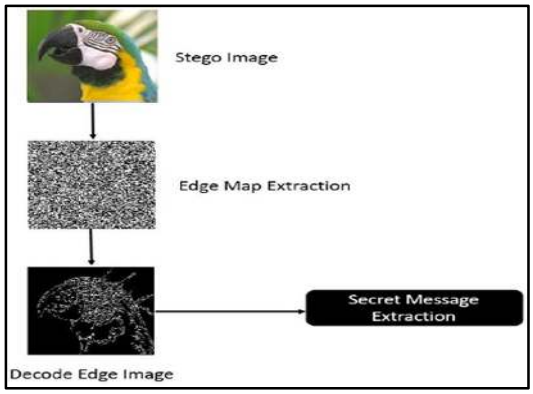

Fig 6.2 The receiver side image steganography system architecture

The receiver side decoding is shown in Fig 6.2. The process involves:

- After encoding the secret message into the image, receiver side decoder is required.

- Construction of decoder is similar to that of the encoder side algorithm.
- If there is a mismatch with any of the algorithm used on encoder side, decoding process cannot be successfully carried out.
- Fig 6.2 shows the reverse engineering approach in which stego image is converted and processed using Edge Map Extraction.

6.5LSB (Least Significant Bit)

Video file is generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. So, video steganography is nothing but a combination of image and audio steganography. So, the combined evaluations i.e., the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. A video stream consists of collection of frames and the secret data is embedded in these frames as payload.

LSB stands for Least Significant Bit. The idea behind LSB embedding is that if we change the last bit value of a pixel, there won't be much visible change in the color. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

6.5.1 Spatial Method

- In spatial method, the most common method used is LSB substitution method. Least significant bit (LSB) method is a common, simple approach to embedding information in a cover file.
- In steganography, LSB substitution method is used, i.e. since every image has three components (RGB).
- This pixel information is stored in encoded format in one byte.
- The first bits containing this information for every pixel can be modified to store the hidden text. For this, the preliminary condition is that the text to be stored has to be smaller or of equal size to the image used to hide the text.
- LSB based method is a spatial domain method. But this is vulnerable to cropping and noise.

- In this method, the MSB (most significant bits) of the message image to be hidden are stored in the LSB (least significant bits) of the image used as the cover image.
- It is known that the pixels in an image are stored in the form of bits. In a grayscale image, the intensity of each pixel is stored in 8 bits (1byte).
- Similarly for a color (RGB-red, green, blue) image, each pixel requires 24 bits (8bits for each layer).
- The Human visual system (HVS) cannot detect changes in the colour or intensity of a pixel when the LSB bit is modified. This is psycho-visual redundancy since this can be used as an advantage to store information in these bits and yet notice no major difference in the image.
- Algorithm of LSB method of steganography: There might be two different phases of LSB method, embedding phase and extracting phase.

Procedure:

Step 1: Extract all the pixels from the given image and store them in some array named (image array).

Step 2: Extract all the characters from the given text file (message file) and store it in the array called (message array).

Step 3: Retrieve the characters from the Stego key and store the mina array called Key array. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data.

Step 4: Take first pixel and characters from Key- array and place it in first component of pixel. If there are more characters in Key array, then place rest in the first component of next pixels.

Step 5: Place some terminating symbol to indicate end of the key.0 has been used as a terminating symbol in this algorithm.

Step 6: Place characters of message Array in each component of next pixels by replacing it.

Step 7: Repeat step 6 till all the characters has been embedded.

Step 8: Again place some terminating symbol to indicate the end of data.

Step 9: Obtained image will hide all the characters that input.

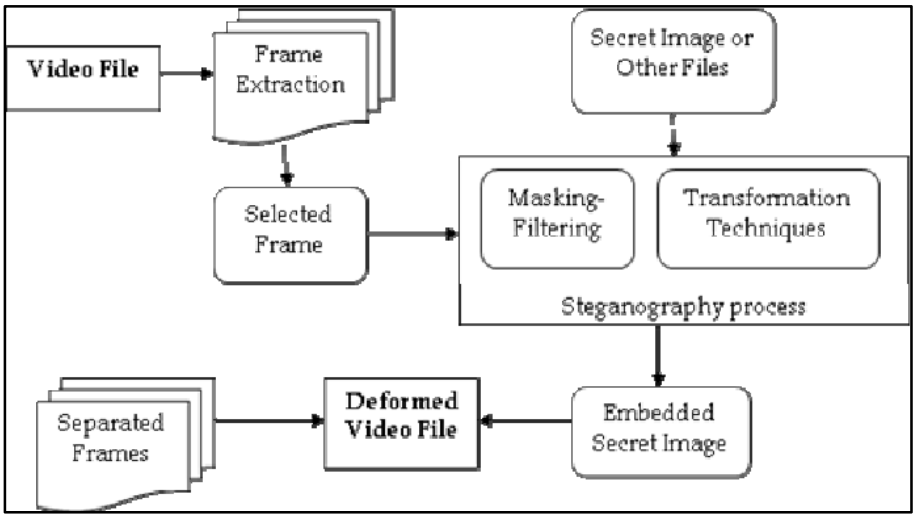

Fig 6.3 LSB Video Steganography

- The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence.
- Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.
- To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.
- When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.
- For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:
  (00100111 11101001 11001000)
  (00100111 11001000 11101001)
  (11001000 00100111 11101001)
- When the character A, which binary value equals 10000001, is inserted, the following grid results:
  (00100111 1110100011001000)
  (00100110 1100100011101000)
  (11001000 0010011111101001)

- In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size.
- The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS),so the message is effectively hidden. As you see, the least significant bit of third color is remained without any changes.
- It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as parity bit.

6.6 Color Detection Algorithm

Algorithm for Embedding Secret message in Multimedia file:

Step 1: Input cover Multimedia file, Secret message and Shared Secret key.

Step 2: Break the Multimedia file into frames.

Step 3: Convert the secret message into cipher text by using secrete key shared by sender and receiver.

Step 4: Find Least Significant Bits of each RGB pixels of the cover frame.

Step 5: Convert the encrypted text message into bits.

Step 6: Embed the bits of the secret message into bits of LSB of RGB pixels of the cover frame.

Step 7: Continue the process until the message fully embedded into multimedia file.

Step-8: Regenerate Multimedia file frames.

Algorithm for Extracting Secret message from Multimedia file:

Step 1: Input stego Multimedia file.

Step 2: Break the stego Multimedia file into frames.

Step 3: Find and retrieve the LSB bits of each RGB pixels of the stego frame.

Step 4: Continue the process until the message fully extracted from multimedia file.

Step 5: using shared key decrypt message to get original data.

Step 6: Reconstruct the secret information.

Step 7: Regenerate Multimedia file frame.

6.7 Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or gray scale images, take a different approach to hide a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies.

Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the noise level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

Chapter 7

FLOWCHARTS

7.1 Encryption

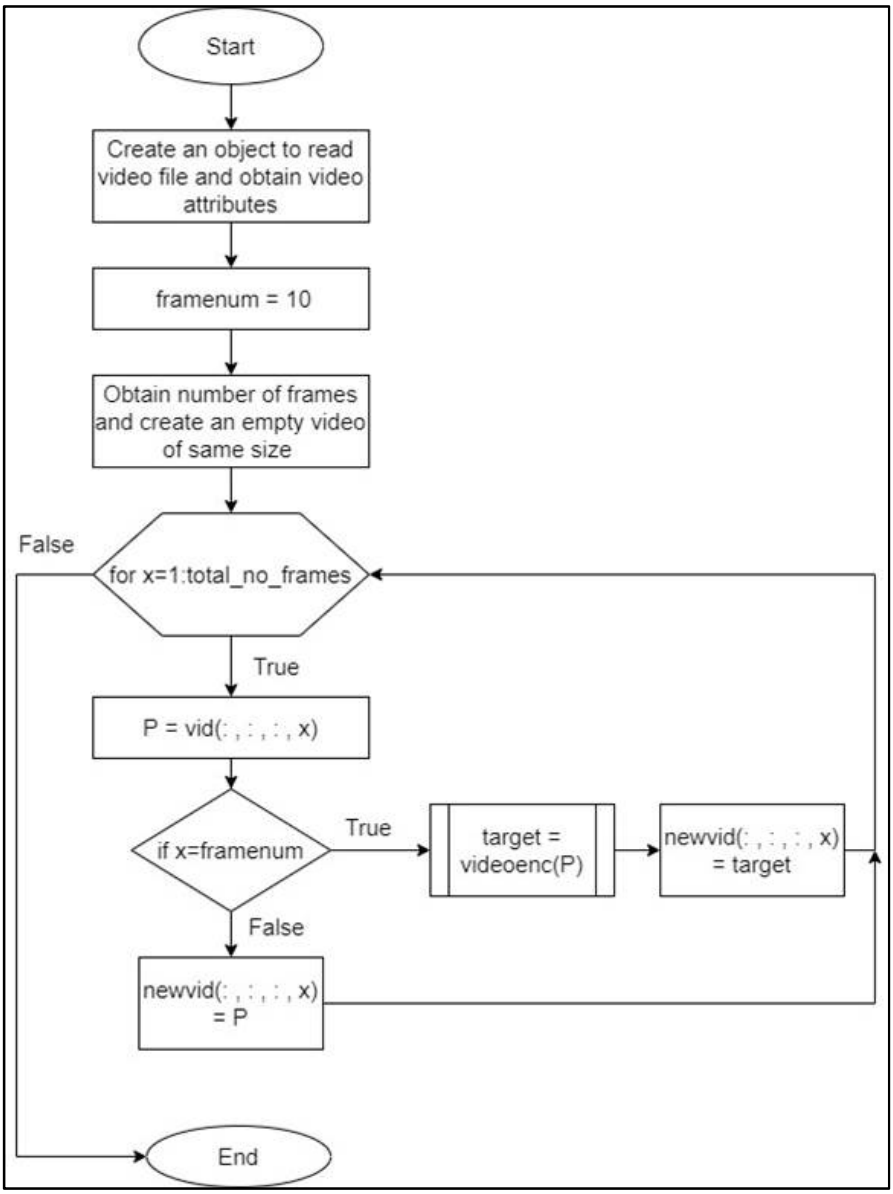

Fig 7.1 Encryption Main Module Flowchart

Step 1: The video data is read into an object to perform encryption such as height, width, number of frames, number of layers etc.

Step 2: A random frame is chosen to hide the secret key. Here frame 10 is chosen.

Step 3: A random 10 digit password is generated using the rand function.

Step 4: The selected frame is sent to a function where the password is hidden in the pixels of all the three layers of the frame. The function flowchart is shown below.

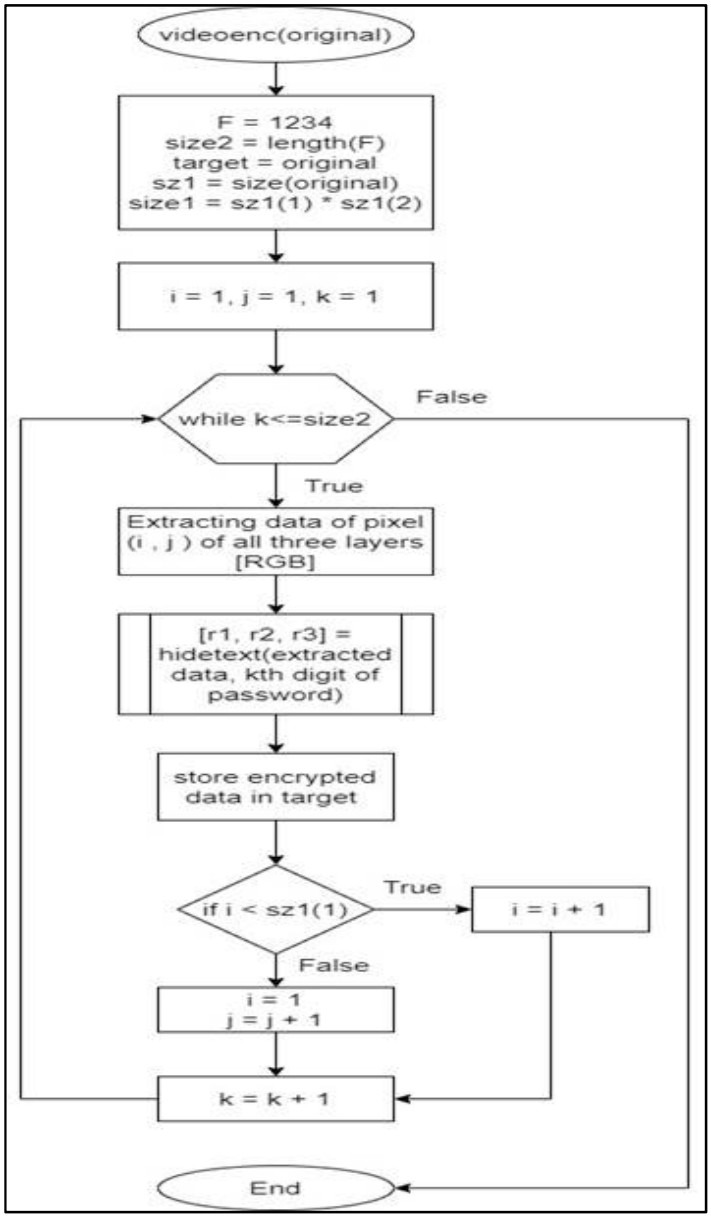

Fig 7.2 Encryption Function Flowchart

Step 5: Each digit of the generated password is converted into binary form and hidden in a particular pixel in the frame.

Step 6: After all the digits are hidden in the frame, the new video frame is sent back and the video is ready to transmit.

7.2 Decryption

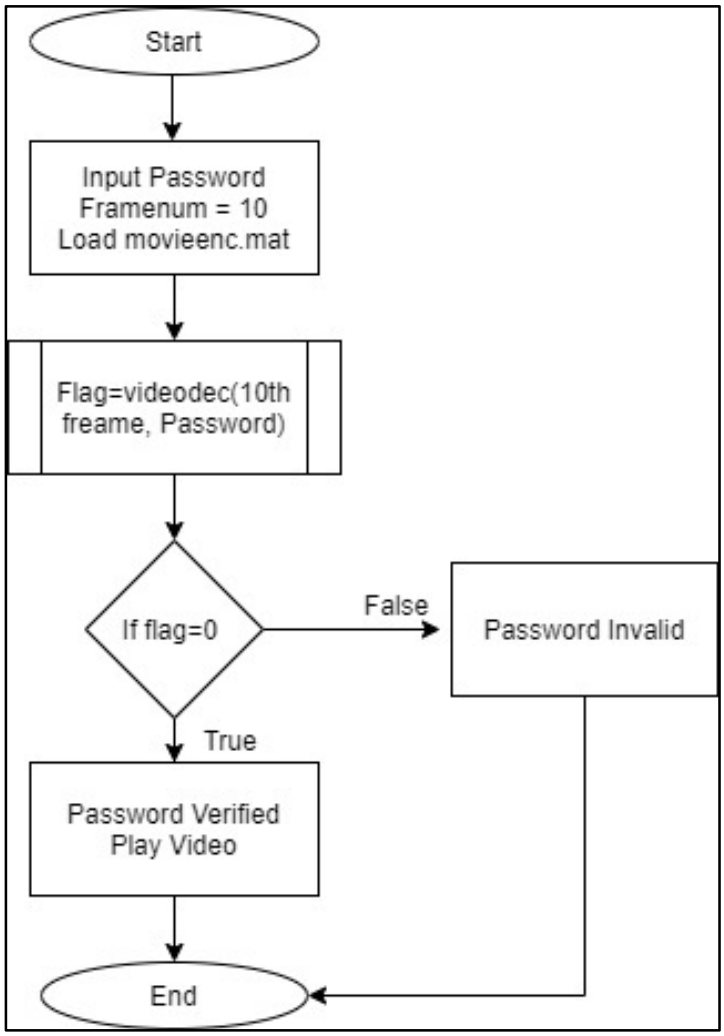

Fig 7.3 Decryption Main Module Flowchart

Step 1: Extract the frame where the secret key was encrypted and send the frame to the function for decryption.

Step 2: In the function, the secret key is extracted from the frame.

Step 3: The extracted key is compared with the key entered by the authorized person. If it matches then flag is set to 0, else the flag is set to 1 and the flag value is sent back to the main function.

Step 4: The video starts playing if flag is 0 and an error message is displayed if flag is 1.

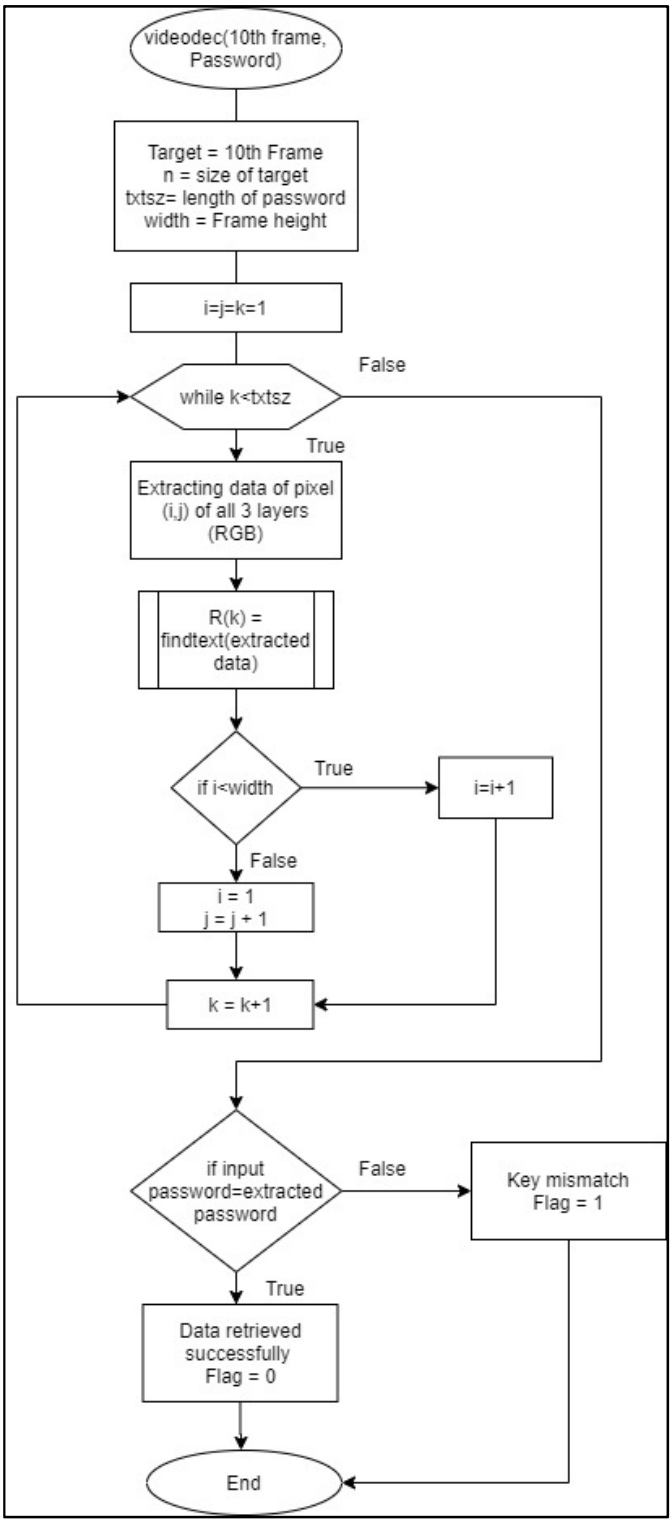

Fig 7.4 Decryption Function Flowchart

Chapter 8

RESULTS

If the password entered by the user matches with the data hidden in the video file, data is retrieved successfully as shown in Fig 8.1 and the video starts to play.

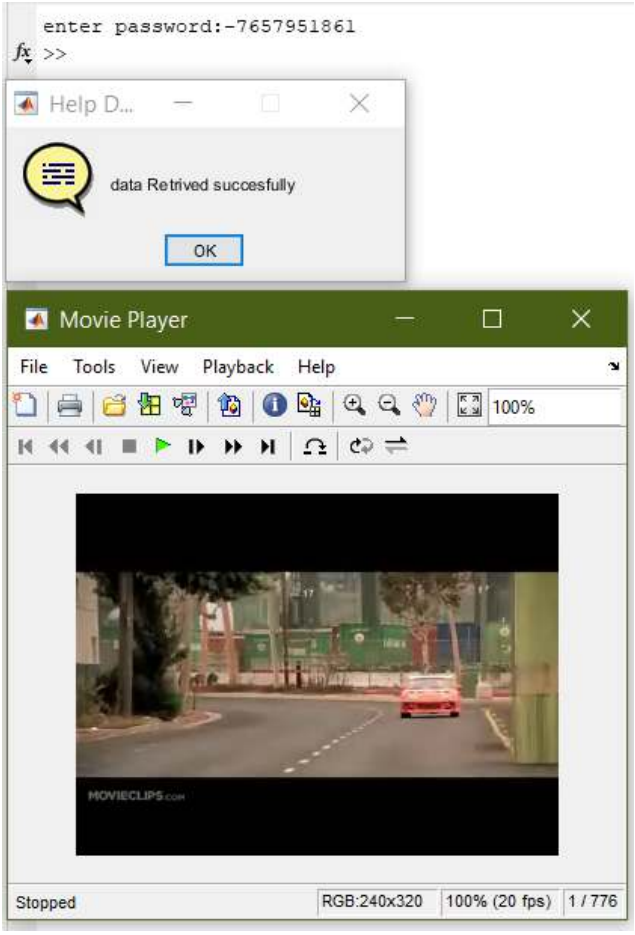

Fig 8.1: Password authentication

If a wrong entry of password is done password authentication fails as there is a mismatch of the password entered by the user as shown in Fig 8.2.

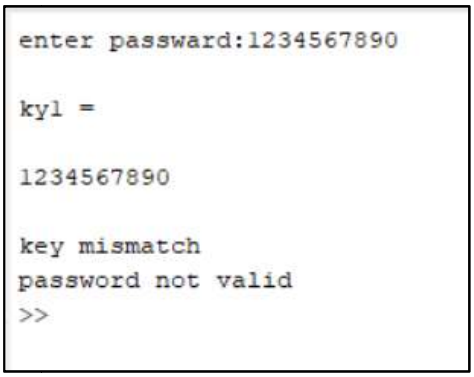

Fig 8.2 Error Message

Chapter 9

APPLICATIONS AND ADVANTAGES

This system increases the security level using these two methods at the theatre. The theatre owner is allowed to make the password entry. Once the password gets verified, the system considers the owner to be an authorized person and allows the movie to be played in the theatre. Consequently the IR LEDs placed along the screen gets turned on which do not cause any disturbance to the audience watching the movie. However they cause disturbance to the movie that is being captured by the cameras. This makes the captured content unfit to be uploaded to the websites.

On the other hand if any other person other than the theatre owner, or any person who doesn't have the information of the password tries to make a password entry, the system considers them as an unauthorized person. Hence does not allow the movie to be played in the theatre. An alert message is sent to the concerned person or to the theatre owner displaying that an unauthorized person tried to play the movie along with the place where it was tried to be played.

This system is easy to implement. It can be used for detecting any kind of piracy and to track online videos to avoid illegal leakage. This system will have low cost, low power consumption and high accuracy.

There can be various other applications of this system which requires high degree of piracy and security such as highly confidential conferences, meetings, research centers etc.

Chapter 10

CONCLUSION AND SCOPE FOR FUTURE WORK

The proposed system is implemented to provide a method to prevent illegal recording of movies in theatres using IR LEDs and concept of video steganography, thus targeting the grey market of piracy. The IR transmitters make the captured videos useless. The concept of video steganography hides the data inside number of frames of image so it is more secured.

Video steganography performs data hiding. The process of encryption and decryption is performed using this concept. Video steganography hides the secret key that is used for password authentication. All the secret data is hidden inside the frames of the video using Matlab software.

As a deterrent against camcorder piracy several watermarking techniques can be implemented. The main idea of this technique is to embed a imperceptible message(i.e, tracking information) into the movie. The message indicates the theatre to which the movie is being distributed, equipment on which it was shown, date and time of showing and information identifying the projectionist. If movies are pirated and illegal recordings are transmitted on Internet or via some other route, then the message can be extracted from the pirated movies to reveal the person or organization responsible for unauthorized release. As a forensic tool, tracking information gives the content, owner information to help manage the piracy problem and serves as the further surveillance and a deterrent to future piracy.

REFERENCES

[1] S. E. Siwek, The true cost of copyright industry piracy to the US economy. IPI Center for Technology Freedom, 2007.

[2] J. Dorning, Intellectual Property Theft: A Threat to U.S. Workers, Industries, and Our Economy. DPE Research Department, 2014.

[3] B. NEWS, "The fact and fiction of camcorder piracy," [Online]. Available: http://news.bbc.co.uk/2/hi/technology/6334913.stm, 2015.

[4] J. Bloom and C. Polyzois, "Watermarking to track motion picture theft," in Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on, vol. 1, Nov 2004, pp. 363–367 Vol.1.

[5] J. Haitsma and T. Kalker, "A watermarking scheme for digital cinema," in Image Processing, 2001. Proceedings. 2001 International Conference on, vol. 2, Oct 2001, pp. 487–489 vol.2.

[6] S. A. Taylor et al., "CCD and cmos imaging array technologies: technology review," UK: Xerox Research Centre Europe, 1998.

[7] G. Zhai and X. Wu, "Defeating camcorder piracy by temporal psychovisual modulation," J. Display Technol., vol. 10, no. 9, pp. 754– 757, Sep 2014. [Online]. Available: http://jdt.osa.org/abstract.cfm?URI=jdt-10-9-754

[8] A. DENSO, "QR Code essentials," 2011, retrieved 12 March 2013.

[9] X. Wu and G. Zhai, "Temporal psychovisual modulation: A new paradigm of information display [exploratory dsp]," IEEE Signal Pro- cessing Magazine, vol. 30, no. 1, pp. 136–141, Jan 2013.

[10] Z. Gao, G. Zhai, and J. Zhou, "Factorization algorithms for temporal psychovisual modulation display," IEEE Transactions on Multimedia, vol. 18, no. 4, pp. 614– 626, April 2016.

[11] C. Hu, G. Zhai, Z. Gao, and X. Min, "Information security display system based on spatial psychovisual modulation," in 2014 IEEE International Conference on Multimedia and Expo (ICME), July 2014, pp. 1–4.

[12] S. E. Siwek, The true cost of copyright industry piracy to the US economy. IPI Center for Technology Freedom, 2007.

APPENDIX A