International Journal of Research in Engineering, Science and Management
Volume-3, Issue-5, May-2020
www.ijresm.com | ISSN (Online): 2581-5792

Infra-Red Ciphered Infringement System Using MATLAB

Madhura Madhukar Hegde[1*], P. S. Ajay[2], G. Aishwarya[3], K. Harshitha[4], R. J. Kavitha[5]
[1,2,3,4]*Student, Department of Electronics and Communication Engineering, Sapthagiri College of Engineering, Bangalore, India*
[5]*Professor, Department of Electronics and Communication Engineering, Sapthagiri College of Engineering, Bangalore, India*
*Corresponding author: madhurahegde211@gmail.com

***Abstract*: Cinema is a major entertainment factor in the present era. Crores of money is spend on cinema by the film – producers every year. Their endeavor is being dismantled by culprits by pilfering the cinema content. Pilfering is carried out by recording the cinema with the help of camera and uploading it to the websites such as torrents.me, Rutracker, etc. In this proposed project, a technical method to prevent video recording in cinema theatre is presented. An invisible light is projected from the screen to the whole audience that falls on the cameras which are optically sensitive to infra-red light in turn disturbing the acquisition functions of any camera making an illegal recording in the theatre useless. This system employs two levels of authentication. Firstly, the smart card that is possessed by the respective theatre officer consists of information which is checked with preloaded reference information stored in the comparator. The signal form the comparator is passed to driver which turns on the infra-red led.**

***Keywords*: Anti-Piracy, IR Screens, LSB, RFID, Steganography.**

1. Introduction

The internet has been one of the most transformative and fast-growing technologies. Internet provides access to any copyrighted contents “Piracy means the unauthorized use of another's production, invention, or conception especially in infringement of a copyright”. Most of the times piracy happens in two ways: 1. Final copy of the movie content might get leaked before its release by the multiple teams working on them. 2. The movie is filmed inside the theatre using portable camera and then uploaded to the websites or sold in form of DVD’s at cheaper rates. Copyright law protects the value of creative work. Making unauthorized copies may subject one to civil and criminal liability. Unauthorized duplicates can expose one to common and criminal risk. Movie hall personnel are provided with night vision goggles that will help them spot any viewer attempting to capture a movie while screening. There are several ways to prevent these protection problems associated with the continuous image issues, one such approach to tackle the problem is steganography. Steganography is the way to dissimulate one document inside another to the degree that others cannot either discern or even perceive the value of the inserted object. Current practices promote the use of advanced picture logs to mask a computerized record containing a mystery message or data. The least important bit insertion in which the smallest critical part of each byte is changed for the bitstring to be used to form the implanted document is one of the most well-known execution techniques. Adjusting the LSB only helps to change the shade minorly and is not normally detected by the human eye afterward. Although the method is admirably useful for 24bit shading of images, steganography did not perform as effectively when using an 8bit shading image record due to constraints in shading variants and the use of a color chart. The framework that was created starts with a 24bit bitmap shading record, which then sends a 8-bit color map to the document and upgrades it. After the pressure cycle, final compacted image includes an instant message. Results show that in the steganographic environment the new method is beneficial. Data concealment is a method to cover messages in a media with the specific goal that an accidental analyst will not think about the proximity of the messages revealed. The 8bit gray photos are selected as the media. Such pictures are referred to as diffuse images. Spreading pictures of political messages are known as stego-images. The quality of the picture gives the possibility of stego-images for data covering system research. In Section 2, the structure of the paper is discussed as follows: The approach is discussed in Section 3, and Section 4 has findings and outcomes. The conclusion of the study is given in section 5. The conclusion of Section 5 is acknowledgment.

2. System overview

This system uses two authentication levels. Firstly, the RFID card held by the theatre official consists of the data checked by pre-loaded reference data placed on the comparator. The signal from the comparator will be passed on to the driver where there are Darlington transistor pairs, where the signal is amplified and reversed. The driver drives the relay that powers the Arduino microcontroller. The output of the controller is provided to the driver by means of a buffer that provides impedance matching between them. Since the output from the microcontroller is low, the driver amplifies the signal and allows the relays to power

the IR LED's. The signals transmitted from the IR LED's which are placed behind and even along the perimeter of the screen are emitted towards the audience. Hence this light from the IR LED's distorts or obscure the acquisition functions of the camera. Since the IR wavelength (700nm1mm) which is lower than the visible light wavelength (400mm- 700mm) the audience present in the theatre will be able to watch the movie without any disturbance from the but the video cameras or the mobile cameras which are charge coupled devices commonly known as CCD, the recorded content becomes blur or unfit to watch.

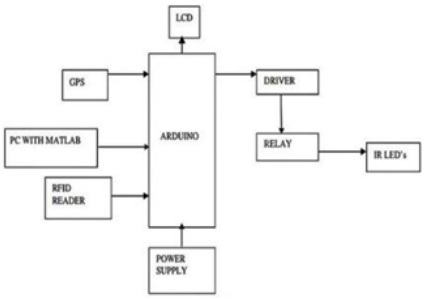

Fig. 1. Block diagram

3. Proposed system

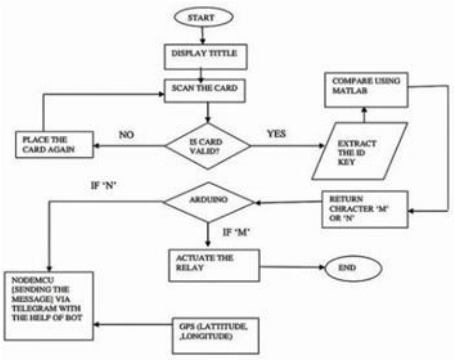

Fig. 2. Flowchart

A. Hiding

Here we are using modulo operator for hiding the key inside an image. The step of hiding is as follows:

First we will target the frame from video which consists of multiple numbers of frames; here frame is 2d which has pixels arranged in the form of rows and columns. After extracting the frame from the video, we will hide the key in corner pixels of the target frame, first we will count the number of characters in the key according to that the number of pixels will be modified, first the pixel values are nullified because in a large frame if we modify pixels it will not affect the video quality much and corner pixels are used, after the nullifying process, the first character in the key is converted to ASCII form and perform bitwise & and bitwise or operation and store the character value in all the three layers. Similarly, all the characters will be converted to ASCII and hided accordingly.

B. Extraction

Here we are using the reverse operation that is performed in hiding, first we will get the target frame from the video, and as we know where the characters are hided. We will get the pixel values and perform the operations bitwise and bitwise or operations on the pixels values that are extracted from each layers, after the above operation on pixels we will get the character values that are hided in the form of ASCII and convert that to character form and we will get the hided key.

C. Color detection algorithm

1) Algorithm for Hiding Secret message in Multimedia file:
Step-a: Load Multimedia file, Secret message and Shared hidden key.

Step-b: Split the Multimedia file into frames.

Step-c: Use secret key received by sender and receiver to convert the hidden message into cipher text.

Step-d: Find Least Significant Bits of every cover frame of Red Green Blue pixel.

Step-e: Convert the encrypted text message into bits.

Step-f: Embed the bits of the secret message into bits of the quilt frame Least Significant bits of RGB pixels.

Step-g: Repeat the method until the message fully embedded into multimedia file.

Step-h: Regenerate Multimedia file frames.

2) Algorithm for Extracting Secret message from Multimedia file:

Step-a: Load ciphered Multimedia file.

Step-b: Break the ciphered Multimedia file into frames.

Step-c: Find and recover the LSB bits of each RGB pixels.

Step-d: Continue the process until the message from the multimedia file is extracted.

Step-e: With the assistance of hidden key decipher message to induce original data.

Step-f: Reconstruct the key information.

Step-g: Regenerate Multimedia file frame.

D. RFID tag scanning

A radio frequency identification reader (RFID reader) is a gadget acclimated assemble information from the partner RFID tag that is made used. The radio waves region unit acclimated exchange information from the magnetic tag to a reader. The RFID card consists of the tag (transponder) that is tiny electronic devices connected or embedded in it, this tag has the special identifier key and is between 3ft to 300ft.The use of the RFID reader in the project to made to secure the authorization of the person trying to play the movie. One Tag is assigned per movie, after the card is scanned, the card number is displayed on the LCD, the last 4 digits of the card is sent to the MATLAB to check if it is a valid ID, only on the correct swipe of the card the movie plays, else there is a message delivered to the registered mobile number through telegram including the GPS location stored. The key is correct, the data is retrieved successfully following the exact opposite of the encryption steps to play the original movie on the screen.

4. Conclusion

The lessons taken from the research that has been done and the room for further progress to make the model more successful are discussed in this section. The main goal is to provide a model that reduces the film piracy mechanism, proposing a model using an LSB method using a secret key embedding method and the use of the IR which affects camera recording in theatre areas. Using IR transmitters, image capture would be blurred. Within zones, for example, these works will serve as theatres for coordinating burglary operations. This has different applications to conceal the obstructive areas, attempts, Imaginative job sections, and chronicled places for visitors, religious sites, upgrade shops, and change rooms at strip centers. It has different applications. The use of video steganography is better than image steganography as the data is contained within the amount of image frames so that it is protected better. This device is a tool for stopping illicit film filming in theatre Environments. This is the target of the grey piracy market. To order to make thecaptured video useless, IR transmittersare used. Various other applications of this method, such as extremely sensitive seminars, seminars, study centers etc., may beintroduced. A simple LSB substitution data hiding procedure is proposed with an ideal pixel change operation. With a small additional multifaceted computational complexity, the wonderful reasoning of the stego can be enhanced remarkably. The optionality of the proposed system is illustrated by broad examinations. The findings are similarly better than the suggested technique for the accuracy of the picture and processing power.

References

[1] Adi Hajj-Ahmad and et.al “Flicker Forensics for Camcorder Piracy,” IEEE, vol. 12, no. 1, pp. 89-99, Jan, 2017.
[2] Zhongpai Gao and et.al, “DLP Based Anti-Piracy Display System,” IEEE VCIP’2014, pp. 145-148, Dec. 2014.
[3] Yu-Mei Wang, “Secured Graphic QR Code with Infrared Watermark,” in IEEE ICASI, pp. 690-693, 2018.
[4] Yuanchun Chen and et.al, “Movie Piracy Tracking using Temporal Psychovisual Modulation,” BMS2017, 2017.
[5] Yutu Nakashima, “Watermarked Movie Soundtrack Finds the position of the Camcorder in a Theatre,” in IEEE Transactions on Multimedia, vol. 11, no. 3, pp. 443-453, April 2018.