International Journal of Modern Developments in Engineering and Science
Volume 1, Issue 5, May 2022
https://www.ijmdes.com | ISSN (Online): 2583-3138

Design and Implementation of an Automated Anti-Piracy System

G. N. Devraj[1], S. G. Mangala Gowri[2], D. Bharath Raj[3*]
[1,3]*Student, Department of Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*
[2]*Associate Professor, Department of Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*

***Abstract*: 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 video in mobile camera and upload it to websites or sell it to people and this goes on. In this project, a technical method to prevent video recording in movie theatres 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.**

***Keywords*: Anti-piracy, authentication.**

1. Introduction

In today's age the growth of the Internet has led to many new innovations in the way it is used. Internet can provide fast access to any kind of information and media, and also the copyrighted contents. "Piracy refers to the unauthorized duplication of copyrighted content that is then sold at substantially lower prices in the 'grey' market". Final copy of the movie content might get leaked before its release by the multiple teams working on them. The more common method is to film the movie inside a theatre and then uploading it on Websites or convert them to DVDs and sell them on the streets. Most box office releases are available online within a few days or even hours of the box office release. Hindering piracy has always been priority number one for movie theatres. The markets around the world have tried to take on the issue of piracy through policing and prosecution. Copyright law protects the value of creative work. Making unauthorized copies may subject one to civil and criminal liability. Night vision goggles are provided to movie hall staffs which would help them to notice any audience trying to record a movie while screening. Instead of treating every movie goer as a potential pirate, an anti-piracy screening system can be implemented in order to make the pirate copy useless as well as having no effect on the audience. Movie piracy has a profound impact on the motion picture industry. The Motion Picture Association of America (MPAA) investigated on the movie piracy in 2005. According to the statistics in the report, the major U.S. motion picture studios lost 6:1 billion or more annually. These losses in revenue will obviously cause serious financial problems for the studios and even contribute to their current downfall. In 2010, for example, over one million copies of James Cameron Avatar were downloaded illegally in just seven days. In the view of the law, movie piracy is considered as crime all over the world. As an important source of movie piracy, the camcorder piracy accounts for about 23% of the piracy methods according to the BBC News. As the source of infringing DVDs, camcorder movies spread rapidly on the internet. These losses in revenue will obviously cause serious financial problems for the studios and even contribute to their current downfall. In 2010, for example, over one million copies of James Cameron Avatar were downloaded illegally in just seven days. In the view of the law, movie piracy is considered as crime all over the world.

2. Proposed Methodology

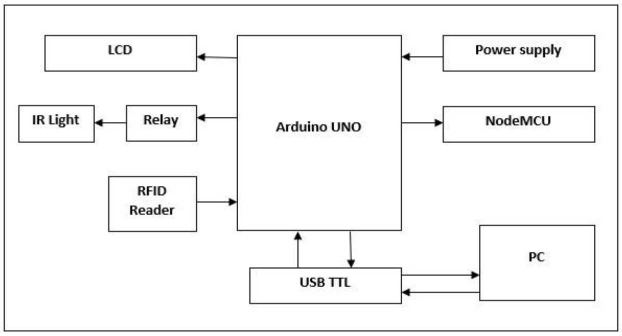


Fig. 1. Block diagram

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 digital output of the comparator is passed on to the optocoupler where it provides an electrical isolation between the comparator and driver thereby preventing the flow of back enfant the comparator. The signal forms the comparator is passed to driver consisting of pairs of Darlington transistor where it undergoes amplification and inversion.

The second level authentication is done by the micro controller. On switching the Micro controller, the keypad gets activated for the password to be entered. If the password is

*Corresponding author: bharathraj62627@gmail.com verified the controller output is given to the driver through the buffer which provides impedance matching between them. Since the output from the microcontroller 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. On placing IR LEDs behind and around the screen in the cinema theatre, the video playing on the screen becomes blur or scrambled for audience watching the movie because wavelength of IR (700nm-lmm) signal is longer than the visible light wavelength (400nm-700nm). 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 blurring or unfit to watch.

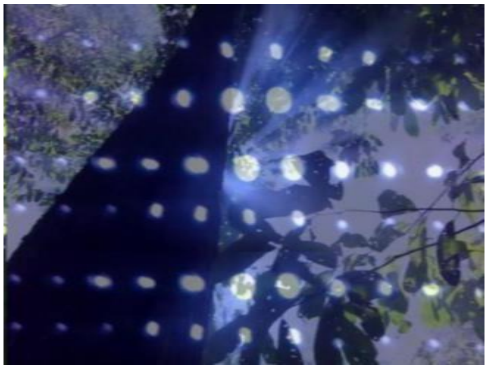


Fig. 2. Normal picture

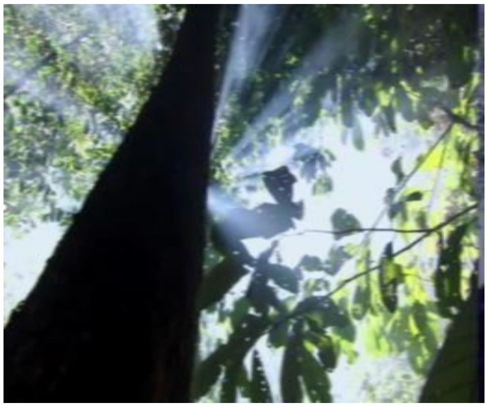


Fig. 3. Picture after placing IR's behind the screen

3. Implementation

The hardware setup of the block diagram of the movie piracy system as shown in fig. 1 is shown in fig. 4.

The system uses:

- Arduino UNO microcontroller
- Power supply
- LCD display
- Node MCU
- RFID
- Relay
- IR LEDs.

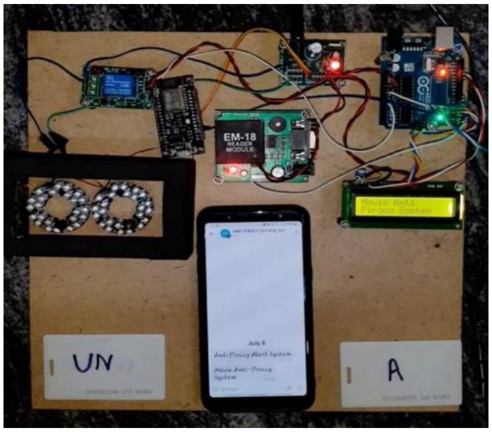


Fig. 4. Hardware setup

On switching on the microcontroller, the system waits for the respective person's input to handle the system and hence displays the project name initially as shown in fig. 5 and the ready status of the system as shown in fig. 6.

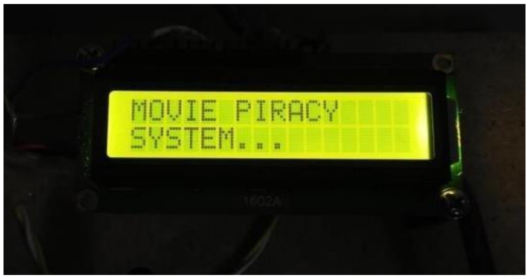


Fig. 5. Display of the project title

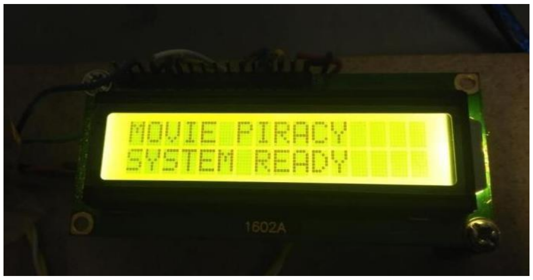
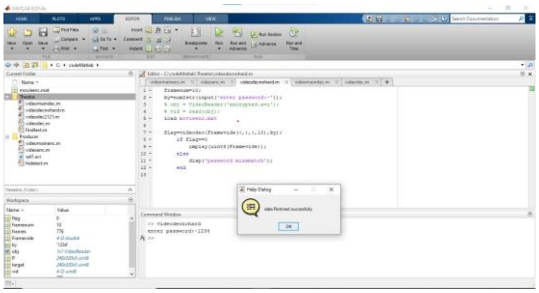


Fig. 6. Ready status of the system

Once the microcontroller switches on, the RFID gets activated for the RFID card. If the password is verified controller output is given to the driver through the buffer which provides impedance matching between them. If the password entered by the user matches with the data hidden in the video file, data is retrieved successfully as shown in fig. 7.



```
framenum=10;
ky=num2str(input('enter password:-'));
% obj = VideoReader('encrypted.avi');
% vid = read(obj);
load movieenc.mat

flag=videodec(Framevide(:,:,:,10),ky);
    if flag==0
        implay(uint8(Framevide));
    else
        disp('password mismatch');
    end
```

data Retrieved succesfully

```
>> videodecnohard
enter password:-1234
>>
```

Fig. 7. Password authentication

If the password entered by the user matches with the data hidden in the video file, data is retrieved successfully as shown in fig. 7.

After authentication of the password, the LCD display displays that the authorized person played the movie as shown in fig. 8.

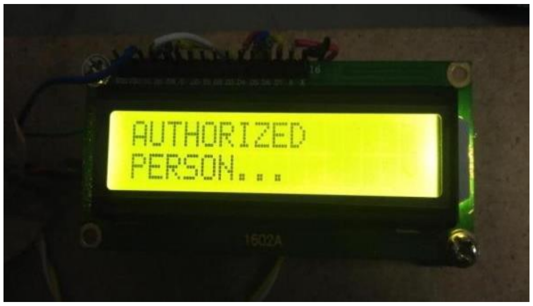
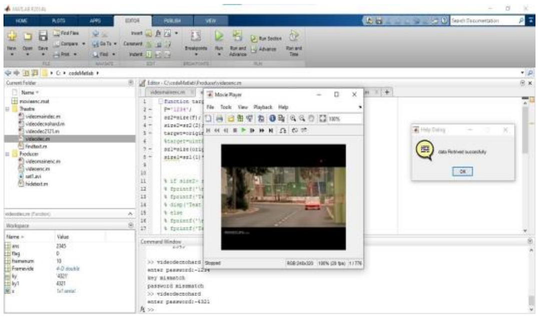


Fig. 8. Displaying authorized person

Since the authentication process becomes successful, movie gets displayed on the screen, also displaying the location at which movie is being played as shown in fig. 9.



```
>> videodecnohard
enter password:-1234
key mismatch
password mismatch
>> videodecnohard
enter password:-4321
>>
```

data Retrived succesfully

Fig. 9. Movie being displayed

Since the output of the microcontroller is low, driver amplifies the signal and actuates the relay to control the IR LEDs. The LEDs turn on once when the password authentication process becomes successful as shown in fig. 9. 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.

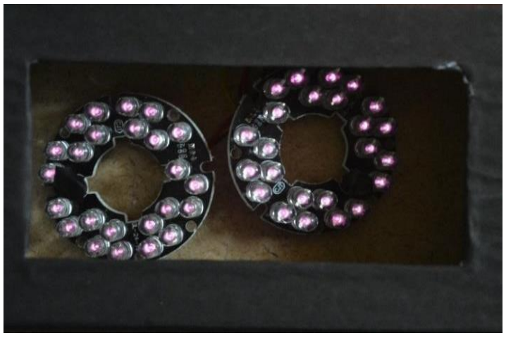
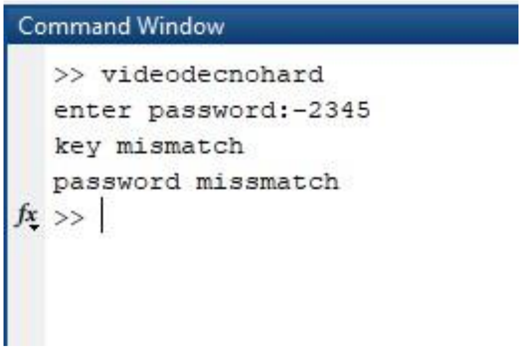


Fig. 10. IR LEDs being turned on

On placing IR LEDs behind and around the screen in the cinema theatre, the video playing on the screen becomes blur or scrambled. it appears so because wavelength of IR (700nm-1mm) signal is longer than the visible light wavelength (400nm-700nm). 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.

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. 11.



```
>> videodecnohard
enter password:-2345
key mismatch
password missmatch
>>
```

Fig. 11. Failure of password authentication process

Simultaneously the LCD displays that an unauthorized person tried to play the movie as shown in fig. 12.

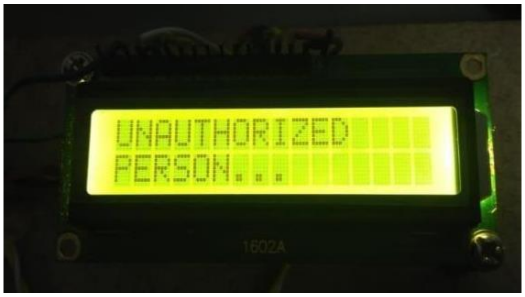
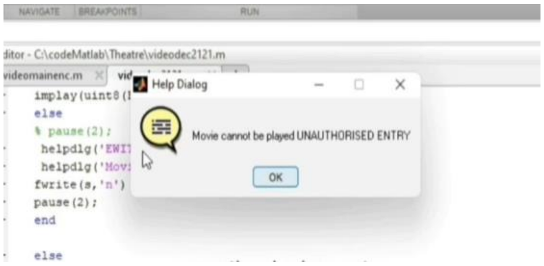


Fig. 12. Display showing about an unauthorized person tries to play the movie

The failure of password authentication does not allow the movie to be played and also an alert message is delivered to the concerned person with the information regarding the location where the movie is being played in an unauthorized way.

A dialog box appears to indicate the same as shown in fig. 13 and the message being sent to the concerned person is shown in fig. 14.

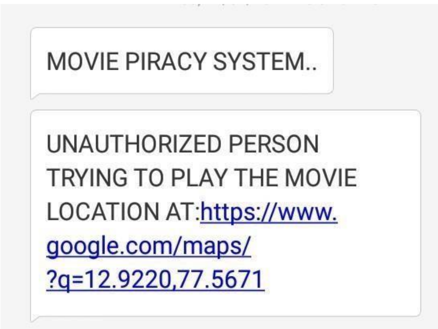


```
imsplay(uint8(I
else
% pause(2);
 helpdlg('EWI
 helpdlg('Movi
fwrite(s,'n')
pause(2);
end

else
```

Movie cannot be played UNAUTHORISED ENTRY

Fig. 13. Movie unable to be played



MOVIE PIRACY SYSTEM..

UNAUTHORIZED PERSON
TRYING TO PLAY THE MOVIE
LOCATION AT:https://www.google.com/maps/?q=12.9220,77.5671

Fig. 14. Message being sent to the concerned person

4. Conclusion and Future Scope

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. IR transmitters used in the system are placed in and around the perimeter of the movie screen. The wavelengths of infrared are longer wavelengths than those visible to humans. This range of light is invisible to human eyes. It is very visible to many types of cameras. Hence these lights would not disturb people watching the movie. It will however distort the recordings made by many types of cameras. Hence the captured content gets blurred or disturbance is introduced in it. 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. The 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.

References

[1] B. V. R. Kumar, B. A. Vardhan, C. H. Rahul Gupta, and P. Surekha, "Reduction of Movie-Piracy using an Automated Anti-Piracy Screen Recording System," *4th International Conference on Information Systems and Computer Networks (ISCON)*, 2019.

[2] P. Dhulekar, S. Choudhari, P. Aher, and Y. Khairnar, "Arduino based Anti-Photography Prohibited Areas," in *Journal of Science and Technology*, vol. 2, no. 5, pp. 6-11, May 2017.

[3] K. A. Abhishek, G. Chetan, M. S. Deepak, M. Akash, and M. Rohith, "Camcorder piracy-RFID based anti-piracy screen," in *International Journal of Scientific Research & Development*, vol. 6, no. 3, pp. 1743-1746, June 2018.

[4] P. Bourdon, S. Thiebaud, and D. Doyen "A theoretical analysis of spatial/temporal modulation-based systems for prevention of illegal recordings in movie theaters," in *Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, March 2008.

[5] Y. Nakashima, R. Tachibana and N. Babaguchi, "Watermarked Movie Soundtrack Finds the Position of the Camcorder in a Theater," in *IEEE Transactions on Multimedia*, vol. 11, no. 3, pp. 443-454, April 2009.

[6] Z. Gao, G. Zhai, X. Wu, X. Min and C. Zhi, "DLP based anti-piracy display system," *2014 IEEE Visual Communications and Image Processing Conference*, 2014, pp. 145-148.

[7] A. K. Veeraraghavan, S. S. Ramachandran, and V. Kaviarasan, "A survey on reduction of movie piracy using automated infrared system," in *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 11, pp. 16633-16637, Nov. 2017.

[8] T. Yamada, S. Gohshi and I. Echizen, "Enhancement of method for preventing illegal recording of movies to enable it to detect cameras with attached infrared-cut filter," *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2012, pp. 1825-1828.

[9] R. Thanki, V. Dwivedi, K. Borisagar, and S. Borra, "A watermarking algorithm for multiple watermarks protection using RDWT-SVD and compressive sensing," in Informatica, vol. 41, pp. 479-493, 2017.