International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 3, ISSN No. 2455-2143, Pages 131-136
Published Online July 2019 in IJEAST (http://www.ijeast.com)

MOVIE PIRACY REDUCTION USING AUTOMATED INFRARED TRANSMITTER SCREEN SYSTEM AND STEGANOGRAPHY TECHNIQUES

Sowmya Sreenath
Department of ECE
SJBIT, Bangalore, Karnataka, India

Dr.Mahantesh K
Department of ECE
SJBIT, Bangalore, Karnataka, India

Abstract— Film or movie is a noteworthy entertainment for individuals in the present life. To engage individuals a great deal of speculation is put on films by the film – producers. Their exertion is being demolished by few individuals by pilfering or pirating the film content. Pirating is the method of duplicating the movies and uploading it to the cloud sources for easy access. They do it by catching the video in portable camera and transfer it to sites or pitch it to individuals and this goes on. These days, camcorder theft has incredible effect on the film business. There are some remarkable innovations can follow the motion picture privateer, the video content saw in the auditorium might be influenced and they can't discourage the need of pilfered motion picture in light of the fact that the watermarks in pilfered moves are imperceptible. The aim of this paper is to embedded a secret key using the stegonography method through MATLAB to secure the movie file. Also develop an infrared transmitter based screen to avoid the movie recording go in vein. Also using the GSM to indicate the authorized person with the details of the piracy of the intruder via SMS. This system is proposed to reduce the piracy record in the field of cinema.

Keywords— Anti Piracy, GSM, IR Screens, LSB, RFID, Steganography

I. 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 duplication of copyrighted substance that is then sold at generously lower costs 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 typical strategy is to film the motion picture inside a theater and afterwards transferring it on Websites or convert them to DVDs and offer them in the city. Most cinema industry releases are open online inside a few days or even hours of the release of the motion picture Blocking theft has dependably been needed number one for cinemas. The business sectors around the globe have endeavored to assume the issue of theft through policing and arraignment.

Copyright law secures the estimation of imaginative work. Making unapproved duplicates may expose one to common and criminal risk. 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 gore 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 theft significantly influences the film business. The Motion Picture Association of America (MPAA) [1] coordinated an examination on the movie theft in 2005. As shown by the estimations in the report, the major , U.S. motion picture studios lost $.6.1 no less than billion yearly. These disasters in pay will unmistakably cause authentic financial issues for the studios and even add to their present thrashing. In 2010, for example, more than one million copies of James Cameron Avatar were downloaded unjustly in just seven days [2].

There are many ways to avoid these security issues concerned with the continuous image issues, one such method to tackle the problem is steganography. Steganography is the way towards concealing one document inside another to such an extent that others can neither distinguish the significance of the implanted item, nor even perceive its reality. Current patterns support utilizing advanced picture records as the spread document to conceal another computerized record that contains the mystery message or data.

A standout amongst the most widely recognized techniques for execution is Least Significant Bit Insertion, in which the least critical piece of each byte is modified to shape the bit-string speaking to the implanted document. Adjusting the LSB will just purpose minor changes in shading, and subsequently is generally not observable to the human eye. While this method functions admirably for 24-bit shading picture documents, steganography has not been as fruitful when utilizing a 8-bit shading picture record, because of confinements in shading varieties and the utilization of a colormap. the display of the consequences of research exploring the blend of picture pressure and steganography. The system created begins with a 24-bit shading bitmap record, at that point packs the document by sorting out and enhancing a 8-bit colormap. After the procedure of pressure, an instant message is covered up in the last, compacted picture. Results show that the last system has capability of being helpful in the steganographic world.

Data concealing is a system for covering riddle messages into a spread media with the true objective that a unintended observer won't think about the nearness of the disguised messages. The 8-bit grayscale pictures are picked as the spread media. These photos are called spread pictures. Spread pictures with the riddle messages introduced in them are called stego-pictures. For data covering frameworks, the image quality proposes the likelihood of the stego-pictures.

The composition of the paper is as follows: In Section 2, the system overview is discussed. A section 3 talk about methodology and Section 4 has outputs and results. Section 5 gives conclusion of the analysis. Section 5 ends with acknowledgement.

II. SYSTEM OVERVIEW

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 opto-coupler where it provides an electrical isolation between the comparator and driver thereby preventing the flow of back the comparator.

The signal form the comparator is passed to driver consisting of pairs of Darlington transistor where it undergoes amplification and inversion. This driver is used to drive the relay which in turn actuates the micro controller. The second level authentication is done by the micro controller. On switching on the 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.

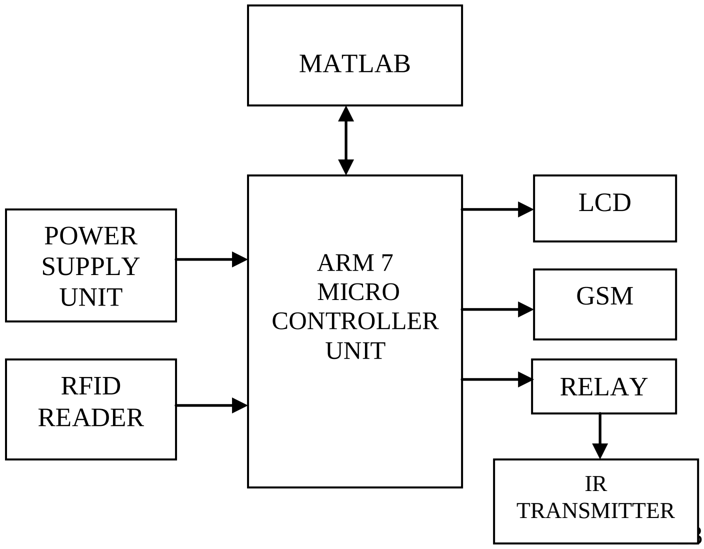


Fig.1. Block Diagram

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. 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.

The block diagram is as shown below with all the required components for the prototype namely, PC with MATLAB, ARM-7 microcontroller, IR-Transmitter, Relay, GSM Modem, RFID reader, LCD.

III. PROPOSED METHOD

This section describes the details of the methods specified as per the algorithm in the previous section along with the flow of the working as described in the figures and explanations in each section,

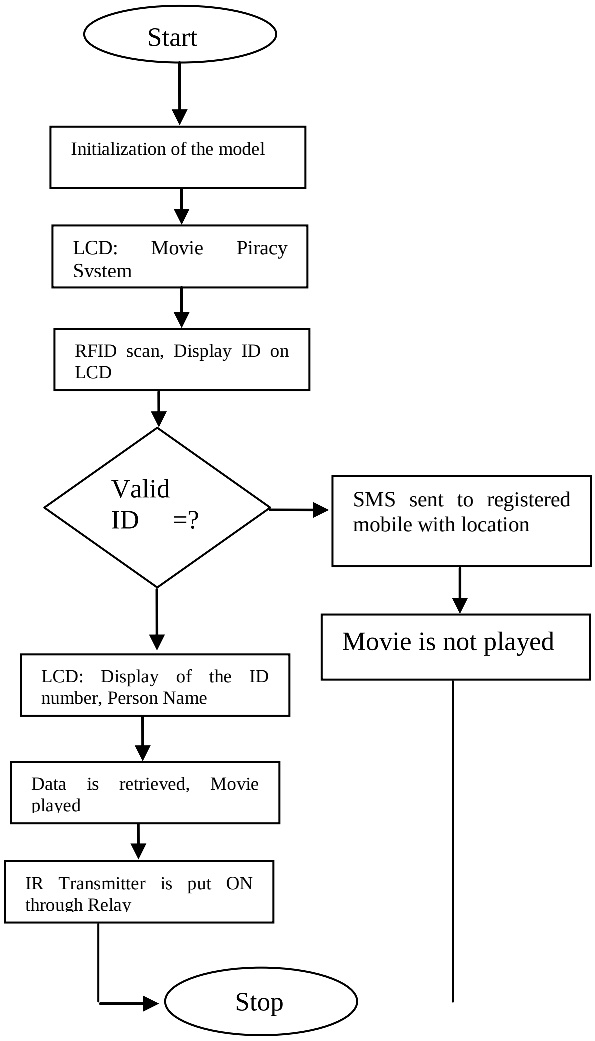

Start
Initialization of the model
LCD: Movie Piracy System
RFID scan, Display ID on LCD
Valid ID =?
SMS sent to registered mobile with location
Movie is not played
LCD: Display of the ID number, Person Name
Data is retrieved, Movie played
IR Transmitter is put ON through Relay
Stop

Fig. 2: Flow of the work

A. Secret Key Embedding Method

A technique called Least Significant Bit (LSB) is made used for proposed system in this paper. Here, a particular frame of the movie is chosen, where the RGB values of the lsb of that frame is manipulated. The manipulation includes a hidden key of multiple of 4bit binary data.

B. Color Detection Algorithm

Below are the detailed steps included as the algorithm for incorporating the Secret-key in cover frame of video

Step-1: Input covers film outline on frame number 10, with the key.

Step-2: Break the video into desired frames.

Step-3: Conversion of the secret message into hexadecimal content by utilizing RFID tag key.

Step-4: Find Least Significant Bits of each RGB pixels of the spread casing frame number 10.

Step-5: Convert the encoded instant message into bits of products of 4.

Step-6: Embed the bits of the mystery message into bits of LSB of RGB pixels of tenth edge of the spread video.

Step-7: Continue the implanting strategy until the key is completely put in into video edge of the document**.**

Step-8: Regenerate video outlines after the inserting is finished**.**

Below are the detailed steps included as the Algorithm for Secret-key Extraction from video frame

Step-1: Choose the encrypted video file.
Step-2: Break the stego video file into frames.
Step-3: Upon key matching, start to retrieve the LSB bits of each RGB pixels of the 10th frame.
Step-4: Continue to decrypt until the secret key is fully extracted from the frame of the video file.
Step-5: Reconstruct the secret information by removing it from the frame.
Step-6: Regenerate video to original.

The different techniques used are listed below:

i. Extraction technique

At the recipient side the impacted (where the data is covered) plentifulness regards are bound by 16 and the remainders of this division are covered up hexadecimal digits. A little while later this is sent to the post-planning system to get the fundamental target content.

ii. Post-preparing

By the resultant hexadecimal digits are changed over to their 4 bit twofold proportionate. These 4 bits are related with packaging a twofold string. By at that point, each 7 bits are sliced and changed over to their taking a gander at decimal proportionate. The characters of this ASCII respect are associated by the string length to get the fundamental target string.

iii. RFID Tag Scanning

A radio frequency identification reader (RFID reader) may be 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 label it ought to be among the change of partner RFID per user, that ranges from three 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 an SMS delivered to the registered mobile number through GSM 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.

IV. RESULTS

The result of the prototype says about the overcome of the disadvantages of the various methods from the literature survey chapter and the effectiveness of the implementation of the developed. The undertaking presents a model arrangement of crushing TV camera robbery in theater upheld Temporal psycho-visual regulation (TPVM)[7]. By misusing the varieties differentiating human eyes and semiconductor imaging sensors in the worldly convolution of an optical sign, keeping an eye on incontestable anyway the TPVM fundamentally based procedure will outwardly obliterate the recorded pic substance though accomplishing visual straightforwardness of inserting examples to the platform group of onlookers. The example (e.g RFID Tag) additionally is the pursuit info to reveal the one accused for the television camera piracy.

Application of video steganography is more useful when compared with image steganography because here the data will be hided inside number of frames of image so it is more secured.

This system provides a method to prevent the illegal recording of movies in theatres. Thus targeting the grey market of piracy.

The IR transmitters are used in order to make the captured video useless.

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

Utilizing the LSB method for the venture consequences of implanting the decreased measured picture of Figure. b into the second arrangement of spread pictures appeared in figure.

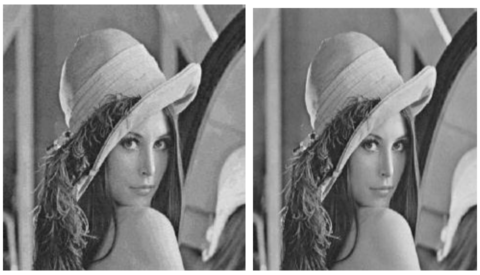


Fig. 3 Stego-images obtained by (a) LSB-substituted method; (b) proposed method, with secret-image is 4-bit inserted.

The consequences of implanting the diminished estimated picture of Figure. a couple of into the second arrangement of spread pictures results demonstrate that comparative PSNR values are gotten for different kind of spread pictures.

Data concealing technique by straightforward LSB substitution with associate best component method is projected. The image quality of the stego-image is improved with low further process quality.

Broad investigations demonstrate the adequacy of the proposed technique. The outcomes acquired likewise show noteworthy improvement as appeared in the table.

Table. 1. Comparison of BITMAP and JPEG images result

	PNSR	MSE	RMSE
BITMAP	62.62	0.0358	0.189
JPEG	62.54	0.0362	0.0190

A standout amongst the most ideal method for discovering a decent steganography procedure is the breaking down the breaking down the bar chart of all stego image and later distinction them and distinctive one. Thus, this strategy is provided for making a mystery put in image that's fully imprecise from the primary image by the human eye and cannot be seen.

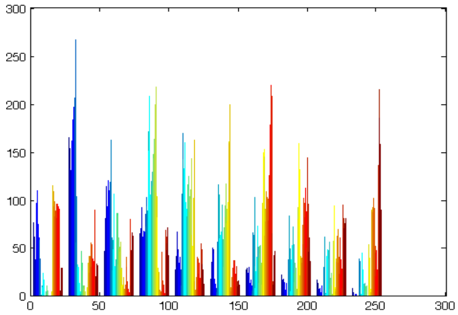


Fig.4: Histogram of original frame image

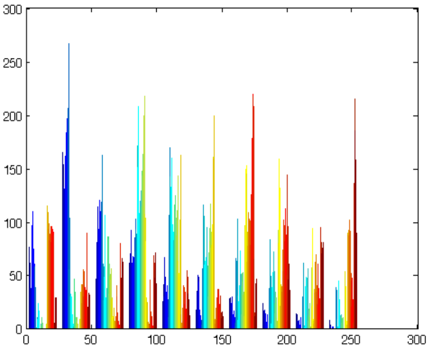


Fig.5: Histogram of frame containing secret-key

A. Results of the Proposed System

This section exclusively shares the hardware design, results at each step along with the figures with respect to the above drawn observations.

Following are the results as per the flow chart from the previous section .

1. The title of the project as soon as the project is initialized. This is an indication as the start of the project.
2. The next step is to intimate the concerned person that the system is turned ON, this is done by sending an SMS alert and the same is shown on the LCD screen.

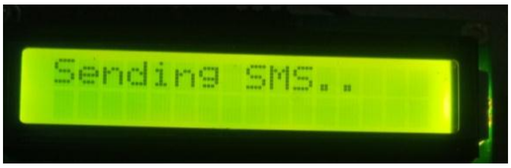


Fig.6: SMS ALERT TO NOTIFY THE SYSTEM IS ON

3. Once the movie is played, it asks the user to scan the RFID Tag to check if the valid user is accessing the movie, this indication is shown on the LCD screen as per figure.

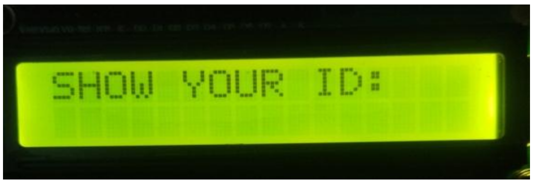
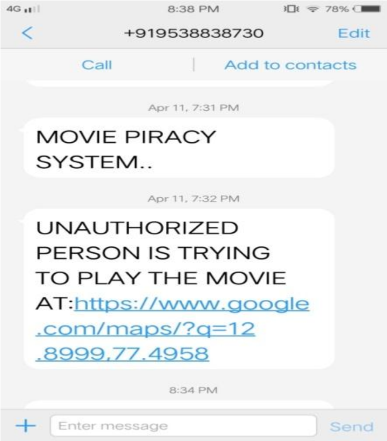


Fig. 7: RFID SCANNING FOR AUTHENTICATION

The scanned Tag will be displayed and the last 4 digits are sent to the MATLAB for verification, if it is wrong then the LCD will display, along with sending intimation to the registered mobile number with the location access as shown in figure



Apr 11, 7:31 PM

MOVIE PIRACY SYSTEM..

Apr 11, 7:32 PM

UNAUTHORIZED PERSON IS TRYING TO PLAY THE MOVIE AT:https://www.google.com/maps/?q=12.8999,77.4958

8:34 PM

Fig.8: SMS received in mobile along with location, in case of unauthorized access

4. For the correct RFID Tag scanned, the LCD displays the RFID Tag along with the name of the person trying to play movie.

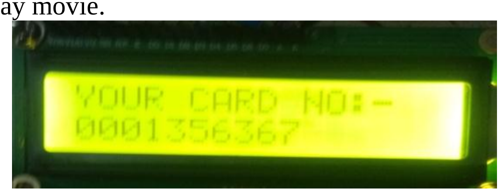
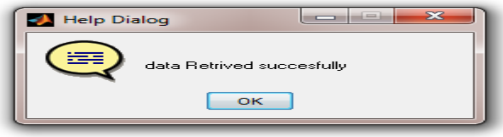


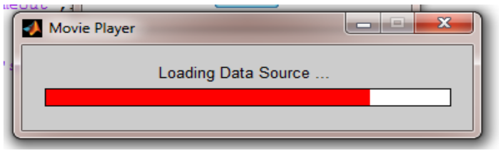
Fig.9: Display of RFID tag read

5. A dialogue box appears when the key is matched in the MATLAB to retrieve the data back figure i.e., decryption of the video file as shown in figure. Later the movie starts playing.



data Retrived succesfully

Fig.10 : Dialogue box for decryption of data



Loading Data Source ...

Fig.11: Decryption of the movie file

6. After the complete data decryption, the movie screen appears to play, pause, rewind or forward actions as shown in the below figure

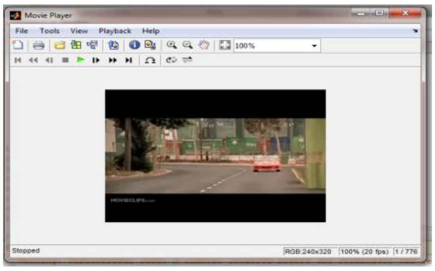


Fig.12: Movie player to play the movie

V. CONCLUSION

This chapter includes the conclusions drawn from the proposed work along with the scope for further development to increase the effectiveness of the model.

The principle goal is to provide a model which reduces the movie piracy system, by proposing a model with secret key embedding technique using LSB method along with usage of the IR leds to affect the camera recording in theater regions. The camera recording will be blurred utilizing IR transmitters. This work will serve valuable during the zones, for instance, theaters for balancing the activity of burglary. It has various applications which consolidate keeping up secret at obstruction regions, endeavors, inventive work sections, chronicled tourist spots, religious spots, enhancements stores, changing rooms at strip malls. Application of video steganography is more useful when compared with image steganography because here the data will be hided inside number of frames of image so it is more secured. This system provides a method to prevent the illegal recording of movies in theatres. Thus, targeting the grey market of piracy. The IR transmitters are used in order to make the captured video useless.

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

A data hiding procedure by clear LSB substitution with an ideal pixel change process is proposed. The delightful thought of the stego-picture can be remarkably improved with low additional computational multifaceted nature. Wide examinations display the electiveness of the proposed framework. The outcomes picked up in like way show critical improvement than the technique proposed concerning picture quality and computational capability.

VI. ACKNOWLEDGEMENT

This research is supported by SJB Institute of Technology, Bengaluru. I sincerely thank our guide Dr. Mahantesh K , for supporting this work by encouraging with his guidance.

VII. REFERENCES

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain , (2011) A New Approach for LSB Based Image Steganography using Secret Key, ,Proceedings of 14th International Conference on Computer and

Information Technology (ICCIT 201 I) 22-24 December.

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

[3] B. NEWS, (2015) “The fact and fiction of camcorder piracy,”.

[4] A. DENSO, (2013) “QR Code essentials,” 2011, retrieved 12 March .

[5] B. NEWS, (2015) “The fact and fiction of camcorder piracy,”.

[6] G. Zhai and X. Wu, (2014) “Defeating camcorder piracy by temporal psychovisual modulation,” *J. Display Technol.*, vol. 10, no. 9, pp. 754–757, Sep.

[7] Guangtao Zhai, Xiaolin Wu, (2014) “Defeating Camcorder Piracy by Temporal Psychovisual Modulation”, JOURNAL OF DISPLAY TECHNOLOGY, VOL. 10, NO. 9, SEPTEMBER.

[8] Lindawati, Rita Siburian, (2017) Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio International Conference on Wireless and Telematics, July 27 – 28.

[9] X. Wu and G. Zhai, (2013) “Temporal psychovisual modulation: A new paradigm of information display,” IEEE Signal Process. Mag., vol. 30, no. 1, pp. 136–141.

[10] Khalid A. Al-Afandy, El-Sayed M. EL-Rabaie, El-Sayed M. EL-Rabaie, Gh. M. El-Banby, (2016) High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography, IEEE.

[11] RAKHI1 & VIJAY PRAKASH SINGH, (2014) " DATA HIDING IN SKIN TONE OF IMAGES USING STEGANOGRAPHY", International Journal of Electronics and Communication Engineering (IJECE), Vol. 2, No. 4, PP. 105-112.

[12] Jain, Nitin, Sachin Meshram, and Shikha Dubey, (2012) "Image Steganography Using LSB and Edge–Detection Technique", International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No. 3, PP. 217-222.