IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

ANTI-COUNTERFEIT SYSTEM FOR THEATRES

Ashritha. R[1],Dhanya Sukanth B K[2], Disha Shivani[3],Sahana S[4]

K. S. Institute of Technology, Electronics and Communication Engineering, Bangalore[1-4]

Abstract: Piracy has become a threat to the film industries over the years. It financially effects the ones that work hard to make movies. It is burdensome to prevent piracy from the viewer's end. Hence, we have created a prototype screen as well as a security method to reduce piracy on a larger level. We use an anti-counterfeit screen built using IR LEDs that displays the location of the theatre, using GPS, when turned on. Also, to increase the security of the movie and the screen, we encrypt it and generate a single use OTP for decryption.

Keywords: emission, IR LEDs, piracy, screen, watermark.

I. INTRODUCTION

Movie piracy has been a worldwide problem for movie makers. Piracy is typically defined as the illicit duplication of copyrighted material for subsequent considerable price reductions on grey markets. In India nowadays, piracy is a pervasive threat. Films from movie theatres are illegally recorded using tools like hand-held cameras and mobile phones. Theater recordings are already entering the market at an astonishing rate owing to the availability of inexpensive smart phones with good cameras. And because of these portable gadgets have high-speed internet access, such recordings are practically quickly posted to data-sharing websites online. One of the associates may decide to sell the copy that is eventually scheduled for release. Another widespread practice is to record a movie in its entirety while viewers are inside the theatre, submit the recordings to websites, and create DVDs from the content. The movie business and production companies suffer enormous losses as a result. Such losses are estimated by market experts and are immediately passed on to the public in the form of higher movie ticket prices. The consequences of piracy and counterfeiting on India's entertainment business are estimated to be 60%. The task of combating this pirate issue has long been one of the top priorities for movie theatres. The markets all over the world have implemented severe rules to address this issue, and they are also pursuing legal action in an effort to stop movie piracy. Piracy must be reduced since it has a negative impact on society and prevents the development of new technologies and formations.

To overcome the problem of piracy, different technologies have been introduced where the quality of the recorded video has been degraded using IR LEDs and various watermarking techniques.

II. LITERATURE SURVEY

Pascal Bourdon et al. [1] has proposed multi primary projection device for preventing illegitimate recording in theatres. The project is elicited from the metamerism principle. The term metamerism means the matching of colour light with various spectral power distributions. A camcorder jamming system is used in this project. This camcorder is made up of three distinct light sensitive cells. In video recording devices, trichromacy is usually gained by using Cyan-Magenta-Yellow or Red-Green-Blue sensitivity functions. This is basically bottomed on two constrains: Signal to Noise ratio - the sensor must get signal so that it makes it feasible to maximize this figure and restrict noise in filmed videos or images. Colour- the light sense should be able to discriminate colours like the human eye does. The difference connecting the two RedGreenBlue triplets, the light detector will give out maximum value. If this discrepancy between them is maximum to be seen by using only one spectrum to emit a pattern and utilizing the other as the background colour, we can attain camcorder jamming. One of the major drawbacks of IR depending camera jamming is that the content is not situated within the appearance range. This method of jamming requires a highly complicated filter. As a colour wheel related emission system teaches temporal modulations, they constructed all camera speed settings to least numbers so that the jamming effect is a metamerism prompted artifact. In the first prototyped presented by them, they were able to get seen artifacts on all the three camcorders. Comparing to the spatial light modulation or IR related techniques one advantage

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

of this approach is durability. They suggest that anti metamerism filters can be designed but are extremely costly and would work on only one camcorder.

Abdullah M et al. [2] has proposed the method of video encryption and decryption which is relayed to colour information transformations on encoding the content of the video. This logic dispenses a pliable function to encrypt any content by quantum measurement to improve the safety of the content. The two main challenges faced in this process is, that the quantum video is generally large and is a heavy load for rectifying all the frames and also the video needs to be rectified in real time, a process that shows to be time taking. This needs to rectify a huge load of data in a short interval which inflicts a burden on storage, network communications etc. the proposed video encryption method has various properties such as high security, high speed, and flexibility. Using the above, a colour information key (CIK) is generated. This key is basically generated in 0s and 1s. Hence the key will be distinct each time hence, will increase the safety of the video. This process is allowing to encrypt many frames of the video continuously. So, if we have a huge video with many frames, encrypting the video will be easier and with good speed and accuracy. It is feasible to interchange two frames in the video and change the content in a frame and also even constraint the encryption to special pixel in a specific frame in the video. During the process of encrypting, the video is changed into a vague set of frames that does not make sense. Similarly, the decrypting is the reverse process of the encrypted video to the original content of the video.
The encryption used in this project is the colour information key (CIK) generation. A colour generation key is a order of numbers allocated by a rule, which is utilised to change the colour in an image or a video. The CIK is updated every time the image is measured. According to the
configuration
of basic colours in RGB colour model only 8 indexes are allocated to the distinct colours from black to white. The key is achieved by this measurement and has the similar length as the count of pixels in the image. As the video is composed of many frames that show very little similarities to each other, this encryption is mainly focused on the key frames and it prepares a duplicate of them to take the quantum measurements and generate colour information key related to the channel of interest. There are few CIK rules to be followed. This process utilises matrixtransformations to enhance the safety factor of video encryption. It manipulates a series of frames at once instead of doing so one after the other. Decrypting of the video is a process to get back the original video utilising a suitable algorithm. This process is used only by authorised people by distributing keys from the encryption side. This is basically the complete reverse process of the encryption procedure. The drawback of this project is that this proposed method cannot deal with images with plain backgrounds as it always has the same colour after the quantum measurement, hence the encryption of such images is vague. The solution to this problem is to upgrade the encoding rule and retransform the related colour variations. The CIK will also be a long sequence if the image has a high-resolution so storing it will need huge storage space.

S S Maniccaama et al. [3] has introduced a method based in SCAN methodology undertaken by scan patterns i.e., keys bring into being by this methodology and the values is being changed utilising a replacement rule. This encryption is based on the repeated product cipher. This proposed encryption has an extra feature such as dependent key permutation, more key storage, encryption of larger blocks etc. This encryption method uses symmetric key encryptions which means the similar key is generated for encryption as well as decryption. The key should be familiar to both transmitter and the receiver in advance to the imparting of the film. This method is explained by grammar and every language has a collection of patterns, a group of variations, a collection of norms to be followed to construct an easy scan pattern to get difficult scan patterns. The video encryption method finds the contrast between adjacent frames and compresses the frames. The maximum pixel distinction between the authentic and recovered video is decided by the end user. Here they use VideoEncrypt() function in the algorithm. Confusion and diffusion properties are satisfied in this method of encryption. The exact prediction of the key makes decryption almost out of the question. The complexity of SCAN methodology is high. But the software implementation takes around 3s-5s to encrypt and decrypt the video. This is impractical for real time applications.

Sridhar C et al. [4] they have used symmetric encryption algorithm for multimedia using hybrid crypto approach. There are mainly two methods used for hybrid crypto approach, they are Advanced Encryption Standard(AES) algorithm which is suitable substitution of the existing DES algorithm. It takes an input of 128bit plain text with an encryption key of 128, 192, 256 bit on total rounds which are 10, 12, 14 respectively. This encryption is not based on the Feistel structure. The

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

other technique is the Elliptic Curve Cryptography (ECC). This stereotype is based on sturdiness of the ECDLP and plainness of AES algorithm. This system is deliberate to give high safety to different data from text documents, audios, videos, images etc. This method first converts the input data into an encoded version in a text form. This data is further sent to an starting encryption utilising AES algorithm, in which the keys are generated randomly. A QR code is generated which is equivalent to the key in the image that is later on utilised by the prototype to get the key in text format. Due to this process advanced safety is provided to key generated in AES. For the next measure of safety, the AES keys are encrypted utilising public key. The encrypted AES key in utilised to encrypt the plain text to transform into a cipher text. Hence the cipher text is already gone through two levels of encryption of both AES and ECC. This forms a hybrid structure of encryption that gives a much better and higher level of security. The decryption process is the exact backward process of the encryption which involves a slight complexity method. The total time consumed for both encryption and decryption is slightly more as a hybrid model or encryption is used. Since the files are compressed the overall space for storing is reduced. The security level expected is very elevated as compared to the previous proposals as it uses a hybrid approach for encryption.

A. Massoudi et al. [5] have used the selective encryption method. selective encryption is a latest swing in image and video encryption. The aim of selective encryption is to decrease the quantity of the data that has to be encrypted while also preserving a sufficient measure of safety and security. An extra feature of selective encryption is to conserve some properties of the original content. In this encryption process the plain text or the content is split in to two equal parts. The first is known as public part, which is not ciphered and known and can be accessible by all users. The other part is protected by encryption. Only authorized people have access to the encrypted data. They have defined a collection of criteria that helps in evaluating selective encryption algorithms. The criterions are: (i) Tunability- this limits the use of a certain algorithm to a group of application. (ii) Visual degradation (VD)- this property measures the disturbance of the cipher video with respect to the original content. This criterion assumes that the cipher content can be decoded and viewed without any decryption. This is not satisfied by all the algorithms present. In few applications, we can achieve sufficient degradation so that a hacker can still understand the content but prefers to pay to access the encrypted data. (iii) Cryptographic security (CS)- this relies on the key and the instability of the encrypted part. (iv) Encryption ratio (ER)- this measures the ratio between size of the encrypted part and the whole content size. The ER must be minimised by selective encryption. The other criterions are compression friendliness, format compliance and error tolerance. The selective encryption is classified into three classes of methods that are:(i) Precompression- this encryption is done before the compression of the content. In most cases, performing encryption before compression of the content causes bandwidth to expand which negatively impacts on compression efficiency. (ii) In compression- this algorithm performs combined compression and encryption. This algorithm implies changes of both encoder and decoder which might affect on format compliance and condensing friendliness. (iii) Post compression- this algorithm performs compression after encryption. This class is generally condensing friendly.

G N Devraj et al. [6] has implemented automated anti- piracy system The media and other websites where people can view content are being invested in to entertain people with content . They capture the video with mobile phones or digital cameras, upload it to websites, or sell it to people, and this goes on and on, causing enormous losses for those who make films. The hardware components used are Arduino UNO microcontroller, Power supply, LCD display, Node MCU, RFID, Relay, IR LEDs. Here there are 2 major levels involved . First, the smart card held by the appropriate theater officer consists of information that is checked against pre-recorded reference information stored . At this point, the comparator's digital output is supplied to the optocoupler, ensuring electrical isolation between the comparator and the drive, which in turn prevents the comparator's reverse current from flowing. The driver, which is made up of pairs of Darlington transistors, receives the signal from the comparator and amplifies and inverts it there.. Second level authentication are performed . When microcontroller is switched, keyboard located on the microcontroller is used to enter the code or a key, where user can enter the password. correct password will be entered and verified, result of the controller is passed through controller via a buffer that provides impedance matching between the two. Since the output from the microcontroller will be low, To control the IR LED, the controller amplifies and turns on the relay.. Signals that are transmitted by IR LEDs located behind the screen covering the entire area behind the screen are broadcast towards the audience. So this invisible light distorts the camera's video quality features. The footage shown on the screen is obscured or jumbled for the audience viewing the movie by positioning IR LEDs behind and around it in the theatre.. The main

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

security feature used here is Video Steganography which hides the data. The encryption and decryption process is done using this concept. Video steganography hides a secret key that is used to verify a password. All the secret data is hidden inside the video frames using MATLAB software.

T Asborn et al. [7] have used Infared Leds which will emit Infared light which not visible to the naked eye. Cameras usually detects the Infared light which human eye can't see, when such inf hits the camera module it causes major disturbance to the video quality which results in an unpleasant or unwatchable format. Here a brief system is made where the authors have tried explaining a system where in Infared waves are projected towards the audience when some tries to use their tabs/phones/digital recorders of any kind they won't be successful to get a watchable quality video. Here we can see that in this Antipiracy Screening System is not able to switch ON or in case of short circuit then, the program will help to identify the culprit using the buzzer and LED. The components mainly used are mentioned and explained a fuse protects any electrical circuit from overcurrent by acting as a safety device. A step-down transformer is that transformer whose primary voltage is higher than its secondary voltage. The main purpose of the component rectifier is to convert alternating current into direct current. Voltage regulator, a device used to design to maintain a constant voltage level automatically, The Arduino Mega is a microcontroller board grounded on the ATmega1280. LED light panels with some indicator lights give a visual indication of system status at one glance. A projector is nothing but an output device that projects an image onto a white screen or wall or any other larger surfaces an A special type of LED called an infrared light emitting diode emits infrared light with a wavelength between 700 nm and 1 mm. 4x4 matrix keypad arrangement is mainly used to reduce the pin count. LCD Display is a mechanism used for displays in the phones, tabs, in few digital cameras, desktops, billboards and computer. Hence, this mechanism that claims to prevent the illegal camera recording of movies in theatres. Therefore, it targets the illegal practises made with digital rights. The Infared that are emitted makes the captured video useless.

Chandana P S et al. [8] has used RFID tags, so these rfid cards which are unique to one another is distributed and assigned to that particular movie. Only via this card and the authorized person can start playing the movie. The rfid cards that are issued, so whoever is the authorized personnel has the right and is allowed to play the movie, other than the appointed personnel no one will be able to play the movie, but when someone else tries the appointed personnel will be notified with the help of a message. Thus, by using rfid cards they are able to allow only authorized person which prevents in pre-releasing of the content. Now IR Leds are placed in all over the screen and around its perimeter. As we know IR led cannot we seen through the naked eye of the human eye, but when when a digital camera or a phone camera is placed and tried to watch or record to that a disturbance is created which causes unclear view of the content. We know that the spectrum of visible light is 400nm-700nm, IR light emits at a spectrum of 700nm-1000nm and infrared is transmitted from 700-780nm which causes disturbance in the camera lens. The lowlevel rays are present from 400nm, where a high-level range can vary more than 700mn. These ranges which are stated causes major disturbance in return we don’t get to capture good quality video.

Hasshi Sudler et al. [9] has explained about the effectiveness anti- piracy system.In every conceivable industry, including music, movies, media, and crucial software that is readily copied and sold, piracy is a big problem. The rapid growth of the broadband connections and high-speed mobile networks the world wide web can be accessed very easily so it's very hard to track every individual data and people's behavior tends to change in accessing pirated copies without care of any digital rights that have been published. The use of digital rights management (DRM) to prevent piracy has failed. Today, 42% of all internet transactions are pirated (Wikipedia, 2012). Although the United States' (21%) percentage of internet piracy is considered modest by international standards, other areas' average rates might reach 88%. (Wikipedia, 2012). Come to a conclusion that the point is in the present era is very hard to find the difference between original and the duplicate one cause of the immensely high quality used in the pirated products. To track down we got to identify the main supply chain that have been majorly altered, new ones can emerge anytime. Even in new eco systems the pirate content is choose offer the paid one. Many schemes like digital rights and several others seem to be proven very ineffective by not dropping the piracy.So the only we can tackle these problems is by joining appropriate technology we have with well-planned business models which are being followed by mega big companies like Apple Inc, Hulu extra where they have been successful when compared to the majority of companies found out there. So combin9ng innovative business models with anti-piracy technologies rather than depending on single technologies like Digital rights management.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

A M Prasanna Kumar et al. [10] have used video stenography which ais a popular encryption and decryption algorithm. Encryption algorithm here at first step of the process of encryption is done to obtain a stego image by involving embedding the undisclosed message into cover image, after this encryption is done all over the image, the stego image is nothing but a image which is very close to the original image but with a secret message encrypted within the image. Now when the message is received it under goes decryption which involves in getting the message out of the encrypted image. Similar to encryption, decryption is carried out onto the the stego image. Ther final step is exact opposite of the encryption process. IR light is unseen to the naked eye of the human being so it doesn't generate any disturbance when watched directly by the viewers but while watching other than the original footage becomes distorted or disturbed when the identical IR rays strike the camera, so the he recorded video in poor condition to watch.

Zhongpai Gao et al. [11] have come up with a new technique where a projector is used to prevent privacy. This project uses a technology called Temporal Psychovisual Modulation (TPVM). We know that the human vision is the integration of millions of light rays and for a continuous picture of what is happening around us, likewise a digital video is integration of several frames that is broadcasted at a very high speed. Digital video uses discrete sampling and has a blackout period between each sampling cycle. Considering this difference of blackout period, the integration of frames of the movie will be displayed continuously to the human eye but when it is recorded using a camcorder, high level of disturbance is observed. The DLP takes 24, 27 or 30-bit RGB data at 120-Hz frame rate and this frame rate includes three colours: red, blue and green. A time slot of 2.78 ms is allocated for each colour. A bit plane is one bit representation of all the pixels in the image. The design of information security is based on TPVM is implemented here. The frames are divided into odd an even frames and each set has a particular pattern assigned to them. The disturbances that are produced are of three kinds: the interference pattern, the coloured fringes and the flashing of the frames. The video that has been recorded will have the above listed disturbances and will be evident that it is a pirated video. This system plays dual role by not only prevents piracy but also helps in determining the location from where the act of piracy has taken place.

B P Arjun et al. [12] have developed a tracking system to detect the person/persons pirating the movies. They have also implemented an IR LED screen which is placed behind the theatre's screen. This project uses a Matrix keypad, GSM module, Microcontroller, ALCD, and an IR LED screen. A card is given to each person entering the theatre to store their information, for authentication purpose. A unique ID will be generated and sent to the person for verification. This process is done via the microcontroller and a GSM module. If the user tries to record the movie, the IR LEDs glow and the movie cannot be recorded and also the pirates can be identified using the details provided by them. The GSM Module and the information embedded in the movie/recording helps them to pinpoint the location, timings of the pirated movie and the details of the projectionist present while the piracy has taken place, therefore this system not only provides anti-piracy techniques to remove piracy, but also provides details of the pirate in case there is a failure of this system or in the cases where piracy has already taken place. Hence this system can be proven to be very effective in many scenarios.

Anusha C R et al. [13] has developed an anti-piracy system by: Designing Infra-red based screen to avoid recording. Steganography Technique to hide secret key to avoid piracy and GSM based alert to inform the authority about piracy along with the location using GPS. In this technique, the property of spectrum of light that isn't visible to naked eyes, i.e. the light-weight rays IR and ultraviolet radiation cannot be detected by human eyes. Whereas the camera lens can detect them. The innovation within the project lies within the design, they use IR semiconductor diode transmitters which are placed on the corners of the screen emitting high intensity of infrared rays beside the flick projection. First, the user is checked by asking for the passcode in order to continue the process, if the wrong password is input an alarm is set off and the location and alert is sent via the GPS and GSM systems embed in the main unit. A special message is encoded into the projected video itself by using steganography techniques and IR Rays are blasted throughout the audience to prevent piracy of the movie. This system can be used to alert authorities early in the piracy process by checking for the passcode provided to authorized personnel, it has functions which enable the system to be used in both prevention and detection of piracy thereby drastically increasing its utility.

Sanath et al. [14] have developed a project that aims at preventing piracy in the theatres. They have built a screen that gets embedded at the back of the theatres' screen and emits IR rays that is only visible to the lens of the camera. The devices used in this project are: a smart card with a built-in microcontroller, comparator, keypad, opto-couplers, driver,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

buffer and a relay. The comparator is used to verify the authentication of the user. The keyboard is used to enter the password that needs to be filled during the authentication process. The relay switches are used to control the IR LEDs, works on the principle of electromagnetism. In this technique, the property of spectrum of light that isn't visible to naked eyes, i.e. the light-weight rays IR and ultraviolet radiation cannot be detected by human eyes. Whereas the camera lens can detect them. The anti-piracy screen is the main system that works for preventing piracy. This screen is activated by the two step authentication process. The password is entered by the owner of the theatre once the keyboard is activated. Once the screen is turned ON, the IR LEDs start to blink continuously at a particular frequency. These rays are not visible to the naked eyes as they are beyond the visible light spectrum range, but are clearly visible to the camera lens. Hence, the capturing to the movie is not possible. The authors claim this project to be cost effective because of the low cost of IR LEDs, easy to implement and also is an effective way to cut down on piracy that effects the cinema industries.

Rajesh Kumar et al. [15] have developed a system which prevents Piracy and recording of the screen in a Theatre. Their system uses a microcontroller to authenticate people in charge of the theatre to turn the projectors on and off and they have designed the system in such a way that if the user is authorised, first the anti-piracy system turns on, only then will the movie start screening. They have used Arduino Uno as their main board to control the electronic components in their system, such as Servo motors, Relays, Keypad, IR Receivers and Transmitters. The working of this system is very simple, as it checks for the authorized person to start the screening via a keypad provided in the system, if the passcode is correct, the IR transmitters are turned on by the Relay. These transmitters are rotated with the help of Micro Servo motors which changes the direction of the IR Rays blasted by the Transmitters, these IR Rays distort the image or video being recorded by a camera thereby preventing piracy. If the passcode entered is wrong, the system itself shuts down so that the movie is not screened. This system is said to be the cheaper and efficient way to prevent piracy with its simplicity and ease of installation, but the amount of distortion in the image depends on number of IR Transmitters used in this system and their distance from the screen.

Nitesh Kumar Dubey et al. [16] have proposed an idea for audio watermarking and also have provided a review on the papers on current watermarking techniques and detecting techniques used for anti-piracy systems. The watermark embedding process is done on the host video i.e the movie, which gives us information about the theatre it is being played on and the show timings of the movie, this in turn helps cyber police or other authorities to detect the exact location of where the piracy is taking place. The detecting process helps us find the position and estimate of the seats where the video was recorded and therefore any camcorder video released on the internet can be narrowed down to the theatre and seat on which the pirate was sitting on and using the database of ticket distribution, the pirate can be caught. The audio watermarking is used for detecting the exact position of the pirate by performing a maximum-likelihood analysis on the entire recorded signal. Different watermarked signals are provided to each of the speakers in the large auditorium, therefore the recorded audio will have watermarked signal of different strengths and delays, which is then used to find the position and seat number of the pirate. Many of the techniques have been reviewed and theoretical solution for audio watermarking and its detection has been provided, which must be tested and implemented in current anti-piracy systems.

Yuachun Chen et al. [17] has built a tracking system using the temporal psychovisual modulation technique. (TVPM). Working of the human eye is based on the constant integration of several images (light rays) captured by the eye. Likewise the digital video works on the similar basis where, it is the integration of the discrete samples which contain a "blackout" period for each sampling cycle. TVPM uses the difference between the perception of the eye and the digital video image forming. Based on this the movie is divided into several different frames and is projected at a very high speed. The human eye cannot make out any difference but shall be clearly visible to the camcorder. This model is divided into three parts: Patterns are embedded on the frames, these frames are projected onto the screens. The visual quality remains intact for the viewers but is heavily degraded for the camcorders. If a pirated version of the movie has been uploaded then based of the pattern that has been embedded on the frames, the information about the theatre and show-time can is revealed. The last part is the identification of the pirate. This is done by the position estimation system. The part of the seating where the pirate is can be recognised and with the help of ticketing system or authentication systems, the information regarding the pirate can be determined. This project mainly deals with the first and the second part and the third part is used for future research purposes. The pattern that are embedded on the screen can either be the details of the theatre, show-time or a QR code. By this the identification of the theatre where piracy has taken place will be much easier.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

III. METHODOLOGY

Initially, the movie is encrypted to make is secure. The theatre owner must request a key (OTP) to activate the IR LED screen and to decrypt the movie. Once the request is sent, an OTP is generated. The theatre owner needs to enter the OTP and once it has been verified, the movie that has to be displayed will be decrypted and played, simultaneously IR LED screen is also turned ON. The IR LED screen cannot be switched off while the movie is playing, it will continue to emit infrared rays until the very end of the movie. A different OTP is generated for each show at the theatre. A GPS module is placed behind the IR LED screen. Using this, the location can be tracked and the same can be displayed on the IR LED screen. By doing so, the location of that particular movie cinema hall can be known in case of attempt to piracy and can take stern actions. The location will be projected on an IR LED screen, which is placed behind the theatre screen where the content will be played. This whole system works simultaneously so that the cinema hall owner can't play the content without the content owner notice and record it. The location of that specific cinema hall will be illuminated with the aid of an IR LED Transmission screen, making it inappropriate to pirate the material when others who are seeing it attempt to capture it. A different key is produced every time to increase security. The projector and IR LED transmission system are shut off after the content is finished.

A. ALGORITHM

1. Request put forth by the theatre owner.
2. Generation of OTP.
3. The theatre owner enters the OPT.
4. Decryption of the movie and the anti-counterfeit screen turns ON.
5. Input from the GPS is fed to the code.
6. The theatre name/location is displayed on the IR Screen.

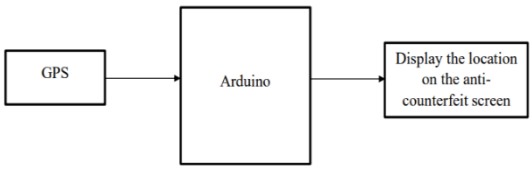

Fig.3.1. Block diagram of the system

B. WORKING

The encryption and decryption of movie file is being done using sanzan library and FFMPEG package in python.The film maker will encrypt the movie video file.By verifying the OTP, the video file's encryption is decrypted.The decrypted file code is executed and prompts the theatre Encrypt the movie file Check if it is an authorised user? OTP is not generated Send the OTP to the theatre owner Decrypt the movie file and play OTP verified? Display “Invalid OTP” Anti-Counterfeit System for Theatres Dept. of ECE, KSIT Page 17 owner to input the user ID that the producer has assigned and given to each theatre owner individually beforehand .The producer has to maintain a database of individual theatre owner’s user ID and their respective e- mail IDs.This is achieved using a firebase which is a backend cloud computing service.The theatre owner is first required to input his assigned user ID.The account ID is then validated.This results in first level of authentication. Afterwards, it generates an OTP and emails it to each theatre

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

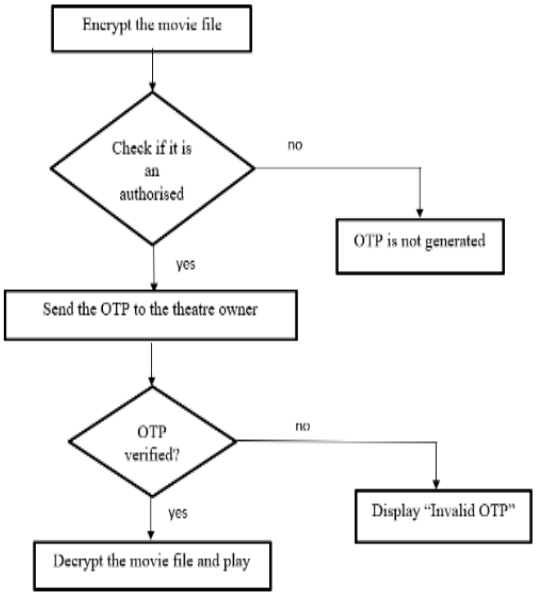

Fig.3.2. Flowchart of the software

owner separately.The owner of the theatre must input the received OTP.The encrypted video file is decrypted and the movie begins to play immediately if the OTP entered is accurate.The OTP verification acts as second stage of authentication.The decrypted movie only plays once in this instance and cannot be downloaded.The OTP will vary depending on the theatrical show. The boards with integrated IR LEDs are located behind a movie screen.It is made to turn ON while the movie is playing, it will be made to emit infrared rays continuously until the end of the movie..These IR LEDs, which are sensitive to camcorders, will display a random message instead of the movie ,that is being shown on the IR LED screen when a spectator tries to capture the movie.

IV. RESULTS

A. SOFTWARE RESULTS

The technology encrypts video files with a special key (OTP), which is securely sent to authorized theatre owners who can decrypt the files. The authorized theatre can decrypt the movie file using a secure key, which reverses the encryption process and recovers the original file. This prevents piracy and ensures that only authorized personnel can access and distribute the content. The output of the software component that was used is shown in the following.

1. Encryption of movie file

The producer encrypts the movie file.In this part the source video file is encrypted using OTP. During this process with the FFmpeg package we sperate the audio and add noise to the video making it unfit to use it even in case some access it without decrypting it.

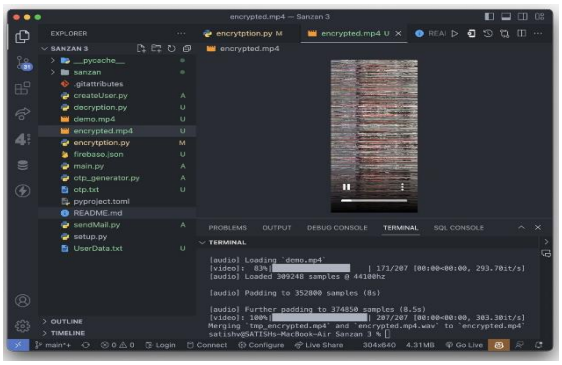

Fig 4.1. Encryption of movie file

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 4, April 2023

DOI: 10.17148/IARJSET.2023.10456

2. Generation of OTP

When a theatre owner requests access to a movie file after user authentication, an OTP is generated. Random python package is used to generate the desired random number of digits length for the OTP. SMTP Lib has been used to send the OTP to the users registered mail ID. For generation of the OTP we use a custom random OTP generator function, in order to generate unique OTP digits for the authentication.

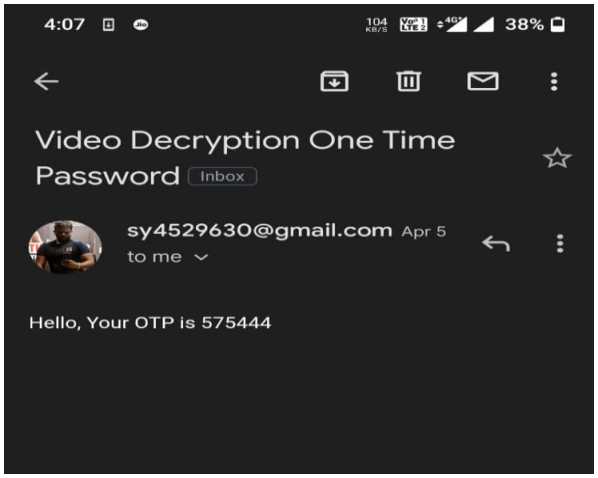

Fig 4.2. Generation of OTP

3. Decryption of movie file

Once the OTP verification is done successfully at producer's side, the encrypted file is decrypted using the OTP which is sent to User's registered Mail Id using the SMTP library and start playing automatically without saving locally.

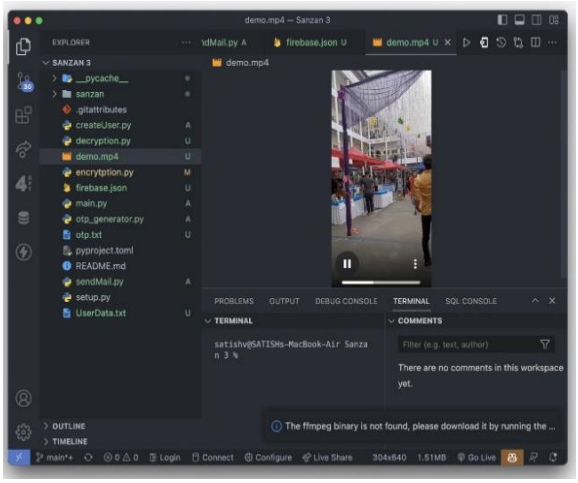

Fig 4.3. Decryption of movie file

V. APPLICATIONS

- Discourage piracy.
- Theatre information displayed using IR LED system is useful in tracking the place of piracy.
- Encryption of films decreases the loss faced by the content owners in the film industries

V. CONCLUSION

Though the increase in piracy seems harmless, the usage of pirated movies by people has led to a decrease in the number of audiences in theatres which creates a cut in revenue collection and even a loss in employment. Our idea for an IR-LED-based anti-counterfeit device substantially reduces the visual quality of the recorded video. We have encrypted the video material to increase security, and a key is required to decode it, the key that's going to be generated is unique for

DOI: 10.17148/IARJSET.2023.10456

each input. We've put in place a GPS module that will show the theatre's name on the IR LED screen in order to detect piracy. As a result, we have attempted to eliminate all methods of piracy possible.

REFRENCES

1. P. Bourdon, S. Thiebaud, J. -J. Sacré and D. Doyen, "A metamerism-based method to prevent camcorder movie piracy in digital theaters," 2010 IEEE International Conference on Multimedia and Expo, Singapore,pp.468473,doi:10.1109/ICME.2010.5582547, 2010.
2. Yan, Fei, Abdullah M. Iliyasu, Salvador E. Venegas-Andraca, and Huamin Yang. "Video encryption and decryption on quantum computers." International Journal of Theoretical Physics 54, No. 8, pp-2893-2904, 2015.
3. Maniccam, Suchindran S., and Nikolaos G. Bourbakis. "Image and video encryption using SCAN patterns.", Pattern Recognition 37, No. 4, pp: 725-737, 2014.
4. Iyer, Sridhar C., R. R. Sedamkar, and Shiwani Gupta. "A novel idea on multimedia encryption using hybrid crypto approach.", Procedia Computer Science, No.79, pp:293-298, 2016.
5. Massoudi, Ayoub, Frédéric Lefebvre, Christophe De Vleeschouwer, Benoit Macq, and J-J. Quisquater. "Overview on selective encryption of image and video: challenges and perspectives.", Eurasip Journal on information security 2008, No.1, pp:179290, 2008.
6. Devraj, G. N., SG Mangala Gowri, and D. Bharath Raj. "Design and Implementation of an Automated Anti-Piracy System.", International Journal of Modern Developments in Engineering and Science 1, Vol. 5, pp:1-4, 2022.
7. Asborn, T., L. Prem Kumar, S. Michael Jose, and M. Santhosh Kumar. "Anti-Piracy Screening System." , Volume 6, No. 2, pp:238-241, 2019.
8. Chandana, P. S., D. M. Rekha, and H. M. Akshatha. "Movie Piracy Reduction using Automated Infrared Transmitter Screen System and Steganography Technique." International Journal of Engineering Research & Technology (IJERT), Vol. 13, 2020.
9. Sudler, Hasshi. "Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy." Business Horizons 56, No. 2, pp:149-157, 2013.
10. Kumar, AM Prasanna, and Bharathi Gururaj. "Deterrence of Piracy Employing IR Transmitter and Steganography System.", Vol. 1, No. 2, pp:32-40, 2021.
11. Gao, Zhongpai, Guangtao Zhai, Xiaolin Wu, Xiongkuo Min, and Cheng Zhi. "DLP based anti-piracy display system." In 2014 IEEE Visual Communications and Image Processing Conference, pp. 145-148, IEEE, 2014.
12. Arjun, B. P., N. Harshavardhana Reddy, H. S. Bharath, and B. Poornima. "Movie piracy tracking system using video steganography." Int J Res Eng Sci Manag, Vol.3, No. 2, pp:665-667, 2020.
13. Anusha, C. R., Y. Ashika, N. Meena, D. B. Pratiksha, and B. Durdi Vinod. "Review on movie piracy reduction using infrared transmitter screen, steganography technique and GSM based alert system." J Remote Sens GIS Technol, Vol.5, No. 2 pp: 19-21, 2019.
14. Nagarathna, N. "Anti-Piracy Screening System.", International Journal of Engineering Research & Technology (IJERT), Vol. 9, No. 05, pp:982-984, 2020.
15. Kumar, BVV Rajesh, B. Akhil Vardhan, CH Rahul Gupta, and P. Surekha. "Reduction of Movie Piracy using an Automated Anti-piracy Screen Recording System: Anti-piracy Screen Recording System." In 2019 4th International Conference on Information Systems and Computer Networks (ISCON), pp. 301-304. IEEE, 2019.
16. Dubey, Nilesh Kumar, and Shishir Kumar. "A review of watermarking application in digital cinema for piracy deterrence." In 2014 Fourth International Conference on Communication Systems and Network Technologies, pp. 626-630. IEEE, 2014.
17. Chen, Yuanchun, Guangtao Zhai, Zhongpai Gao, Ke Gu, Wenjun Zhang, Menghan Hu, and Jing Liu. "Movie piracy tracking using temporal psychovisual modulation." In 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 1-4, IEEE, 2017.

