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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

# PREVENTION OF THEATRE PIRACY: A SURVEY

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

Student, ECE, KSIT, Bengaluru, India[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 REVIEW

[1]. A.K.Veeraraghavan et al. to decrease the problem of piracy, suggests the idea of infrared blasters, which is placed in the projector circuit which is helpful in sending high infrared rays .infrared blaster and projector work together as one with synchronization. The blaster sends the burst of IR digital cameras placed in front of the film screen. when placed in the projector circuit, it also emits Infrared light beams in addition to the visible film projection light beams. Here, it is mostly influenced by the parameters of the radiation's frequency and wavelength. These variations are done using microcontroller. The person who is trying to record the movie by using camera should use more filters to avoid the effect of IR which is most difficult and not possible. The author of this particular paper proposes the idea of merging invisible light beams with the original visible rays. here the projector will send high intensity of infrared rays with the film projection. IR burst a transmitter is placed in the projector itself .Both the infrared blaster and projector will work together as one with synchronization. The blaster send the burst of IR radiations which are reflected back to the audience which is invisible for them but visible to cameras while playing the movie. The person who is trying to record the film will get distorted images in the recording camera.IR burst transmitter is the main hardware used in this project which helps in reduction of piracy. It should be used of high intensity because it reduces the clarity of the image. The transmitter helps in changing the frequency and wavelength of IR beams. LED is the most important part of the hardware part of this project with the variable frequency attached to the IR burst transmitter. The basters used is not of direct infrared as it affects the human eyes .the main drawback of using infrared is produces lot of heat, this is a avoided using the air conditioner in the theatres and as the film screens are white in colour, the absorption of heat is very less.in this project, they have used a definite program to filter and improve the clarity of both video and audio of the film or movie. Instead of using normal projector in theatres they have come up with the projector which has combination of both IR blaster and projector which works in sync to prevent or decrease the rate of piracy. When the wavelength of IR rays keeps on

  

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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

changing during the play of the movie, the one who tries to record has to keep on separating the filters due to restriction of the filtering capacity of the commercial filters. the wavelength of rays keeps on changing in small intervals using IR blasters because of the person recording may have more filters to filter the rays .The future scope of this project is to use this idea beyond theatres in public or private meetings or in government organizations where installing electronic jammers is not feasible.

[2]. P. Vijayalakshmi et al. has tried to implement new technology which helps to curb the piracy. He has introduced Temporal Psycho visual Modulation [TVPM] where it helps to differentiate between human eye view-point associated camera image will form an unseen able pattern on the digital screen and projector. At each sampling cycle some amount of video recorded is fainted out to reduce the quality of recorded frames. The motion picture which has specific group of frames has certain designs and broadcast them quickly so that viewers will not be able to recognize the difference but the video recorder will be knowing because the camcorder will contain extreme objectionable artifacts. Several watermarking solutions are envisioned as a preventive measure against the video camera piracy. The primary goal of these methods to instil an observably message into the visual presentation. The notification suggests the instrument of distribution, the rostrum the day and the hour the video was telecasted and possibly information identifying the skilled worker. The messages from the unauthorized films can be retrieved to identify the individual or group who has for the unapproved unharness if the Movies are illegally downloaded and pirated. are distributed through the online or other channel. Following information serves as a rhetorical tool that provides information to the content owner to assist control the pirate issue, and a deterrence to future infringement.

But Two issues exist with watermarking techniques. First, because of the inability to actively prevent or counter camera piracy. The tags in the illegal downloads are unnoticeable and not offensive enough. Another one is, the steganographic change must be impalpable both visually and acoustically. The image watermarking approach may nevertheless leave behind certain sensory artefacts, and the visual material shown in the theatre may also be impacted. In system applications, there are mainly 3 steps involved as mentioned, they are pattern embedding, pattern extraction and frame conversion. In pattern embedding, According on TPVM screen technology, unlicensed movies captured on camcorders will have certain artefacts that drastically lower the image quality, but not the visual appeal of viewers. Coming to pattern extraction, the theatre and show time where the unauthorized movies were produced may be found using the tracking data. exposing the organization's role in the unauthorized release and encouraging it to strengthen its anti-piracy preventative measures. In frame conversion, the video is converted into total number of frames. In the TPVM design, a show with a faster refresh rate distributes atom frames, and separate viewers can independently see self-directed pictures by fusing the atom frames optically electrically and psycho visual in cascading using their own HSV and display-synchronized altered viewing equipment. This procedure gives the TPVM show paradigm the desirable capability of running numerous exhibits concurrently on the same screen, considerably enhancing the usefulness of digital displays. Designers provide a summary about the dual view screen's heuristic algorithm and suggest an iterative technique to enhance the systems' overall performance on how the human eye's spatial integration takes shape. Author also includes that future enchantment can be done through improving security safeguards by enabling low-cost encryption key. It displays a specific time and date.

[3]. Takayuki et al. have developed a project that aims at preventing piracy in the theatres. This IR-cut filter is added to the camcorder's lens so that it will be horizontal to the screen that's because the device must be directed at the screen to be utilized for illicit recording. An IR camera placed behind of screen may pick up the IR rays that is the filter secularly mirrored.IR noise emission systems are used to contaminate recorded information with unwanted noise that are undetectable to the human eye but are detected by cameras' CCDs or CMOS sensors. A visible region cut filter-equipped IR camcorder is positioned in the middle of the screen behind it, with IR emitter filters in units recognition newly connected on a regular basis. . For studying the IR light emitted from different surfaces, a PC application is employed. The plane IR-cut filter has many dielectric layers and returns infrared light from various directions within one outgoing direction. The non-specular surfaces reflect the incoming IR light in diverse ways due to their varied forms and surface properties (diffuse reflection). The specular reflection pictures captured by the IR camcorder may be used to analyse the images of the algorithm for detecting filters, which can then identify an IR-cut filter. The LEDs for filter identification are positioned around the recorder, which is positioned in the middle of the screen behind it. The IR camcorder detects the IR light that the IR-cut filter reflects and travels through the screen's speaker holes. It was a square filter that was used to cut IR. The authors conclude that since the filter was found in less than a second, real-time detection is feasible. Thus, even when camcorders have an IR-cut filter, the improved approach may still be utilized to find them being used illegally in movie theatres. The technique has been improved and now will be able to recognize the IR reflection coming from an IR-cut filter and this improvement allows the technology to detect video recorders with a connected IR-cut filter, according to testing with our prototype system.

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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

[4]. Othman O. Khalifa et al. have proposed multimedia encryption schemes. In this study, various encryption techniques and typical video algorithms were described and compared. Considering their stream size, security level, and encryption speed, among other things. The trade-off between the stream's quality and the encryption algorithm of choice was demonstrated. The goal for authors was to achieve efficiency, adaptability, and safety. They have tried to explain about the different types of symmetric and asymmetric encryptions algorithm. In symmetric key encryption, both the transmitter and the receiver use the same key for encryption and decryption. Symmetric keys can ensure secrecy, but they cannot provide authentication since it is impossible to use cryptography to determine who really transmitted a message if two people are using the same key. Despite their limitations and issues, symmetric keys are still used in many applications since they are so rapid and may be difficult to break if using a large key size.. Asymmetric keys would take too long to encrypt and decrypt massive amounts of data, whereas symmetric keys can handle it. For the encoding of PIN numbers, financial transactions, and other data, the DES is frequently utilized. The input key has a parity check bit per eighth bit, effectively reducing the key size to 56 bits. Two keys are utilized in the public key algorithm. There are two types of keys: a public key that anyone can access, and a private key that should only be shared by the owner. Using the sender's private key, the data would be encrypted if it was necessary to authenticate. and the data might be decrypted by anybody who holds the related public key. The data was encoded by an individual who has access to that private key, so the receiver can be sure of that. thanks to this. The author has even mentioned about the difference between symmetric type of encryption and asymmetric type of encryption also mentioned about the digital video encryption methods like It contains sub 4 algorithms for the native algorithm, pure permutation method, zig-zag permutation algorithm, and video encryption algorithm. After analysing all algorithms, the author gives a conclusion that video encryption algorithm is the best because it offers good security across the board, size preservation, and reasonably quick encryption and is able to satisfy the needs of the majority of multimedia applications. Any other approach experiences problems with either poor security, slow performance, or escalating stream size. In this paper video encryption algorithms for video streams were described and is conclude that choosing an encryption technique for an MPEG video stream involves trade-offs and depends on the intended use.

[5]. Howard Cheng et al. has proposed a novel solution called partial encryption where Only a portion of compressed data is encrypted using an encryption algorithm. In data decomposition, the algorithm is firstly divided into two parts namely important parts and remaining part which is not important in the original data. The partial encryption is done only to the important part of the original data and this technique also supports in transmission of important part first and unimportant part later if necessary. They have expected that one of the partially encryption approaches is utilized for intraframe coding. Furthermore, it has been found that low resolution photos are secure against tree authentication attacks when using partial encryption, and that the security of zero-tree oriented partial encryption techniques is not significantly impacted by image resolution. The movies are protected by encryption. A motion vector is computed for each block of the current frame in common motion compensation algorithms, which divide it into units of a fixed size Combining these camera motions is thought to be more effective, even when numerous blocks referring to the same item may contain motion vectors that are identical or comparable. The other method of encryption is Quad tree encryption, Top-down or bottom-up implementations of quadtree compression are both possible A full quadtree of height n serves as the starting point for a bottom-up implementation of the method. First, the topmost level of the quadtree is inspected. If 4 child leaf nodes are homogenous or comparable, they are merged. This is replayed at the next highest level once there appear to be no branch endings at a level or if the root is reached. Since it is more effective, a bottom-up approach is frequently favored in practice. In order to speed up the processing and transfer of images and videos, partial encryption has been presented in this study. The computation time for both decryption and encryption is greatly decreased for both photos and movies. It is practical since it is simple to implement and to compute. They come to the conclusion that partial encryption can help secure picture and video communication processing by lowering the encryption and decryption times.

[6]. Min ku lee et al. has suggested approach falls under the category of SEA-based methods. It varies from many other SEAs, though, in that it may be used on top of a video codec. Traditional SEAs were made to rely on the video codec and the techniques used in the video decoder and encoder for video both encryption and decryption, respectively. The video security algorithm is therefore difficult to distinguish originating from the video autoencoder. Traditional SEAs with accompanying video compression methods in this regard are less practical since, in order to include the video encryption methods, they need to modify the industry-standard video compression algorithms. The suggested technique is intended to operate without the need for video codecs or video security systems. This was made possible by using the video ciphertext before decoding and the video encryption algorithms after video encoding. The suggested approach encrypts a crucial portion of the bitstream that controls the decoding process and is close to the initial code in the video binary data, as opposed to typical SEAs that encrypt specific syntax components throughout the entire video bitstream. The initial bitstreams employed in all studies were 146 compliance bitstreams with a variety of NAL subcomponents compressed using different HEVC encoder parameters. When the bitstream encoded using the suggested techniques is decrypted with the HEVC decoder, the encryption was tested to see if decoding was feasible. The results demonstrated

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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

that the bitstream encoded using the current SEAs could be decrypted and that the encrypted reconstructed video had a poorer video quality. The proposed approaches, however, were unable to decode the encrypted bitstream, and no video data was discovered. Consequently, the suggested techniques were more secure than the current SEAs. In this paper, they suggested a brand-new architecture for selective encryption and decryption based on the HEVC start code. When compared to the current SEAs, the suggested approaches had a number of advantages. First, since they encoded the area next to the start code, which was often included with the video bitstream, they were irrespective of the video codec. Additionally, unlike the previous SEAs reliant on video codecs did not provide conformance with the standard video codec, The encryption system for video codecs. Second, any data from a movie that couldn't be deciphered was blocked by the suggested approaches. In contrast, current SEAs only partially allow information to be acquired from the decrypted video and suffer from quality distortion.

[7]. Chandana et al. have used an innovative technique to decrease film piracy that occurs from taping films in the theatres utilizing mobile phones or cameras or any other electronic devices. According to these authors this issue can be decreased by embedding IR LEDs(light emitting diodes) behind the theatre screen. They have used IR LEDs because infrared light is not seen to the human eye and hence does not interrupt the viewers but when the same infrared light hits the camcorder or any electronic device it causes some disturbances in the recorded video which results in degradation of the captured videos. The components used in this project are LCD display(16x2), relay, microcontroller, RFID reader, RFID tag, GSM module, IR transmitter, buzzer and a power supply. On turning on the microcontroller using a relay the radio-frequency identification reader reads the distinctive code that is previously generated and concealed utilizing a steganography technology. Once the tag used is verified, the card no: is seen on the LCD, if the card is verified successfully then the LCD display exhibits “movie is ready to play”. If the card is not valid then a notification is sent to the proprietor with the location and the LCD displays “movie is not played”. The main objective of the RFID reader in this project is to protect the authorization of the person who is playing the movie. In this paper they make use of infrared LEDs which are mounted throughout the corners of the theatre screen. They release IR light or rays that are not visible to the human eye but disturb the videos recorded through cameras. This in turn does not harm or distract the audience in the theatres but only blurs the video that is captured. The advantage of this system is it can be used in confidential meetings, research centres, religious spots etc. The main drawback of this project is that the IR tag given to the theatre owners or the authorized person can be lost and misused if lands in the wrong hands. One can forget carrying the IR tag with them which might lead a lot of disturbance in the theatres.

[8]. Zhongpai et al. have explained three methods that prevent piracy of movies in the theatres. The first method explains the projection of microscopic light from the screen to the viewers in the theatre. As cameras are sensitive to infrared rays and ultra-violet rays which is invisible to the human eye, they cause disturbance to any functions of the camera making it impossible to record in theatres accurately. The second explains us the methods for tracking and blinding the recording in theatres. It uses a light beam which is ejected from the screen in the direction of the viewers and is projected back from any metal or a shiny body. The camcorder that is filming can be identified due to the mirroring from the camera lens. Once the camcorder is identified, the ray is sent towards it and makes it impossible for it to record any video. The third method explains the approach of spatiotemporal modulation. In this project design they have developed a method to construct optical signals projected by the movie projector for the purpose of overthrowing film piracy while keeping up visual transparency to theatre viewers. They have used the mechanism of DLP. They use a DLP digital controller which takes input of 24,27, or 30bit RGB data at up to 120hz. This camera frame is collection of three colours i.e., red, green, and blue with each colour divided uniformly.

Each colour has a 2.78ms time slot assigned to them. In this project, they propose an implementation method which is based on the idea of utilizing the mechanism of man eyes and sensors. Due to the blackout period, the camera will not be able to get all the signals projected from the projector. But the viewer can receive the signals by simultaneous combination of light beam which shall not be deprived of any content of picture or video. They suggest that the information based on TVPM can also be utilized in this system. These frames are divided from projector screen into odd and even frames. According to authors, the generated technique must follow two basic concepts. First is to reduce the artifacts to the viewers such that the viewers should only see the content without any disturbance. The other principle is, increasing the inconvenience to the camera to overcome the camera counterfeit which means we need to increase the distance between O/E and I. To avert the grey scale values crossing the scale they made an advancement. In the beginning a binary image is chosen as the interference pattern D. Because of blackout period the videos or image might lose few optical signals, which actually leads to the interference pattern and colored fringes to come out. In this project they have recorded the video using Sony HDR-CX240 handy Cam. The pirated video contains visible and disturbing pattern. The pirated videos have coloured fringes which immensely disrupt the original film. Anti-piracy is successfully gained in this system. But the only drawback is that even if there are colored fringes there is a good visibility of the images in the video.

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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

[9]. Lei Tang et al. includes combining of cryptographic methods with those of digital image processing to produce compression. For greater efficiency, a lengthy decompression and encryption process is followed by decryption in the fewest possible stages. The method used here are practical and providing security while he similar to current video encoding and decoding efficiency algorithms to protect the content without affecting the quality of images when decrypted to retrieve the original image. The methods used here can we highly modified/adjusted to different levels to provide different levels of security based on the users need and confidentiality which can be used in various scenarios of electronic gadgets used these days. One major pro of this paper is that they use methods that are highly used JPEG and MPEG formats. Additionally, the algorithms are tested and evaluated through a series of experimental, to opt for the most efficient methods. First the author has described about mpeg and jpeg.

There is a main special property of digital images which acts as a major advantage to us, it is that we do not need to treat digital image as bit streams and encrypt each bit which will be very time consuming. The main simple idea here is that to use a random permutation list which will further replace the zig-zag order of the digital image to map the 8x8 block to a 1x64 vector. Based on the permutation list we can derive the secret which is 1x64.

Finding the secret key becomes highly tough to crack by using inverse DCT operations in excess to increase the complexity to undermine our plan using an ad hoc approach. So present algorithm used here is basically divided into three main component steps which are followed by generating a list of permutations using 64 cards. After the 8x8block can be quantized, they proceed to finish the splitting process before applying the random permutation list to the split block and passing the outcome to the entropy coding. In this research, we describe a method for combining cryptographic methods with digital image processing methods to accomplish compression decompression and encryption decryption in a single step.

[10]. Peggy et al. mainly focuses on the rapid ballooning worldwide which is highly used by adults and teens. They try to tackle all the main concerning and emerging piracies such has selling counterfeit products which mainly know has Turbulent virtual water, which is rapidly growing of all replicated products on the internet which concerning for well established brands. Also, another major concern they are trying to tackle is the internet piracy pyramid, here they create a market for counterfeit products. The Warez scene is a well-known in the cyber-crime, the software will be cracked, violating the laws and an unpaid version will be upload for other user's access recurring a huge loss for the creator can be accessed by any user creating huge losses for content creators at various levels. Above all these the internet sites which provide access to such content and products, to overcome this authorization of product becomes a significant concern. As they are over millions of websites it becomes very hard to track such piracy, though they shut down millions of websites they will always be new ones emerging day to day.

The main factors developed to overcome piracy and fight against them in the present market are the various enforcement strategies to fight against them, government regulations like the DMCA and operations like Operation Buccaneer. Operation Buccaneer, working closely with its partners in Australia, Finland, Norway, Sweden, and the UK, the US Customs Service to infiltrate the activities of criminals using the Warez scene to distribute movies, video games, and software online. Operational Digital Gridlock These joint operations through person-person networks with direct connectivity, the Underground Network attempted to illicitly distribute over direct use of copyrighted materials to person-person networks. So many such government operated agencies came to act to tackle piracy and illegal counterfeit products.

We can come up to a conclusion that all of this just an beginning in this modern digital era which is going to flood with users daily and they got to grow stronger, improve their tactics to overcome piracy problems which are growing at a concerning level and The battle will take place in a virtual warzone, requiring a thorough knowledge with quantifiable consequences and executive skill that understands the issues related to generating such products and piracy.

## III. CONCLUSION

Though the increase in piracy seems harmless, the usage of pirated movies by people has lead 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 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.

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

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 9, Issue 12, December 2022

DOI: 10.17148/IARJSET.2022.91211

## REFERENCES

[1]. Veeraraghavan, A. K., S. Shreyas Ramachandran, and V. Kaviarasan. "A survey on reduction of movie piracy using automated infrared system." International Journal of Innovative Research in Computer and Communication Engineering Vo.5, No.11, pp: 16633-16637, 2017.

[2]. Vijayalakshmi, P., G. Aiswarya, S. Vishali, and R. Thirumagal. "Movie Piracy Tracking Using Temporal Psycovisual Modulation." Int. Res. J. Eng. Technol 6, No. 3, pp:3965-3968, 2019.

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

[4]. Abomhara, Mohamed, Omar Zakaria, and Othman O. Khalifa, "An overview of video encryption techniques." International Journal of Computer Theory and Engineering, Vol.2, No. 1, pp:103, 2010.

[5]. Cheng, Howard, and Xiaobo Li, "Partial encryption of compressed images and videos." IEEE Transactions on signal processing Vol. 48, No. 8 pp:2439-2451, 2000.

[6]. Lee, Min Ku, and Euee Seon Jang, "Start code-based encryption and decryption framework for HEVC." IEEE Access Vol. 8, pp:202910-202918, 2020.

[7]. 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) 13.

[8]. 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.

[9]. Tang, Lei. "Methods for encrypting and decrypting MPEG video data efficiently." In Proceedings of the fourth ACM international conference on Multimedia, pp. 219-229. 1997.

[10]. Chaudhry, Peggy E., Sohail S. Chaudhry, Stephen A. Stumpf, and Hasshi Sudler. "Piracy in cyber space: consumer complicity, pirates and enterprise enforcement." Enterprise Information Systems, Vol. 5, No. 2, pp: 255-271, 2011.