

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

Prevention of Video Piracy through Advanced Video Watermarking

Dharani Kumar R A¹, Dinesh S², Satish Kumar D³, Chitra R⁴

U.G[B.E] Students, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India ^{1,2,3},

Assistant Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India ⁴

ABSTRACT: A standout among the most critical things that have been tormenting the film business for long is video theft. The two most famous types of video robbery are the camera/theater print taping the on-screen projection of a motion picture in a film and the second is the DVD arrange arrival of the motion pictures which are being utilized to print different duplicates. There have been rehashed endeavors and requests to execute robbery and spare the film business. So to overcome from this video robbery we proposed a two strategy in which the video is embedded with watermark. In first manner each time client asks for the video to the server. The server will at first authenticate whether the copyrighted video is watermarked or not. If the video is watermarked, at that point the server will display the error, or else the server will their decline their demand. In second technique, the secret key is generated for the copyrighted watermarking video, in which the server initially ask for secret key then only the video is allowed to upload.

KEYWORDS: Watermarking, Embed, Copyright, Authenticate, Secret Key, Motion Picture.

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Only network security can remove Trojan horse viruses if it is activated. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Video Piracy is the act of acquiring, copying and then selling or distributing a copyrighted video without the consent of the copyright owner. A block diagram illustrating the unauthorized distribution of a copyrighted video. Usually, a movie is first released to theaters and then to digital versatile disk (DVD) after approximately sixteen weeks [1]. Currently, camcorder theft is one of the most significant problems facing the film industry and is the single largest source of video piracy [2]. When this type of theft occurs, a copy of a digital movie is captured from a large-screen movie theater using a camcorder and then distributed worldwide via the Internet without any copyright protection. Approximately 90 percent of the first available versions of illegally distributed new release films are pirated in this way [2]. Although there are strict laws in many countries against cam recording, they have proven to be ineffective and it has not been possible to prevent this practice. An unauthorized user may also create an illegal copy of a movie from a DVD and distribute it through a web server while a pirate may perform different types of intentional and unintentional attacks before uploading a movie to the Internet. Therefore, concern over protecting the copyright of digital video content is increasing [5]–[7]. Several techniques designed to protect video content from unauthorized access include cryptography, steganography and watermarking. Cryptography, which means “secret writing”, comes from the Greek words Krypto’s for “hidden or secret” and graphene for “writing”. It involves processes of communication where a message, called plaintext, is scrambled into ciphertext using a specific key which is then required to retrieve the message. The processes of scrambling and unscrambling the message using this key are called encryption and decryption respectively. The purpose of encryption is to make data unintelligible to unauthorized persons during its transmission from a sender to receiver. However, once the data is decrypted at the receiver’s end, it is no longer protected from unauthorized distribution. As robustness to a geometric attack is still an unsolved problem in the field of digital image and video watermarking, digital watermark is a kind of marker covertly embedded in a

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

II. LITERATURE REVIEW

In 2005, Eugene T. Lin, Ahmet M. Eskicioglu, Reginald L. Lagendijk, Edward J. Delp, published a paper about "Advances in Digital Video Content Protection". The use of digital video offers immense opportunities for creators; however, the ability for anyone to make perfect copies and the ease by which those copies can be distributed also facilitate misuse, illegal copying and distribution ("piracy"), plagiarism, and misappropriation. Popular Internet software based on a peer-to-peer architecture has been used to share copyrighted movies, music, software, and other materials.

In 2002, Christophe DeVleeschouwer, Jean-Francois Delaigle, and Benoit Macq published a paper about "Invisibility and Application Functionalities in Perceptual Watermarking—An Overview". In which they describe about digital watermarking. Digital watermarking consists of hiding subliminal information into digital media content, also called host data. It can be the basis of many applications, including security and media asset management. In this paper, we focus on the imperceptibility requirement for image watermarking.

In 2001, Chun-Shien Lu, Member, IEEE, and Hong-Yuan Mark Liao, publish a paper about "Multipurpose Watermarking for Image Authentication and Protection". We propose a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image's wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image.

In 2000, Chun-Shien Lu, Member, IEEE, Shih-Kun Huang, Chwen-Jye Sze, and Hong-Yuan Mark Liao, publish a paper about "Cocktail Watermarking for Digital Image Protection". A novel image protection scheme called "Cocktail Watermarking" is Proposed in this Paper. We analyze and point out the inadequacy of the modulation techniques commonly used in ordinary spread spectrum watermarking methods and the visual model-based ones. To resolve the inadequacy, two watermarks which play complementary roles are simultaneously embedded into a host image.

In 1999, Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn published a paper about "Information Hiding—A Survey". Information-hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence.

III. PROPOSED SYSTEM

➤ SYSTEM DESIGN

The new copyrighted movie is embedded with a watermark, and it is released worldwide. Any unauthorized user records the movie through cam recorder and then uploaded to the web. New user requests the movie to the server. The server initially authenticates the video whether this video is embedded with watermark or not through the watermark extraction. If the movie is embedded with watermark, then user cannot view the file or download the movie, the server it will decline the request from fulfill. A watermarking algorithm must ensure that the watermark embedded in a host video does not significantly affect the visual quality of this video. A watermarking algorithm is imperceptible if the human eye cannot distinguish between an original and watermarked video. In second technique, the secret key is generated for the copyrighted watermarking video, in which the server initially asks for secret key then only the video

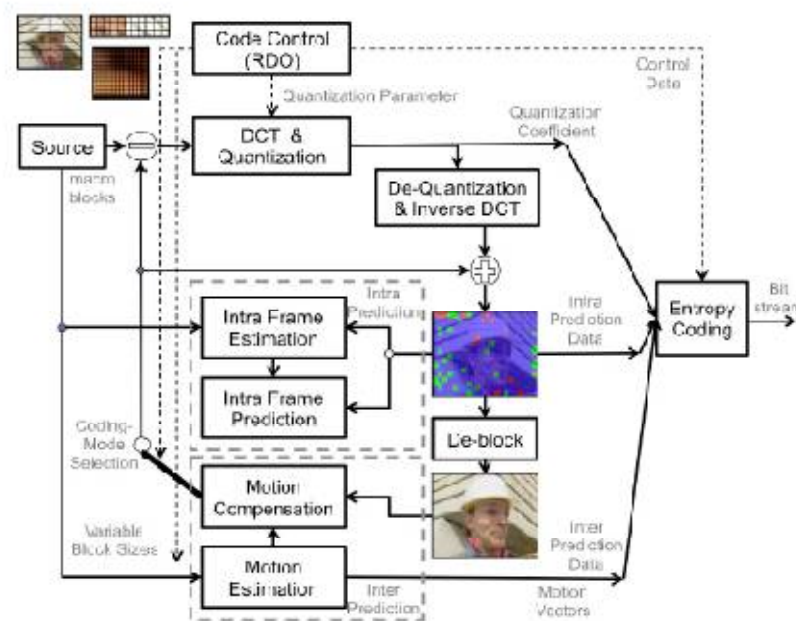
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

is allowed to upload. If the user is not having the valid key, then the user is not allowed to post the copyrighted video which is embedded with watermark.



A. SLICING

In general, a coded picture is divided into one or more slices. Slices are self-contained and can be decoded and displayed independently of other slices. Hence, intraprediction of DCT coefficients and coding parameters of a macroblock is restricted to previous macroblocks within the same slice. This feature is important to suppress error propagation within a picture due to the nature of variable length coding. In regular encoding, when FMO is not used, slices contain a sequence of macroblocks in raster scan order. However, FMO allows the encoder to create what is known as slice groups. Each slice group contains one or more slices and macroblocks can be assigned in any order to these slices. The assignment of macroblocks to different groups is signaled by a syntax structure called the "slice group id".

B. MOTION COMPENSATION

Since MPEG-1, motion compensation is a standard coding tool for video compression. Using motion compensation, motion between frames can be encoded in a very efficient manner. A typical P-type block copies an area of the last decoded frame into the current frame buffer to serve as a prediction. If this block is assigned a nonzero motion vector, the source area for this copy process will not be the same as the destination area. It will be moved by some pixels, allowing to accommodate for the motion of the object that occupies that block. Motion vectors need not be integer values: In H.264, motion vector precision is one-quarter pixel. Interpolation is used to determine the intensity values at non-integer pixel positions. Additionally, motion vectors may point to regions outside of the image. In this case, edge pixels are repeated.

C. MOTION VECTOR PREDICTION

Because adjacent blocks tend to move in the same directions, the motion vectors are also encoded using prediction. When a block's motion vector is encoded, the surrounding blocks' motion vectors are used to estimate the current motion vector. Then, only the difference between this prediction and the actual vector is stored.

D. BLOCK TRANSFORMATION AND ENCODING

The basic image encoding algorithm of H.264 uses a separable transformation. The mode of operation is similar to that of JPEG and MPEG, but the transformation used is not an 8x8 DCT, but an 4x4 integer transformation derived from the DCT. This

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

transformation is very simple and fast; it can be computed using only additions/subtractions and binary shifts. The necessary post-scaling step is integrated into quantization (see below) and therefore omitted. The basic functionality of the H.264 image transformation process is as follows: For each block, the actual image data is subtracted from the prediction. The resulting residual is transformed. The coefficients of this transform are divided by a constant integer number.

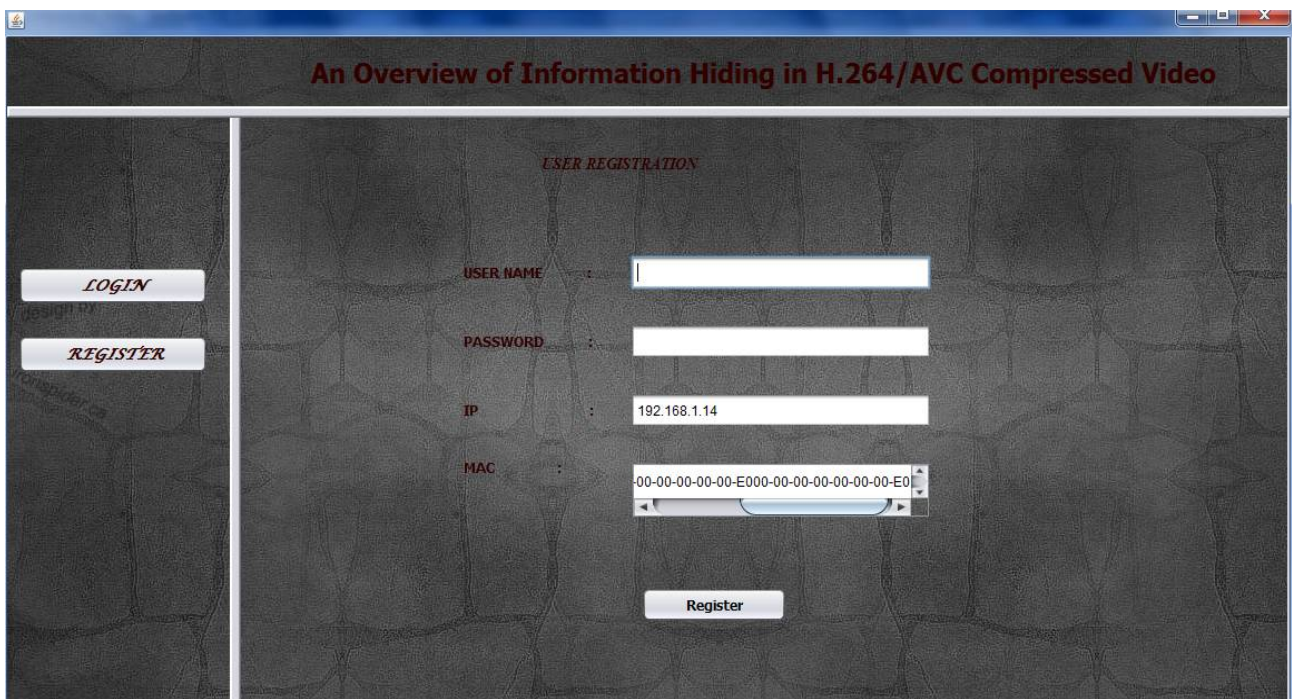
E. MACROBLOCK ORDERING

In this paper, we make use of the explicit assignment of macroblocks to slice groups to hide messages in the video stream. Since macroblocks can be arbitrary assigned to slice groups, we propose to use the slice group ID of individual macroblocks as an indication of message bits. Assume for instance that two slice groups are used, the allocation of a macroblock to slice group 0 indicates a message bit of 0 and the allocation of macroblock to slice group 1 indicates a message bit of 1. Hence, one message bit per macroblock can be carried.

➤ PROPOSED ALGORITHM

Watermarking, which is embedded with a movie contains a secret message inside the host information, is a specific type of information stowing away with an alternate reason than steganography. In proposed system, the new copyrighted movie is embedded with watermark, and it is released in worldwide. Any unauthorized user records the movie through camrecorder and then uploaded to the web. Now user request the movie to the server. The server initially authenticates the video whether this video is embedded with watermark or not through the watermark extraction. If the movie is embedded with watermark then user cannot view the file or download the movie, the server itself will decline the request from fulfill. In second technique, the secret key is generated for the copyrighted watermarking video, in which the server initially asks for secret key then only the video is allowed to upload. If the user is not having the valid key, then the user is not allowed to post the copyrighted video which is embedded with watermark.

IV. RESULTS



An Overview of Information Hiding in H.264/AVC Compressed Video

USER REGISTRATION

LOGIN

REGISTER

USER NAME :

PASSWORD :

IP : 192.168.1.14

MAC : 00-00-00-00-00-E000-00-00-00-00-00-E0

Register

Fig.1

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In Fig.1, registration process is proceeding by giving appropriate user name and password, then it will automatically invoke IP address and MAC address. After registration, with the help of user name and password, it can be logged on.

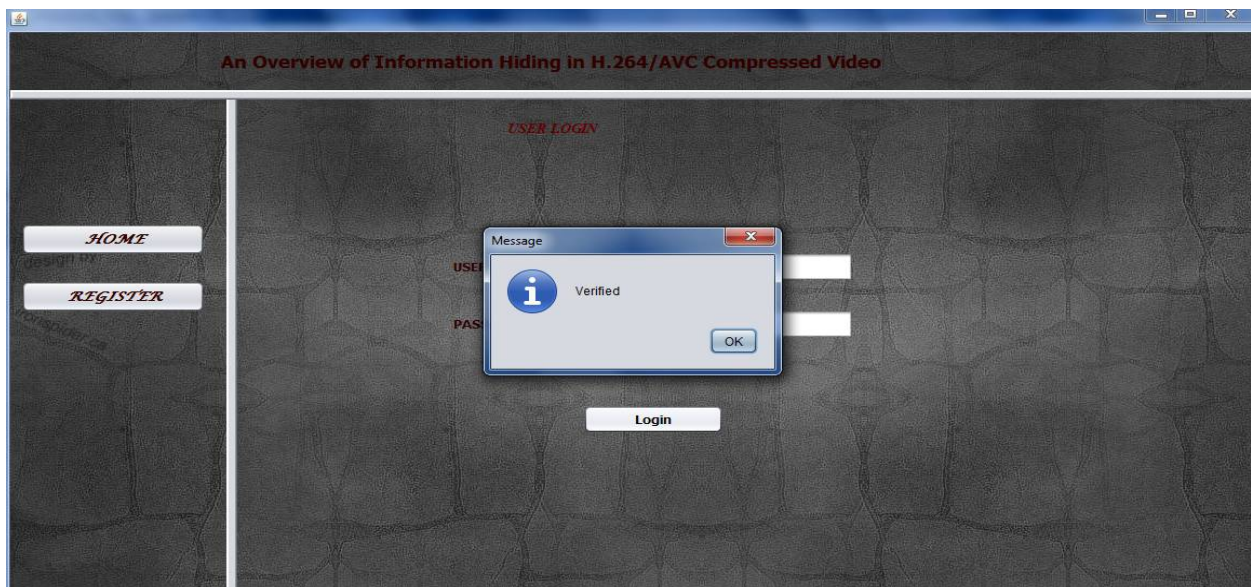


Fig.2

In Fig.2, it will check whether the given user name and password is appropriate or not. This process is done by checking the given user name and password with the database. If it is an appropriate one, it will show verified dialog box or else it will show error.

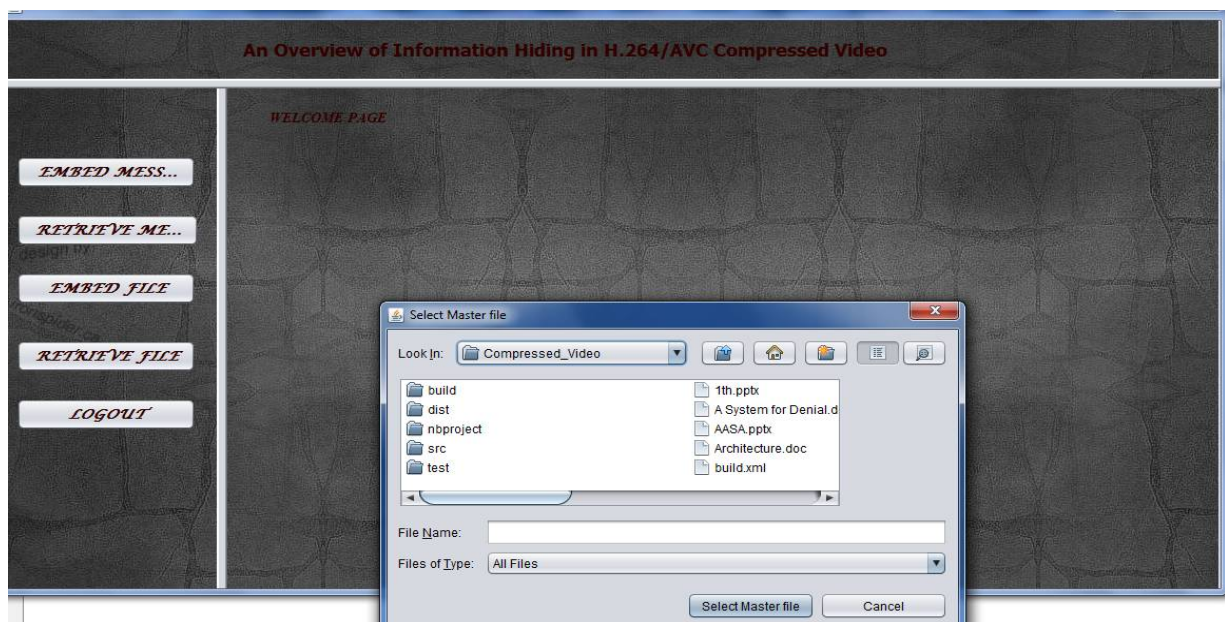


Fig.3

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In Fig.3, the file can be embedded in the video and also it can be retrieved from the video. By selecting the master file(video), the files like document, images, pdf can be embedded in the master file.

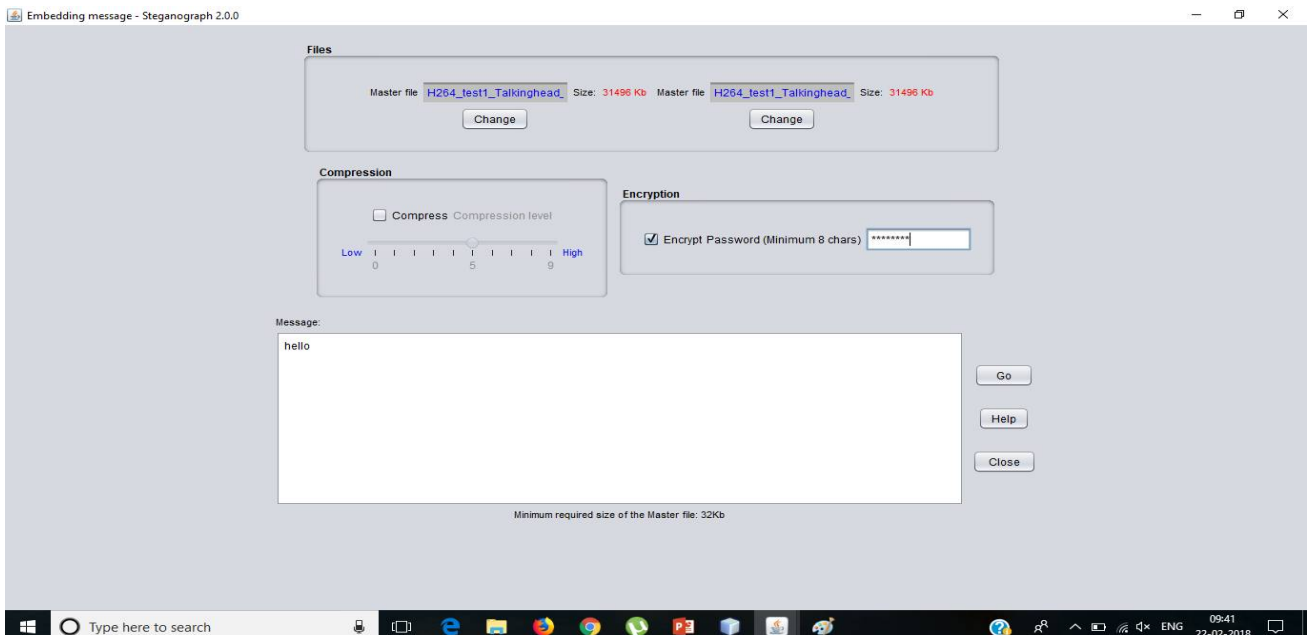


Fig.4

In Fig.4, after selecting the master file the message can be embedded in the video. The master file is compressed based on compression ratio. After that, using encryption key the master file is encrypted.

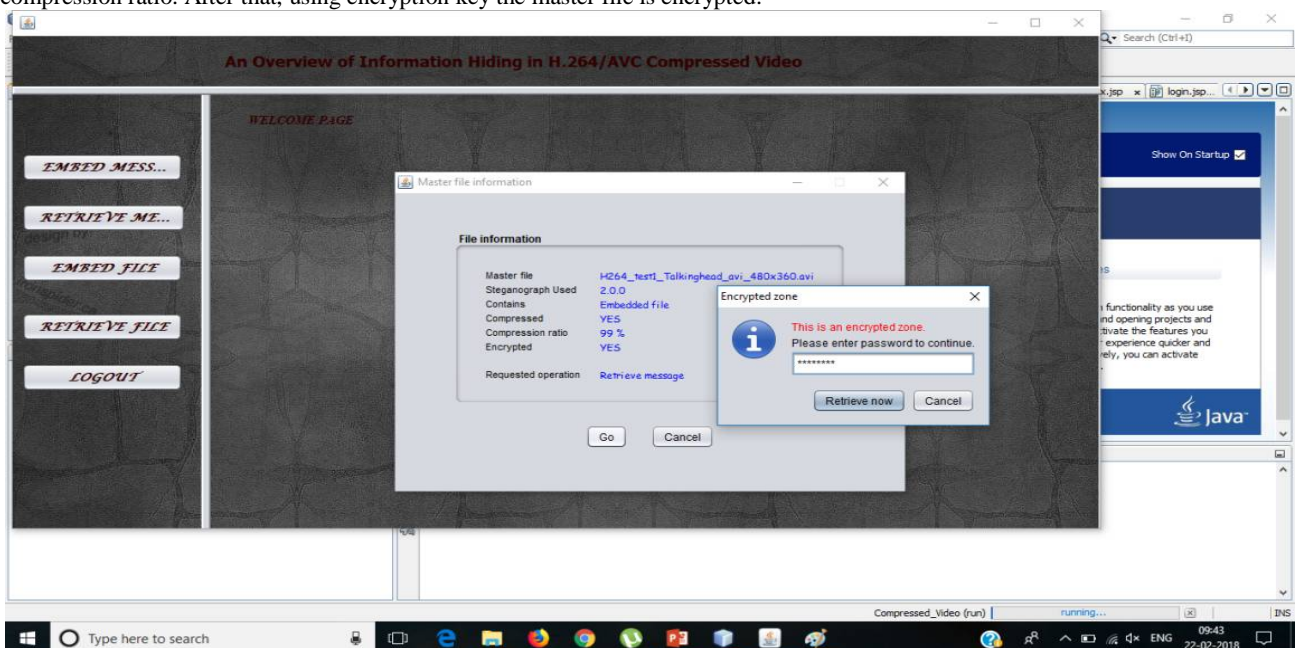


Fig.5

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

In Fig.5, the embedded message can be retrieved by selecting the retrievemessage button. After that, the retrieve file dialog box is opened and encryption key is given for retrieving the embedded message in the master file.

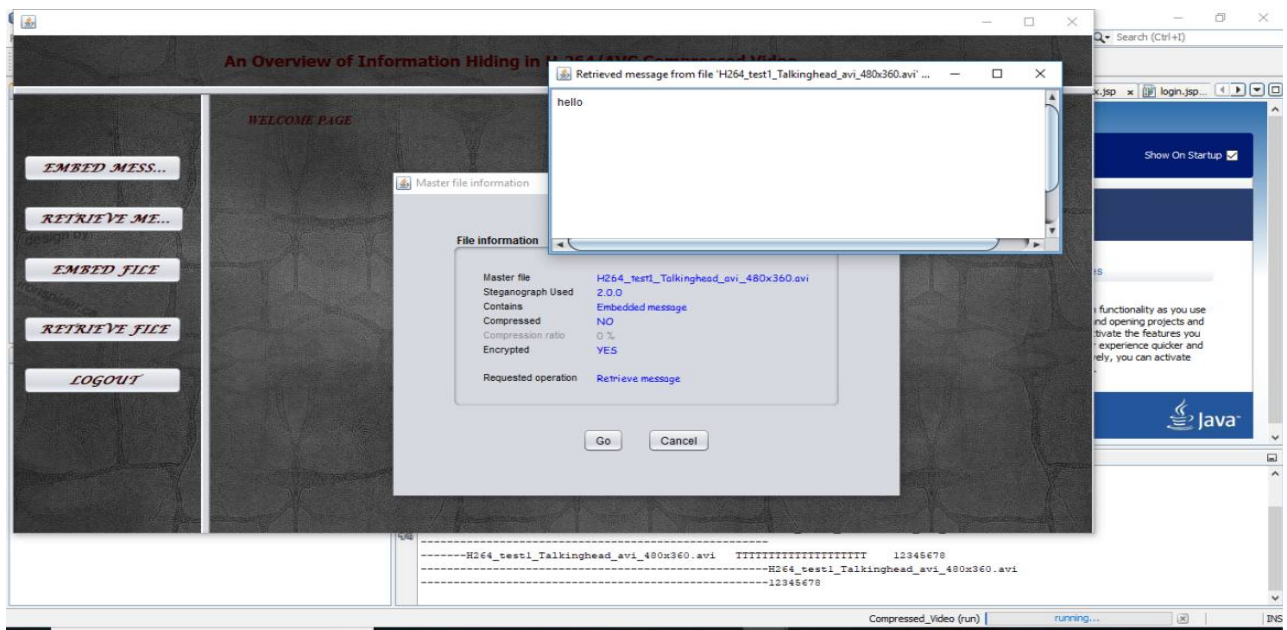


Fig.6

In Fig.6, after the encryption key is given, the encryption key is checked with the database for security purpose. If the encryption key is valid, the embedded message in the master file is retrieved.

V. CONCLUSION

Video robbery is the act of gaining, replicating and after that offering or appropriating a copyrighted video without the assent of the copyright proprietor. Video theft not just damages the film business by causing misfortunes of income however its impact resonates all through the worldwide economy and results in misfortunes of employments and organizations. So to overcome from this existing system a technique is proposed which watermark to preserve the copyrighted video from piracy. A watermarking algorithm provides advantages by ensuring that the watermark embedded in a host video does not significantly affect the visual quality of this video. A watermarking algorithm is imperceptible if the human eye cannot distinguish between an original and watermarked video. If a device detects the presence of a watermark during playback or copying of a video content, it prevents from being copied or played for other than its stipulated use. However, as video streaming has become widespread, it can also be exploited to control online streaming or downloading by placing a watermark decoding filter at the ISP network node.

REFERENCES

- [1] E. Smith and L. A. E. Schuker, "Studios unlock DVD release dates," *The Wall Street Journal*, Feb. 2010.
- [2] J. D. Koch, M. D. Smith, and R. Telang, "Camcording and film piracy in asia-pacific economic cooperation economies," *International Intellectual Property Institute*, Aug. 2011.
- [3] B. Stelter and B. Stone, "Digital pirates winning battle with studios," *The New York Times*, Feb. 2009.
- [4] "Economic consequences of movie piracy – Australia," Jan. 2011.
- [5] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," *IEEE Internet Computing*, vol. 6, no. 3, pp. 18–26, May 2002.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

- [6] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
- [7] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, "Cocktail watermarking for digital image protection," IEEE Transactions on Multimedia, vol. 2, no. 4, pp. 209–224, Dec. 2000.
- [8] "Steganography," [Online]. Available: <http://en.wikipedia.org/wiki/Steganography>, 23 Dec. 2003.
- [9] N. Terzija, Robust digital image watermarking algorithms for copyright protection, Ph.D. thesis, University Duisburg-Esen, Oct. 2006.
- [10] C. I Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," IEEE Signal Processing Magazine, vol. 18, no. 4, pp. 33–46, Jul. 2001.
- [11] H. S. Malvar and D. A. Florˆencio, "Improved spread spectrum: A new modulation technique for robust watermarking," IEEE transactions on signal processing, vol. 51, no. 4, pp. 898–905, 2003.
- [12] K. Wang, G. Lavouˆe, F. Denis, and A. Baskurt, "Three-dimensional meshes watermarking: Review and attack-centric investigation," in International Workshop on Information Hiding, pp. 50–64, Springer, 2007.
- [13] X. Zhang and S. Wang, "Fragile watermarking with error-free restoration capability," IEEE Transactions on Multimedia, vol. 10, pp. 1490–1499, Dec 2008.
- [14] C. D. Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Transactions on Multimedia, vol. 5, pp. 97–105, March 2003.
- [15] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.
- [16] F. Willems, D. Maas, and T. Kalker, "Semantic lossless source coding," in Proc. 42nd Annu. Allerton Conf. Communication, Control and Computing, 2004.
- [17] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 7, pp. 989–999, 2009.
- [18] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," IEEE Transactions on Image Processing, vol. 22, no. 12, pp. 5010–5021, 2013.
- [19] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," IEEE Transactions on image processing, vol. 23, no. 4, pp. 1779–1790, 2014.
- [20] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on circuits and systems for video technology, vol. 16, no. 3, pp. 354–362, 2006.