ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 12, March 2016

AN EFFICIENT MULTIMEDIA CONTENT SECURITY SYSTEM TO EVADE REPLICA

Prakash.M [1]
PG Student,
Dept. of MCA , VSB Engineering College,Karur

Sumithradevi.C [2]
Assistant Professor,
Dept. of MCA , VSB Engineering College,Karur

Abstract : In the presence of overwhelming amount of digital video data, the need for automated procedures to protect owners against unauthorized use of their content. This paper uses strengths of TIRI - DCT algorithm, content based features for finger-print generation of a particular video, and two fast search methods for efficient match of finger-prints within a large database. The contribution of this paper include, extracting compact content-based signatures from TIRI image constructed from the video. To detect query video is pirated video or not, the finger-prints of all the videos in the database are extracted and stored in advance. The search algorithm searches the stored fingerprints to find close enough matches for the finger -prints of the query video. The proposed system can be used for video indexing and copyright applications.

Index Terms: Content based finger-printing, multimedia duplicate detection, multimedia finger-printing, video copy detection, video copy retrieval

1.INTRODUCTION

Advances in processing and recording equipment of multimedia content as well as the availability of free online hosting sites have made it relatively easy to duplicate copyrighted materials such as videos, images, and music clips. Illegally redistributing multimedia content over the Internet can result in significant loss of revenues for content creators. Finding illegally-made copies over the Internet is a complex and computationally expensive operation, because of the sheer volume of the available multimedia content over the Internet and the complexity of comparing content to identify copies. Video copy detection is the process of detecting illegally copied videos by analyzing them and comparing them to original content. The goal of this process is to protect a video creator's intellectual property.

Fingerprinting is an important tool for automated multimedia identification. It involves computing a short and compact identifier that captures robust and distinct properties called a “fingerprint”, which can be used for identifying the multimedia. Fingerprinting has found applications in content filtering on user-generated content (UGC) websites, automatic multimedia tagging, and other applications in multimedia management. Fingerprinting schemes that utilize various features of multimedia in different domains have been proposed, a review of which may be found. A fingerprint, or small amount of data, is derived from the media and stored in a database. An unknown work is fingerprinted and matched to the database. Video fingerprinting is a technique in which software extracts characteristic components of a video file. The characteristics can be both visual as well as audio. The fingerprints are highly compressed files and can be stored in databases for comparison. In contrast to watermarks, fingerprints are not embedded into the audio-visual material. Fingerprinting does not require any modification of the original content. It is often used in broadcasting to track the airing of television programmes and commercials. In contrast to perceptible watermarks, fingerprinting does not visually prevent unlawful use of content. Video segment identification has many applications such as video content monitoring, copyright enforcement, and video structure analysis and so on. For video segment identification in large database of video sequences, query clip is usually firstly represented as a feature vector or a set of feature vectors, which is expected to be a unique signature in high dimensional space. Then they obtained signature will be sequentially compared with those of a series of sliding matching windows in the target video stream, or used to do fast searching based on the previously built index structure. Christo Ananth et al. [1] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. First of all, the performance of keyframe based shot representation strongly depends on the accuracy of shot segmentation algorithm and the appropriate selection of key frame to characterize the video content.

2. EXISTING APPROACHES

The existing approaches for video copy detection. They are,

♣ Watermarking Approach

♣ Image based approach to video copy detection

2.1 Watermarking Approach

Water marking relies on inserting information into the video stream in order to detect copies. Copy detection for digital media is critical to preventing copyright violations and enforcing copy right. Watermarking [3] is the most widely accepted form of copy detection. This approach utilizes 3-D DCT algorithm.The drawback of 3-D DCT algorithm is its binarization phase. To obtain common threshold for the binarization phase is far from optimal, because different frames are having different frequencies. However, there are two significant limitations in water marking approach. They are, Legacy Content and Attacks .

Legacy Content: Since watermarks must be introduced into the original content before copies are made, it cannot be applied to content which is already in circulation. For example, watermarking approach would not provide a solution to find all clips of star wars posted on the web.

Attacks: The watermark on a particular piece of content is compromised; there is no alternative approach to copyright enforcement.

2.2 Image Based Approach to Video Copy Detection

This approach introduces a video copy detection system which efficiently matches individual frames and then verifies their spatio - temporal consistency [7]. The approach for matching frames relies on a local feature indexing method, which is at the same time robust to significant video transformations and efficient in terms of memory usage and computation time. It matches either key frames or uniformly sampled frames.

2.2.1 Key Frames : Key frames are characteristic frames of the video. Key frames are used to obtain similar frames for two matching videos. To extract key frames, first detect shot boundaries by measuring gray level changes on a spatio - temporal slice of the video, and thresholding them [3]. The video hashing technique [15] is applied to every frame of a video sequence.

2.2.2 Limitations

The image based approach to video copy detection system efficiently matches individual frames and then verifies their spatio-temporal consistency. The approach for matching frames relies on a recent local feature indexing method, which is at the same time robust to significant video transformations and efficient in terms of memory usage and computation time. This image based approach matches either key frames or uniformly sampled frames. To further improve the results, a verification step has been taken to robustly estimates a spatio-temporal model between the query video and the potentially corresponding video segments. The video matching is based on individual key frames, so the searching time is very low. The image based approach is not tolerable to all the attacks on video signals such as, changes in brightness/contrast, rotation, frame loss, noise addition and spatial/temporal shift.

3. PROPOSED CONTENT BASED VIDEO COPY DETECTION SYSTEM (CBCD)

CBCD is a complimentary approach to watermarking technique. Because watermarks must be introduced into the original content before copies are made , it cannot be applied to content which is already in circulation. CBCD provides solution to the problem of legacy content and attacks [10]. Suppose the watermark on a particular piece of content is compromised there is no alternative approach to copy - right enforcement. The primary thesis of content based video copy detection system is to detect the copies of video clips to find whether it is a pirated copy or not. The proposed video copy detection system based on content based finger-printing can be used for video indexing and copyright applications. The system depends on a finger-print extraction algorithm followed by a fast approximate search algorithm. The finger-print extraction algorithm extracts compact content-based signatures from special images constructed from the video. Each such image represents a short segment of the video and contains temporal as well as spatial information about the video segment. These images are denoted as temporally informative representative images (TIRI). TIRI is a blurred image that contains all possible motions in a particular video sequence. Each TIRI image represents a short segment of the video and contains spatial and temporal information about the video segment. The TIRI image plays a vital role in generation of finger-print for any input video because of its compactness [13]. The TIRI image is generated by extracting the features from all the short segments of a particular video.

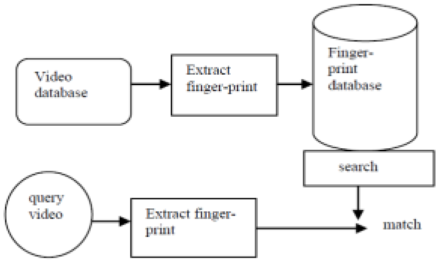

Figure 1: Schematic representation of video copy detection system

The fig 1 shows, all the finger-prints are stored in advance, If a query video is given, extract finger-print for that particular query video then searches all the finger-prints in a finger-print database .If a match is found the query video is a pirated video, otherwise it is not a copied video.

MODULE DESCRIPTIOIN

A content protection system has three main parties: (i) content owners (ii) hosting sites and (iii) service providers. The first party is interested in protecting the copyright of some of its multimedia objects, by finding whether these objects or parts of them are posted on hosting sites. The third party is the entity that offers the copy finding service to content owners by checking hosting sites.

Distributed Index Module: Maintains signatures of objects that need to be protected; Keyframes are extracted from the reference video database and features are extracted from these keyframes. The extracted features should be robust and effective to transformations by which the video may undergo. Also, the features can be stored in an indexing structure to make similarity comparison efficient.

Reference Registration Module: Creates signatures from objects that content owners are interested in protecting, and inserts them in the distributed index;

Query Preparation Module: Creates signatures from objects downloaded from online sites, which are called query signatures.It then uploads these signatures to a common storage; Query videos are analyzed. Features are extracted from these videos and compared to those stored in the reference database. The matching results are then analyzed and the detection results are returned.

Object Matching Module: Compares query signatures versus reference signatures in the distributed index to find potential copies. It also sends notifications to content owners if copies are found;

Video Copy Detection Based on the Content: In this case, the signature which defines the video is the content. The function of the algorithms of video copy detection based on the content extract the fingerprint through the features of the visual content. Then the fingerprint is used to compare with fingerprints from videos in a database. This type of algorithms has a difficult problem. It's really hard to solve if a video is a copied video or a similar vide. The features of the content are very similar from one video to the other, and the system can think that the image is copied, but really it isn't.

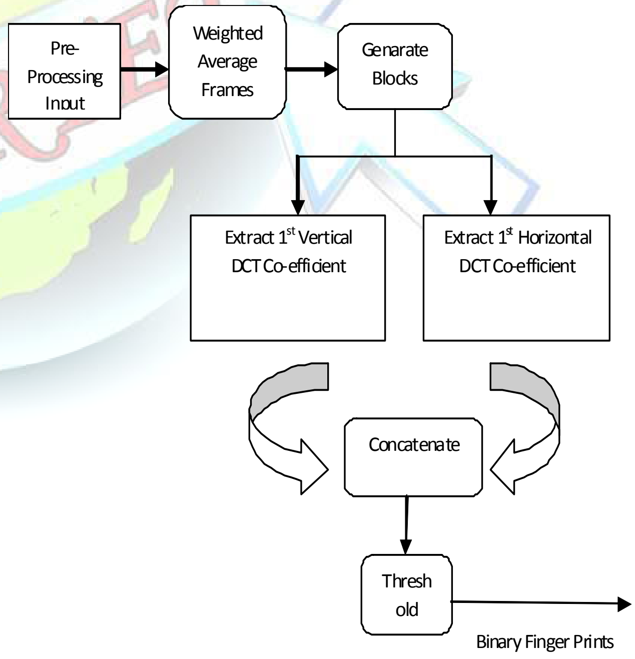

Figure 2: Schematic representation of proposed TIRI-DCT algorithm

4. STEPS INVOLVED IN PROPOSED TIRI-DCT ALGORITHM

1. In this step, first select the video from the video database, and then split the particular video into frames. After splitting the video into frames, convert the frames into Luminance and Chrominance Valued (LUV) frames.

2. After pre-processing, the video frames are divided into overlapping segments of fixed-length, each containing j frames. Then the finger-printing algorithm is applied to these segments. The amount of overlapping is experimentally chosen to be 50%. Overlapping reduces the sensitivity of the finger-prints to the “synchronization problem” which is referred as “time shift”.

3. For TIRI image generation, spaio-temporal finger-printing method [2] is adopted. This method calculates a weighted average of the frames to generate a Temporally Informative Representative Image (TIRI). The TIRI image is a special image that plays best to capture the temporal information in a video. The resulting TIRI image is basically a blurred image that contains information about all possible existing motions in a video sequence. By using proposed TIRI-DCT algorithm, features are derived by applying a 2D-DCT on overlapping blocks of size from each TIRI with 50% overlap. The first horizontal and the first vertical DCT coefficients (features) are then extracted from each block.The figure2 shows pre-processing step is applied to weighted average of the frames. Then generate TIRI-blocks and the first horizontal and vertical DCT co-efficient are extracted from each block. The values of the features from all the blocks are concatenated to form the feature vector. Each feature is then compared to a threshold and binary fingerprint is generated.

4. The features are derived from the TIRI image, and the finger-print is generated by using TIRI-DCT algorithm .The resulting finger-print is just a string of bits that represents the signatures of the video data. In order to determine whether a query video is an attacked version of a video in a database or not, its fingerprint is first extracted. The fingerprint data base is then searched for the closest fingerprint to the extracted query fingerprint. It should be mentioned that in copy detection, the problem is to determine if a specific query video is a pirated version of a video in the database. If the finger-print match is found, the query video is a pirated or copied video, otherwise it is not a copied video.

4.1 Advantages of Proposed System:

- Accuracy.
- Computational Efficiency.
- Scalability and Reliability.
- Cost Efficiency.
- The system can run on private clouds, public clouds, or any combination of public-private clouds.
- Our design achieves rapid deployment of content protection systems, because it is based on cloud infrastructures that can quickly provide computing hardware and software resources.
- The design is cost effective because it uses the computing resources on demand.
- The design can be scaled up and down to support varying amounts of multimedia content being protected.

After the generation of finger-prints for a particular query video,to examine whether a query video is an attacked version of video in a database or not,The fast matching of finger-prints within a large database by using two fast search methods have been done.

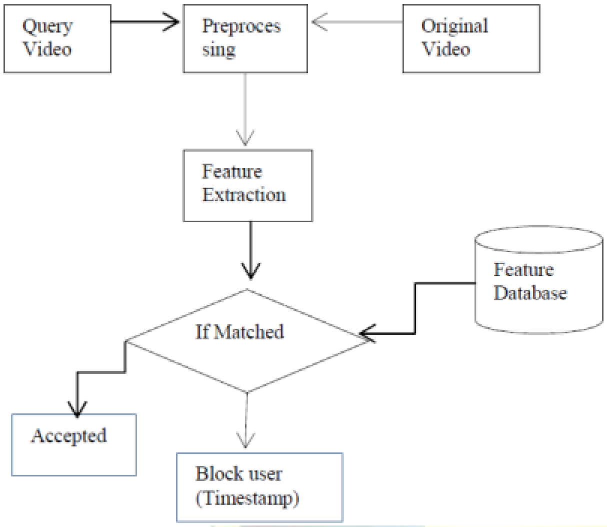

Figure 3: Flow chart for finger-print extraction of video

5. CONCLUSION AND FUTURE WORK

The fingerprinting system is proposed for Video copy detection system.It can be used for copyright management and indexing applications.The system consists of a fingerprint extraction algorithm followed by an approximate search method. The proposed fingerprinting algorithm which is Interest point Matching Algorithm extracts robust, discriminate and compact fingerprints from videos in a fast and reliable fashion. The fingerprint extracted using this algorithm maintains a good performance for attacks such as noise addition, changes in rightness or contrast rotation, time shift, and changes in background. Two fast searching methods: Inverted file based searching and cluster based similarity search are implemented for efficient searching in the fingerprint database. Future work includes enhancing the security to the fingerprint. It also includes the study of the performance of the system in the presence of some other attacks, such as large geometric attacks like cropping or inserting some logo. Comparing to the other fingerprinting methods our system will reduce the searching time so it improves to faster searching methods.

REFERENCES

[1] Christo Ananth, M.Danya Priyadharshini, “A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks”, International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[2] O. Ku¨cu¨ ktunc, M. Bastan, U. Gu¨du¨ kbay, and O ¨. Ulusoy, “Video Copy Detection Using Multiple Visual Cues and MPEG-7 Descriptors”, 2010.

[3] J. Law-To, C. Li, and A. Joly, “Video Copy Detection: A Comparative Study,” Proc. ACM Int’l Conf. Image and Video Retrieval, pp. 371-378, July 2007.

[4] X. Zhou, L. Chen, A. Bouguettaya, Y. Shu, X. Zhou, and J.A. Taylor, “Adaptive Subspace Symbolization for Content-Based Video Detection,” IEEE Trans. Knowledge and Data Eng., vol. 22, no. 10, pp. 1372-1387, Oct. 2010.

[5] A. Joly, O. Buisson, and C. Frelicot, “Content-Based Copy Retrieval Using Distortion-Based Probabilistic Similarity Search,” IEEE Trans. Multimedia, vol. 9, no. 2, pp. 293-306, Feb. 2007.

[6] H. Liu, H. Lu, and X. Xue, “SVD-SIFT for Web Near-Duplicate Image Detection,” Proc. IEEE Int’l Conf. Image Processing (ICIP ’10), pp. 1445-1448, 2010.

[7] TRECVID 2008 Final List of Transformations, http://www-nlpir.nist.gov/projects/tv2008/active/ copy. detection/final.cbcd. video.transformations.pdf, 2008.

[8] N. Guil, J.M. Gonza´lez-Linares, J.R. Co´zar, and E.L. Zapata, "A Clustering Technique for Video Copy Detection," Proc. Third Iberian Conf. Pattern Recognition and Image Analysis, Part I, pp. 452-458, June 2007.

[9] K. Sze, K. Lam, and G. Qiu, "A New Key Frame Representation for Video Segment Retrieval," IEEE Trans. Circuits and Systems Video Technology, vol. 15, no. 9, pp. 1148-1155, Sept. 2005.

[10] J. Yuan, L.-Y. Duan, Q. Tian, S. Ranganath, and C. Xu, "Fast and Robust Short Video Clip Search for Copy Detection," Proc. Pacific Rim Conf. Multimedia (PCM), 2004.

[11] S. Cheung and A. Zakhor, "Efficient video similarity measurement with video signature," In *IEEE Trans. on Circuits and System for Video Technology*, vol. 13, pp. 59-74, 2003.

[12] M.R. Naphade et al., "A Novel Scheme for Fast and Efficient Video Sequence Matching Using Compact Signatures," In *Proc. SPIE, Storage and Retrieval for Media Databases 2000*, Vol. 3972, pp. 564-572, 2000.

[13] A. Hampapur, K. Hyun, and R. Bolle., "Comparison of Sequence Matching Techniques for Video Copy Detection," In *SPIE. Storage and Retrieval for Media Databases 2002*, vol. 4676, pp. 194-201, San Jose, CA, USA, Jan. 2002.

[14] Junsong Yuan et al., "Fast and Robust Search Method for Short Video Clips from Large Video Collection," in *Proc. of ICPR'04*, Cambridge, UK, Aug. 2004.

[15] R. Lienhart et al., "VisualGREP: A Systematic method to compare and retrieve video sequences," In*SPIE. Storage and Retrieval fro Image and Video Database VI*, Vo. 3312, 1998.

[16] J. Oostveen et al., "Feature extraction and a database strategy for video fingerprinting," In *Visual 2002, LNCS 2314*, pp. 117-128, 2002.