Two Phase Approach for Copyright Protection and Deduplication of Video Content in Cloud using H.264 and SHA-512

Dr.B.Basaveswara Rao [1], Qutaiba Mumtaz Dawood[2] ,Dr. K. Gangadhara Rao [3],
[1]*Computer Centre,* [2,3]*Department of Computer Science and Engineering*
Acharya Nagarjuna University, Guntur 522501, Andhra Pradesh, INDIA.

Abstract: *Cloud computing offers a new way of service provision by rearranging various resources over the Internet. The most important and popular cloud service is data storage. In order to preserve the privacy of data holders, data are often stored in cloud in an encrypted form. However, encrypted data introduce new challenges for cloud data deduplication, which becomes crucial for big data storage and processing in the cloud. Traditional deduplication schemes cannot work on encrypted data. Among these data, digital videos are fairly huge in terms of storage cost and size; and techniques that can help the legal aspects of video owner such as copyright protection and reducing the cloud storage cost and size are always desired. This paper focuses on video copyright protection and deduplication. A video copyright and deduplication scheme in cloud storage environments using the H.264 compression algorithm and SHA-512 hashing technique is proposed. This paper proposes a combined copyright production and deduplication based on video content to authenticate and to verify the integrity of the compressed H.264 video. The design of the proposed scheme consists of two modules. First, a H.264 compression algorithm is applied on the given video by the user. Second, a unique signature in different time interval of the compressed video is generated by the user in such a way that the CSP can use it to compare the user's video against other videos without compromising the security of the user's video. To avoid any attacker to gain access to the hash signature during uploading to the cloud, the hash signature is encrypted with the user password. Some experimental results are provided, showing the effectiveness of our proposed copyright protection and deduplication system.*

Keyword – *Video copyright, Video deduplication, H.264 compression.*

1. Introduction: Cloud computing offers a new way of Information Technology services by rearranging various resources such as storage, computing and providing them to users based on their demands. Cloud computing provides a big resource pool by linking network resources together. It has desirable properties, such as scalability, elasticity, fault-tolerance, and pay-per-use. With the advent of social websites such as Facebook, YouTube, to name a few, video data are among the most widely types of shared data in the clouds [5]. The H.264 video format has a very broad application range that covers all forms of digital compressed video from low bit-rate Internet streaming applications to HDTV broadcast and Digital Cinema applications with nearly lossless coding. With the use of H.264, bit rate savings of 50% or more compared to MPEG-2 Part 2 are reported. Digital videos are fairly huge in terms of storage cost and size; and techniques that can help reduce the cloud storage cost and size are always desired. New technologies also pose new questions regarding the legal aspects of copyright protection, which are often resolved through litigation between owners and content distributors. Copyright production of the publishing Video is big challenge is that how to insure and keep a single copy of the video in the cloud. More specifically, in the cloud, there are N number of movies, songs, personal record videos, all those uploaded by N number of users and in all these cases CSP cannot keep only single copies of the video or may publish illegally video by third party. As we know some users can easily download any video and upload again in their web or on the YouTube channel, so in this way the legal video_ owner's loose copyright of the video, chance of counting views, or the producers of movies, songs lose their money if the movie become illegally available in the cloud. To keep copyright for each video that can only video_ owner have rights to upload it, or by block his/her video from uploading by other users into cloud environment a Novel

Approach for copyright production and Deduplication Video in Cloud Using H.264 Compression And SHA-512 Hashing Techniques are proposed. In this paper, a scheme is proposed that achieves a copyright and video deduplication in cloud storage environments .To keep only single copy for uploaded video by the legal video_ owner in the cloud, copyright protection and deduplication techniques are used. For copyright production video two types of video_owners are there, 1) A video_owner who wish to upload the video and keep it uniquely in the cloud environment, the user generates set of hash signatures, encrypt these hash with a secret key, then compress the video and upload it to the cloud 2) An video_owner who wish to block a video for upload to the cloud environment, the user generates only the set of signatures and encrypt it with secret key then upload it to the cloud. The CSP uses this these set of signatures to remove the duplicate copy or block video from uploading by other users, CSP before store or publish any video in the cloud, a request has been sent to the user to upload the metadata for the specific video and this metadata have numbers of hashing from the video in different time interval that allow the CSP to check with the saved metadata table if its duplicate the CSP rejects uploading, otherwise the user can upload the video. In more details, the user compresses the original video using the H.264 compression algorithm, next calculates the signatures based on the GOP from the output bit stream and makes the number of hash signatures using SHA-512. After these processing steps on the original video, the set of hashing signatures will encrypt with the secret key and then uploaded in the cloud storage. This hash signature is encrypted using AES encryption [19] and sent as supplemental information in the video bit stream. The CSP will decrypts these set of hashing signatures and check for the identical GOPs with the help of the hashing table, if identical GOPs are detected, the CSP will run POW[12] to proof video owner of this video for type one user. For the second type user the CSP will reject the uploading in case of duplicate set of signatures are available for these particular data already in the cloud storage. In this way, the CSP will protect the copyright of the legal owner and save huge space by performing cross-user video deduplication in the cloud storage. Extending the previous works [1], this paper focuses on video copyright protection and deduplication. A video copyright and deduplication scheme in cloud storage environments using the H.264 compression algorithm is proposed. The design of the proposed scheme consists of two modules. First, a H.264 compression algorithm is applied on the given video by the user. Second, a unique signature in different time interval of the compressed video is generated by the user in such a way that the CSP can use it to compare the user's video against other videos without compromising the security of the user's video. Third the video_owner will encrypt the set of hash signatures with a secret key. The CSP will not be able to modify the video content itself, but will be able to make the process of deduplication of the videos using the signatures generated by the users.

1.1. Objective

In this paper, an attempt has been made to implement A Novel Approach for Copyright protection and Deduplication Video in Cloud Using H.264 Compression and SHA-512 Hashing Techniques. The video of the user is protected through the numbers of hashes, which is also compatible with the cloud systems. In a more detailed way, the user extracts and generate the hash value of the video during the compression process and then sends set of signatures with the video to the cloud; the cloud compares received a set of hash with hash table, if its match, the CSP rejects uploading. If no duplicate is found, proof from the cloud will be returned, the user upload compressed video and sent it to Cloud after the CSP will insert received hash to the hash table. In case video_owner gives authority to multiple users to publish his/her video in the cloud, the CSP will run a deduplication procedure to keep only single copy and give the link to all other users, to save storage space. To ensure legality of senders CSP will run POW. The main objective of this paper is to protect copyright and save storage space.

1.2 Organization

The organization of the paper is as follows. Section 2 presents literature review. Section 3, discusses the preliminaries of copyright protection and Deduplication. In Section 4 presents the proposed System. The Methodology is discussed in Section 5. The Implementation and Results are presented in section 6. Section 7 discusses about Conclusion and Future scope of the work.

2. LITERATURE REVIEW

The videos are often compressed enough before being stored in the cloud. A MPEG and H.264 compression algorithms are the most popular methods used for video compression. The MPEG algorithm [2] is an object-based algorithm that makes use of local processing power to recreate sounds and images**.** On the other hand, the H.264 algorithm [3] is a block-based motion compensation codec most widely used for high definition (HD) videos. Its working is based on frames, which are further

divided into macro blocks (MB). According to [3], the H.264 algorithm yields a better motion compensation minimum clock size support and a better bit rate, compression efficiency, compared to the MPEG algorithm. For these reasons, we have adopted the H.264 compression algorithm in the proposed scheme in order to facilitate the copyright production and deduplication of the video. There exists some relevant work in the area of H.264 video authentication as typified by references [6]-[11]. Mainly two methods have been used: digital watermarking [6][7][8][9] and external digital signature [10][11]. Digital watermark techniques embed an invisible signal (for example, company logo or personal symbol) into video so as to attest the owner identification of the media and discourage the unauthorized copying. While watermark techniques emphasize protecting the right of service providers, digital signature focuses on that of the customers. For example, a video purchaser may want to know whether the product he or she bought is from the legal seller and is the authentic one. The Digital signature scheme can be used to solve this problem. First the video seller extracts some information dependent on the content of the original video and encrypts it into a small-size file, which is called a signature. Then the signature file is sent to the purchaser with the original video [10]. An obvious drawback of these schemes is any attacker can get the signatures during transfer from video_owner to the cloud. In the proposed scheme, the user encrypts the set of hash signatures with secret key such as user login password. In order to perform the copyright production and deduplication on the videos, the CSP needs to compare the received set of signatures against the ones already in the cloud storage. Different signature generation schemes for different scenarios have been proposed in the literature. In [17], two robust hash algorithms based on discrete cosine transform (DCT) are proposed, one based on the classical basis set and the other on the randomized basis set. The DCT hashes are robust, but are less secure as videos with similar hashes can easily be found. Moreover, this approach does not use video compression, thus the approach may not be efficient in terms of storage savings when large videos are used. In [17], a robust hash based on 3D Set Partitioning In Hierarchical Trees (SPIHT) compression algorithm is proposed. The 3D discrete wavelet transforms are used to generate the hash of the compressed video, which is unique and robust. But, it is shown that the SPIHT algorithm is not as efficient and practical compared to the H.264 compression algorithm. Lefebvre et al [18] extended their image hashing technique based on the Radon transform to video hashing. Their idea is to select some key frames in the video and to apply their image hashing technique to the key frames hoping that the key frames would tolerate acceptable modifications. The drawback of this (and any key frame based) approach is that an attacker can modify the video in such a way that key frames are not affected but the other frames are affected. In this paper, an effective technique for content-based H.264 video authentication is described. It is based on digital signature generated from the robust features picked out from transform domain of each GOPs. The core idea is that the video_owner is calculating the set of signatures locally from the information produced by the compression algorithm and then encrypt it with user password for security purpose. The proposed scheme collects information from DC and lowest AC coefficients of the DCT to generate the hash. The idea is that the low frequency components remain almost same for minor modifications and at the same time remain sensitive to malicious modifications as they contain predominant energy. In case to block video from upload by another user, the video_owner upload only sets of signatures to CSP with a request to block any other user from uploading same video. In case video_owner looks to upload has/her video for the purpose of publishing the same in the cloud with avoiding other users from uploading same copy, the video_owner need to upload both, a set of signatures and compressed video and then the CSP will store these sets of signatures and used it for matching purpose. In some case, video_owner gives authority to multiple users to publish his/her video in the cloud, the CSP will run deduplication procedure to keep only single copies in term to save storage space. To ensure the legality of senders, CSP will run POW. The POW [12] lets the user efficiently prove to the CSP that the user holds a file, rather than just some short information about it. This allows controlling attacks on file-deduplication systems where the attacker obtains a short summary of the file and uses it to fool the CSP into thinking that the attacker owns the entire file.

3. Preliminaries:

This part of the paper first defines the notations used in this paper, followed by a brief review of some of the tools utilized as a part of the proposed scheme. The notations used are given in Table 1.

Table 1.Notations Used in This Paper

Acronym	Description
CSP	Cloud Server Provider
SHA	Secure Hash Algorithm
GOP	Group Of Pictures
HD	High Definition
MB_S	Macro Blocks
DCT	Discrete Cosine Transform
SPIHT	Set Partitioning In Hierarchical Trees
DS	Digital Signature
AES	Advanced Encryption Standard

3.1 Secure Hash Algorithm SHA-512

Is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). Cryptographic hash functions are mathematical operations run on digital data, by comparing the computed hash to a known and expected hash value, a person can determine the data's integrity. The message to be hashed is first:

1. Padded with its length in such a way that the result is a multiple of 1024 bits long, and then
2. Parsed into 1024-bit message blocks $M^{(1)}$; $M^{(2)}$;……;$M^{(N)}$.

The message blocks are processed one at a time: Beginning with a fixed initial hash value $H^{(0)}$, sequentially compute

$$H^{(i)} = H^{(i-1)} + C_M^{(i)} (H^{(i-1)}),$$

Where C is the SHA-512 compression function and + means word-wise mod 2^{64} addition. $H^{(N)}$ is the hash of M.

3.2 Group of Pictures GOP

The GOP is a collection of successive pictures within a coded video stream. Each coded video stream consists of successive GOPs, from which the visible frames are generated. Encountering a new GOP in a compressed video stream means that the decoder doesn't need any previous frames in order to decode the next ones, and allows fast seeking through the video.

A GOP can contain the following picture types:

i) Intra coded picture or I frame – a picture that is coded independently of all other pictures. Each GOP begins (in decoding order) with this type of picture.

ii) Predictive coded picture or P frame – contains motion-compensated difference information relative to previously decoded pictures. Each P picture can only reference one picture, and that picture must precede the P picture in display order as well as in decoding order and must be an I or P picture.

iii) Bipredictive coded picture or B frame – contains motion-compensated difference information relative to previously decoded pictures. Each B picture can only reference two pictures, the one which precedes the B picture in display order and the one which follows, and all referenced pictures must be I or P pictures.

3.3 H.264

H.264 was developed over a period of about 4 years. The roots of this standard lie in the ITU-T's H.26L project initiated by the Video Coding Experts Group (VCEG) with initial focus on video conferencing and telephony applications. At a high level, the basic coding structure of this standard is similar to that of MPEG-2, H.263 or MPEG-4 part 2. Each picture is compressed by partitioning it as one or more than one slice. Each slice consists of Macroblocks, which are 16 pixels wide and 16 pixels high (16x16). Each Macroblock is further divided into sub-Macroblock partitions – 16x8, 8x16, 8x8, 8x4, 4x8 and 4x4. The 4x4 sub-macroblock partition is also called a block. The hierarchy of a video sequence from a sequence to pixels is given by:

Sequence (pictures (slices (macroblocks (sub-macroblocks (blocks (pixels)))))).

3.4 POW

Proof-of-ownership [12] is a protocol in two parts between two players on a joint input F (which is the input file). First the verifier summarizes to itself the input file F and generates a (shorter) verification information v. Later, the prover and verifier engage in an interactive protocol in which the prover has F and the verifier only has v, at the end of which the verifier either accepts or rejects. In another word, POW enables user to prove their ownership of data copies to the server. The storage server derives a short value ϕ (M) from a data copy M .To prove the ownership of the data copy user needs to send ϕ' to storage server such that $\phi'=\phi$ (M).

4. THE PROPOSED SYSTEM

The method presented is designed to work in compressed domain; where cryptographic hash function has been used to ensure copyright production and deduplication videos by hashing the inherent features of the compressed H.264 video to produce a compact size signature .These sets are stored and used after to verify the copyright and delete extra copies. In this proposed method, the input video is segmented into GOPs and from each one generates a unique signature. For each GOPs, features from each I frame are extracted and hashed by a cryptographic hashing function SHA-512 to generate a unique hash signature for each GOP. In other words, the user wants upload video to the cloud, first should generate set of hash signatures that can be used as the verification of the copyright and upload it to the cloud by using SHA-512 , in case of the set of hash signatures are already existing in the cloud ,the CSP reject uploading the video otherwise accepted. If the user wishes to give authority to N number of other users to publish has/her video, then the CSP run POW [12] to verify whether this user is permitted to upload and publish this video and then applying deduplication procedure.

4.1 DCT

The Discrete Cosine Transform (DCT) [16] operates on X, a block of N × N samples (typically image samples or residual values after prediction) and creates Y, an N × N block of coefficients. The action of the DCT (and its inverse, the IDCT) can be described in terms of a transform matrix A. The forward DCT (FDCT) of an N × N sample block is given by:

$$Y = AXA^T \quad (1)$$

and the inverse DCT (IDCT) by:

$$X = A^TYA \quad (2)$$

Where X is a matrix of samples, Y is a matrix of coefficients and A is an N × N transform matrix. The elements of A are:

$$A_{ij} = C_i \cos \frac{(2j+1)i\pi}{2N} \quad \text{where} \quad C_i = \sqrt{\frac{1}{N}} \ (i = 0) \ ,$$

$$C_i = \sqrt{\frac{2}{N}} \ (i > 0)$$

Equation 1 and equation 2 may be written in summation form:

$$Yxy = Cx\,Cy \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} Xij \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)y\pi}{2N}$$

$$Xij = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Cx\,Cy\,Yxy \cos \frac{(2j+1)y\pi}{2N} \cos \frac{(2i+1)y\pi}{2N}$$

4.2 Signature generation process

The signature generation is based on the method proposed in [10] and [11] where content-dependent robust bits are extracted from MB and used to check copyright video which is compressed by H.264. The H.264 standard supports codes sequences containing I and P slices. I slices contain intra coded MBs in which each 16x16 (INTRA 16x16) or 4x4 (INTRA 4x4) luma regions is predicted from previously coded samples in the same slice. The INTRA 4x4 mode is based on predicting each Luma block separately and is well suited for coding parts of a picture with significant detail. The Features used for digital signature generation are the set of coefficients extracted from INTRA and INTER prediction MBs including INTRA 16x16, INTRA 4x4 and INTER 4x4 prediction MBs. For INTRA 4x4 and INTER 4x4 MBs, the quantized DC coefficient and the first two quantized AC coefficients belonging to low frequency coefficients in zig-zag scan order and surrounding the DC value of every 4x4 block are taken as the feature data for the MB. These features data are collected in a buffer for every coded MB within every frame until the end of the GOP is reached. In H.264, the end of the GOP is indicated by an instantaneous decoder refresh (IDR). At each end of the GOP, the values present in the buffer are hashed using SHA-512 to produce a 512 bit message digests. After the scrambling digests are used as set of signature which can use later as copyright verification. The signature generation is carried out in the compressed domain, and the signatures are generated from the information produced in the transform domain of the H.264 compression algorithm. The content dependent robust bits are extracted from the macro-blocks and are further used as the signature for authenticating the compressed video. Indeed, the video is first broken down into GOPs, which are authenticated individually by hashing the features extracted from their 'I' frames.

The hash is then considered as the digest digital signature for all the frames in the GOP. The proposed digital signature generation scheme shown in Figure 1.

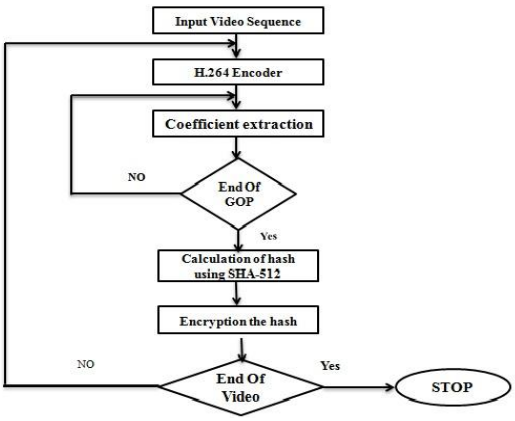

Figure 1. Proposed digital signature generation scheme

4.3 Signature verification

A hash signature is a mathematical scheme for proving the authenticity of digital messages or documents. A valid hash signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). There are two scenarios in verification process named Type I and Type II, in type I the video_owner generates set of hash signatures locally then encrypt it and uploaded to the cloud. The CSP compare sets of signatures with already exist sets in cloud storage, if its match, then CSP rejects uploading the video, otherwise video_owner will upload it to the cloud. Type II, the video_owner wish to block the video from uploading by unauthorized user without uploading his\her video to the cloud storage .The video_owner generate set of signatures and upload it to cloud storage with a request to block this video, in this case the CSP update the database with received set of signatures . The videos are hashed by the SHA-512 to produce a set of digital signature, which is compared to the hash table in the cloud.

4.4 Analysis

An important feature of our scheme is that digital signature which is dependent on the content of the frames within each GOP. If an unauthorized user uploads the same set of signatures for the particular video then the CSP will reject the uploading. In some case, legal user or authority user modifies the contents of the video therefore a few frame(s) will be changed, then some digital signatures of the GOPs changes. In this case, the CSP will send the message to video_owner and check whether r this uploading with permission of video_owner or not in case of partial modification, the CSP will run Deduplication procedure. In purposed work, a set of hash signatures are extracted locally in user PC and sent it to the CSP separately to avoid the change that will occur in video during transmission from the PC to the Cloud. The modification that can occur in video like (Blurring, contrast increase or decrease, brightness increase or decrease, H.264 compression, frame dropping, shafting and rotation) can affect the signature which makes it impossible to get back the same set of signatures in both sides (PC and Cloud). The CSP requests the user to send the hash signatures of all the GOPs contained in the tampered and compares the hash with hash tables.

5. Methodology and Implementation.

This system is divided into two sections first one is for uploading video and keeps a single copy in the cloud, and the second one is for the Block video from uploading:

5.1 Methodology for Uploading the Video:

1. Register video_owner on the cloud server.
2. Video_owner selects the video to upload and generates the Digital Signatures after compression by using H.264 and SHA-512.
3. Encrypt the generated Digital Signatures with the user password.
4. Video_owner sends encrypted set of Digital signatures to the cloud.
5. The CSP will decrypts the Digital signatures and check whether the received set of digital signatures already exists in the cloud or not,
   i) If the set of signatures has already existed, the CSP will reject uploading the video,
   ii) If the set of signatures does not exist, then the CSP will accept uploading the video and update the signature table.

5.2 Methodology for blocking the Video:

1. Register video_owner on the cloud server.
2. Video_owner generates the Digital Signatures locally by using SHA-512 then upload it to the cloud.
3. In case of other users try to upload the same video with the same set of signatures then

the CSP will reject the uploading process, because set of digital signatures already exist in the cloud.

6. Implementation and Results:

The implementation of the proposed copyright production and deduplication system consists of two components. The two components are implemented as Java applications, and run on a computer equipped with a 2.4 GHz Pentium Dual-Core CPU and 4GB RAM. The test machine runs 64 bit version of windows 7. The implementation has been conducted by keeping in mind the following essential requirements: (i) some digital space must be saved by applying the H.264 compression algorithm and deduplication; (ii) the compression algorithm to be efficient in terms of computation, complexity and storage overheads; (iii) the digital signature generation step must be robust enough to identify the GOPs for copyright and deduplication;(iv) avoiding unauthorized user from uploading. Therefore, our goal is to show that our proposed scheme protects copyright and delete duplicate copy of the video which is uploaded by illegal users.

Table 2. Video Information

Video sequence	Size of video (MB)	Total GOPs	Avg size of GOP(KB)
Foreman	0.944	14	60.74
Akiyo	1.17	20	53.33
Mobile	2.80	20	154.66
Grandma	3.07	58	54.9
highway	6.14	134	49.45

Table 2 gives a specification of these video sequences of different sizes used in a proposed scheme, 5 different video sequences are presented, namely Foreman, Akiyo, Mobile ,Grandma and highway. The videos have been chosen for testing because they belong to different classes of videos [20]. Foreman and highway are classified as non-complex textured and medium intensity video. Akiyo, mobile and Grandma are classified as non-complex textured and low intensity motion videos.
The videos are input into the H.264 compression algorithm. The first frame is the I frame and the rest of the frames are P frames, which implies a IPPP format. The algorithm works on 4 × 4, 16 × 16 MB modes for I and P frames.
The essential requirement of the proposed scheme is that the inclusion of the copyright and deduplication process should not incur any extra overhead on the process of uploading the videos in the cloud storage from the user's end, the proposed scheme should be computationally cost-effective in terms of resources at the user's end. Use the H.264 compression algorithm as the basis of all our further computations. Since videos are compressed anyways before being uploaded in the cloud, the computational overhead in reduced to a great extend. The video_owner is calculating the signatures from the information produced from the compression algorithm .In case to block video from upload by another user, the video_owner upload only sets of signature to CSP with request to block any other user from uploading same video. In case video_owner look to upload has/her video and publishing in the cloud with avoiding other users from uploading same copy, the video_owner need to upload both sets of signatures and compressed video. Average time to calculate Hash signature and length of signatures are showing in Table 3.

Table 3. Compression performance of the videos

Video sequence	Average time to encode(sec)	Average time to calculate Hash signature (sec)	length of signatures (byte)
Foreman	183.713	0.131	3841200
Akiyo	217.615	0.12	3921863
Mobile	208.95	0.17	3658140
Grandma	207.125	0.1507	4305933
highway	275.35	0.158	4358923

From Table 3, it can be observed that the average time to encode the videos is much higher than that to calculate the signature. For example the Grandma video sequence, the average time to encode the video is 207.125 seconds and the average time to calculate the signature at the GOP level is 0.1507 seconds, which is little compared to the time to encode. For example, as can be seen from Table 3, the size of the actual signature for the Akiyo video is 3921863 bytes, which has been reduced to 512 * 20 = 10240 bits by the SHA-512 hash(In case of 20 GOPs generate taken from table 2). These set signatures will be transmitted along with the compressed video, but because of their size, they do not incur any overhead in terms of bandwidth consumption. For the CSP, the benefit comes when compare the sets of

signature rather than entire video. The size of the video to be stored also gets reduced after compression, which is also a benefit for the CSP in terms of storage savings.

If video_owner permit N number of users to publish his/her videos, then the CSP need to apply cross-user deduplication to find out the partial duplicate in the video or full copy duplicate. To calculate the amount of space saved in the cloud storage in the case that the CSP practices cross-user deduplication at the GOPs level the data sets each consists 20%, 40%, 60%, 80% and 100% duplicate of GOPs are prepared.

Table 4 Files duplicate information

Video name	space saved for 20% duplicate of GOPs (MB)	space saved for 40% duplicate of GOPs (MB)	space saved for 60% duplicate of GOPs (MB)	space saved for 80% duplicate of GOPs (MB)	space saved for 100% duplicate of GOPs (MB)
Foreman	0.220	0.439	0.533	0.669	0.899
Akiyo	0.323	0.647	0.972	1.03	1.150
Mobile	0.804	1.606	2.205	2.505	2.750
Grandma	0.827	1.653	1.939	2.388	2.950
highway	1.722	3.444	4.231	5.630	6.135

From the results shown in Table 4, it can be observed that the space saved in the cloud is increasing as the size of the file increases, in case of (20%,40%,60,80%) scheme offer better space saved compared to other schemes ,for 100% duplicate the scheme offer same size of saving.

7. Conclusion and Future work.

In this paper the concept of copyright production and deduplication was proposed to protect the video from illegal uploading and save storage by deleting duplicate copy in the cloud. Copyright production and Deduplication techniques have a lot of advantages, but new techniques pos new challenges. Proposed work provides copyright production, space saving as well as the security to the data, by use SHA-512.The proposed scheme authenticates each GOP within the video separately. For each GOP, robust features are extracted from transform domain of H.264 encoder to generate a unique digital signature by using SHA-512 which is encrypted and uploaded later to the CSP for matching purposes.Experimental results showed that the percentage of digital storage space saved by the CSP is higher than existing one and is secured against the semi-honest CSP since the CSP does not have full information required to recover the video.In the future, we plan to test the proposed scheme in real cloud storage environments. We also intend to strengthen the security of the proposed scheme by incorporating in it proofs of retrievability (POR) of the videos [14][15].There is also a possibility that multiple hash tables may be created for different types of video. This would increase the speed of lookup and is also collision free.

8. References

[1] Implementation of New Secure Mechanism for Data Deduplication in Hybrid Cloud. K. Gangadhara Rao, B.Basaveswara Rao and Qutaiba Mumtaz Dawood.e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. VI (Nov.-Dec. 2016), PP 12-18

[2] Iain E. G. Richardson. The MPEG-4 and H.264 Standards, pages 85–98. John Wiley Sons, Ltd, 2004.

[3] H.264 baseline codec v2. http://www.mathworks.com/matlabcentral/fileexchange/40359- h-264-baseline-codec-v2. Updated on February 2013.

[4] Baris Coskun, Bulent Sankur, and Nasir Memon. Spatio–temporal transform based video hashing. Multimedia, IEEE Transactions on, 8(6):1190–1208, 2006.

[5] Dropbox hacked. http://www.businessinsider.com/dropbox-hacked-2014-10. Accessed on November 2014.

[6] G. Qiu, P. Marziliano, A. T. S. Ho, D. J. He and Q. B. Sun, "A hybrid watermarking scheme for H.264/AVC video," in Proc. 17th Int. Conf. Pattern Recogn., U.K., 2004.

[7] J. Zhang and A. T.S. Ho, "Efficient video authentication for H.264," IEEE Proc. of the first International Conference on Innovative Computing, Information and Control (ICICIC'06), 2006.

[8] Nguyen, D.B.H. Tay, and G. Deng, "A Fast Watermarking System for H.264/AVC Video," IEEE Asia Pacific Conference on Circuits and Syst., APCCAS, pp. 81–84, December 2006.

[9] S. Ueda, H. Shigeno and K. I. Okada, "NAL Level Stream Authentication for H.264/AVC," IPSJ Transactions on Database, Vol. 48, No. 2, pp. 635–643, 2007.

[10] N. Ramaswamy and K. R. Rao, "Video Authentication for H.264/AVC using Digital Signature Standard and Secure Hash Algorithm,"NOSSDAV'06, Newport, Rhode Island, USA, May 2006.

[11] K. Ait Saadi, A. Bouridane and A. Guessoum, "Combined Fragile Watermark and Digital Signature for H.264/AVC video Authentication," EUSIPCO 2009, Scotland, Glasgow 2009.

[12] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 491–500.

[13] T. Wiegand, GJ. Sullivan, G. Bjøntegaard and A. Luthra, "Overview of the H.264/AVC video coding standard," IEEE Trans. Circuits Syst. Video Technol., Vol. 13, No. 7, pp. 560-576, 2003.

[14] A. Giuseppe, B. Randal, C. Reza et al., "Provable dat possession at untrusted stores," Proceedings of CCS, vol. 10, pp. 598–609, 2007.

[15] A. Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 584–597

[16] Richardson, I.E.G.: H.264 and MPEG-4. Video Compression for Next-generation Multimedia.pages NO.:46-50 Wiley, Chichester, England (2004)

[17] Ravi Kumar Vadapalli and P.K. Bora. Perceptual video hashing based on 3d spiht coding of 3d dwt coefficients. In National Conference on Communications (NCC-2008), pages 173–177, 2008.

[18] Cedric D.Roover,Christophe D. Vleeschouwer, F. Lefebvre and Benoit Macq, "Robust video hashing based on radial projection of key frames," IEEE Transactions On Signal Processing, vol. 53, no. 10, pp. 4020–4037, Oct. 2005.

[19] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" . *Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001*. Retrieved October 2, 2012.

[20] Nithin M Thomas, Damien Lefol, David R Bull, and David Redmill. A novel secure h. 264 transcoder using selective encryption. In Image Processing, 2007. ICIP 2007. IEEE International Conference on, volume 4, pages IV–85. IEEE, 2007.