RESEARCH ARTICLE OPEN ACCESS

Secure Video Data Deduplication in the Cloud Storage Using Compressive Sensing

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

ABSTRACT
Cloud storage provides scalable and low cost resources featuring economies of scale based on cross-user architecture. As the amount of data outsourced grows explosively, data deduplication, a technique that eliminates data redundancy, becomes essential. The most important cloud service is data storage. In order to protect the privacy of data owner, data are stored in cloud in an encrypted form. However, encrypted data introduce new challenges for cloud data deduplication, which becomes crucial for data storage. Traditional deduplication schemes cannot work on encrypted data. Existing solutions of encrypted data deduplication suffer from security weakness. This paper proposes a combined compressive sensing and video deduplication to maximize deduplication ratios. Our approach uses data deduplication to remove identical copies of the video. Our experimental results show significant storage savings, while providing strong level security.

Keywords: – Video Deduplication, Compressive Sensing, Cloud Computing, video Compression.

I. INTRODUCTION

Cloud computing provides a new way of Information Technology services by rearranging resources (storage, computing) and providing them to users based on their demands. The most important and popular cloud service is data storage service. Cloud users upload personal or confidential data to the data center of a Cloud Service Provider and allow it to maintain these data. To save space in cloud storage one of the important methods is data deduplication, it is one of the compression technique that allows only one copy of the data to be saved and eliminate the extra copies. Deduplication has proved to achieve higher cost savings, reducing up to 90-95 percent storage needs [1] and up to 68 percent in standard file systems [2]. Clearly, the savings, which can be passed directly to cloud users, are significant to the economics of cloud business. Providers of cloud-based storage such as Dropbox [3], Google Drive [4], and Mozy [5] can save on storage costs via deduplication: should client(s) upload the same file, the server detects this and stores only a single copy. There are two categories of data deduplication, Single User Deduplication and Cross User Deduplication. In the single - user deduplication, only the data belonging to a single user is being scanned to remove identical copies. In cross-user deduplication, the data belonging to different users are being scanned to find duplicates for removal. Cross-user deduplication gives better results than single-user deduplication. However, cross-user deduplication creates privacy and security concerns for users who want to maintain the privacy of their data stored online [6] [7]. To increase security level and privacy, users need to encrypt their data before storing on a remote server, use of the standard encryption method with different keys for each user data which generates different cipher texts to the same data so cloud storage will get different cipher texts for identical file which makes duplicate check in cloud storage impossible. Data deduplication has until now been achieved by using metadata or cryptographic hashes. However, usually the values of hash in each video will affected and show a failure because most of the videos undergo operations like compression, frame rate changes, filtering, spatial geometrical transformations (like shifting, scaling and shearing, bending etc.,) these tools have become insufficient for proper content finding. Compressive Sensing techniques are used in proposed scheme. Compressive Sensing (CS) is a signal acquisition method that can ensure reconstruction with high probability by using a little amount of the random samples, which are obtained by projecting the original

signal onto a random basis linearly [8]. This means that samples are interdependent and follow a certain pattern in their representation. This implies that there is a certain degree of redundancy in the original signal. In case of image and video, low complexity of the sensing scheme plays an important role in designing an imaging sensor. Block-based CS (BCS) scheme, where non-overlapped blocks are sensed separately, comes to solve this issue due to its advantage of low complexity sampling and high reconstruction quality [9]. However, the traditional BCS samples all blocks with the same number of measurements, neglecting the subjective importance of each block to the Human Visual System (HVS), that can lead to difficulty of recovering fine grained details. In this paper, we introduce a novel video deduplication technique based on compressive sensing. In proposed scheme user/s needs to calculate SHA3 hash for each image in GOP. SHA3 is a standard that was developed by the National Institute of Standards and Technology (NIST) based on Message Digest (MD5) algorithm. These hashes used as a seed to generate Φ matrices, then user sends Y matrices to the CSP and keep the hash (seed) in local machine. This paper aims at efficiently solving the problem of video deduplication through compressive sensing in cloud computing. Unlike existing video deduplication systems which work in encrypting whole video and generates hashes for each GOP, may get effected by the operations like shifting, scaling and coding. The advantages of this scheme are threefold.

1) It will allow users to save digital storage space and cost by uploading a portion of a compressed video through compressive sensing.

2) It will ensure the security of the video from the CSP, since only an encrypted part of the compressed video is uploaded which will be meaningless to the CSP without any decompression.

3) Cross-user deduplication will allow the CSP to further save digital storage space by removing identical video coming from different users and keep only a single copy.

The rest of the paper is organized 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 presents Conclusion and future scope of the work.

II. LITERATURE REVIEW

Data deduplication is a technique for eliminating duplicate copies of repeating data in the cloud storage. By deduplication the cloud service provider stores only one copy of the file and passing the link on request. Deduplication can be applied either at the File level or at the Block level. For File level, it deletes the duplicate copy of the same file (identical file). At the block level delete duplicate block occurs in non-identical file. The technique is used to modify storage utilization and can also be applied to network data movement to trim the amount of bytes that must be sent [10]. There are two major categories of data deduplication, Single User Deduplication and Cross User Deduplication. In the single - user deduplication, only the data belonging to a single user is being scanned to remove identical copies. In cross-user deduplication, the data belonging to different users are being scanned to find duplicates for removal. Cross-user deduplication gives better results than single-user deduplication. Unfortunately, Cross-user deduplication would lead to a number of threats potentially affecting the storage system [11] [12]. The theory of Compressive Sensing (CS) provides a new approach for signal acquisition wherein signal can be exactly reconstructed using a small number of random linear measurements, under certain sparsity conditions [15]. Since most signals are indeed compressible in some transform domains, CS has attracted a lot of attention in many applications, including medical imaging, camera design, and multimedia sensor networks due to its potential of reduction of sampling rates, power consumption and computation complexity in the image acquisition. Recent development of compressive sensing (CS) theory has drawn extensive attention, which gives rise to a new solution to signal acquisition and reconstruction [13]. The underlying idea is that when a signal is sparse enough in some domain, it can be decoded from fewer measurements than those suggested by the well-known Nyquist sampling theory [14]. The underlying part in CS is the matrix Φ, there are some desirable properties that we should satisfy it to constructed sensing matrix Φ such as NSP, RIP and incoherence for more details check [17]. This paper proposes a combined Compressive Sensing and data deduplication to maximize deduplication ratios. The recent past in this area of research indicates that not much work has been done to perform video deduplication through CS. The results of this work are being compared with two different schemes of single and cross user deduplication [15][23].In [15] video

compression using the H.264 compression technique for single user deduplication and showed the volume of data to be uploaded to the cloud for different video resolutions. In [23] video compression using the H.264 compression technique for cross user are applied. The results of the three schemes give a proof that using CS for video deduplication is a highly efficient.

III. PRELIMINARIES

This part of the paper first defines the notations used in this paper, followed by a brief review of some security primitives utilized as a part of our secure deduplication. The notations used are given in Table 1.

Table .1. Notations Used in This Paper

Acronym	Description
CSP	Cloud Service provider.
GOP	Group Of Picture.
CS	Compressive Sensing.
BCS	Block-based Compressive Sensing.
RIP	Restricted Isometry Property
KF	Convergent encryption key for file F.
CF	Cipher File.
NSP	Null Space property.
SHA3	Secure Hash Algorithm 3.
H	Hash function.
AES	Advanced Encryption Standard.

A. Convergent encryption.

Traditional encryption though provides data confidentiality, is incompatible with deduplication. Because of this reason that the traditional encryption requires different users to encrypt their data with their own keys. In this case where two identical files being encrypted with different keys will give two different cipher texts so deduplication will be impossible. To overcome this problem convergent encryption is used, the main idea of convergent encryption is that each user encrypts his data by using a convergent key K with symmetric encryption [18].

B. Compressive Sensing

In recent years, compressive sensing (CS) has attracted considerable attention in areas of applied mathematics, and computer science by suggesting that it may be possible to surpass the traditional limits of sampling theory. Compressive sensing builds upon the fundamental fact that we can represent many signals using only a few non-zero coefficients in a suitable basis. Nonlinear optimization can then enable recovery of such signals from very few measurements. The theoretical foundation of compressed sensing is come from Kotelnikov, Nyquist, Shannon, and Whittaker on sampling continuous-time band-limited signals [20, 21, 22]. Their results demonstrate that signals, images, videos, and other data can be exactly recovered from a set of uniformly spaced samples taken at the so-called Nyquist rate of twice the highest frequency present in the signal of interest. The resulting Nyquist rate is so high that we end up with far too many samples. Alternatively, it may simply be too costly, or even physically impossible, to build devices capable of acquiring samples at the necessary rate. CS enables a large reduction in the sampling and computation costs for sensing signals that have a sparse or compressible representation, when the signal is sparse in a known basis we can vastly reduce the number of measurements that need to be stored.

IV. CROSS-USER VIDEO DEDUPLICATION USING CS

Video is a sequence of images to form a moving picture. Frame rate, the number of still pictures per unit of time of video, ranges from six or eight frames per second (frame/s) for old mechanical cameras to 120 or more frames per second for new professional cameras. The minimum frame rate to achieve a comfortable illusion of a moving image is about sixteen frames per second [19]. In the proposed scheme will grouped each 16 pictures called as a Group of picture 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. Now apply Compressive sensing CS for each picture in GOP. Compressive sensing relies on a very simple theory from which the most benefit can be gained in the presence of a sparse signal. A signal can be very efficiently compressed if it is sparse in nature. There are two conditions under which recovery after compressive sensing is possible [17]. The first one is sparsity which requires the signal to be sparse in some domain. The second one is incoherence which is applied through the Restricted Isometric Property RIP.

Now formulate a scheme in the context of video deduplication. Let X be a vector which represents a sparse signal for single image I in GOP for user A. User A then calculates the SHA3 hash for each image in GOP, which is represented as $H_n = SHA(I_n)$, where n is number of images in GOP. Using H as a seed for the random distribution of the Sub- Gaussian Distribution, the user will generates the matrix Φ for each image in GOP which will by default satisfy the RIP property. Now let us suppose User B has an identical copy of the video which contents same set of image I in GOP and calls it P. User B calculates the hash for each image P in

GOP, it will obtain H, exactly the same signal and hash value as I. This method is called convergent encryption [18]. Use of convergent encryption of the same image in GOP through the same algorithm to generate a hash, the resulting Y will be exactly same. The users B or other users will discard X, upload Y to the cloud and keep the seed (H) in local machine. Since the size of H is nominal as compared to Φ and also much smaller than X, the users will not have to save much on their machines. The biggest element in the whole process is the sensing matrix Φ, which will be regenerated with the help of the seed H for each image to obtain the original image to prepare the video. In order to save digital storage space in the cloud environment, the cloud will perform deduplication on the sets of the Y matrices, coming from different users. The CSP receives n number of sets of matrix Y from different users, then apply deduplication to remove identical sets of matrix and keep single sets of matrix Y for each video for multiple users, by this way CSP save a huge space in storage.

The convergent encryption will ensure the generation of the same sets of matrix Φ for identical images belonging to different users. The fact that the user will use the SHA3 hash (seed) of the image as a seed for the random generation of the Sub-Guassian Matrix, will also ensure that identical matrices will be generated for identical images. All this process is transparent to the user since they do not know each other and are still able to produce identical data for a particular video through convergent encryption. The CSP will keep only single unique sets of the Y matrix and will keep track of the users sharing this matrix. In order for a user to decompress the video, he/she will ask the CSP for sets of Y matrices and then by applying the matrix multiplication between Y and Φ (Φ which is generated by the seed), will recover sets of X_s and prepare the video. Since the CSP is semi-honest, it should not be able to extract any information regarding the video from sets of the matrices Y_s.

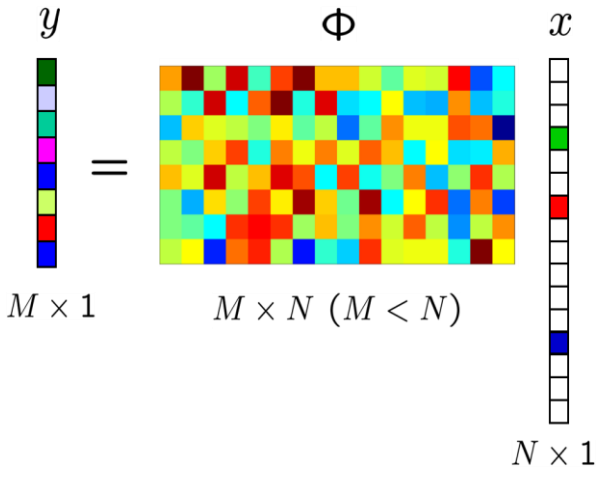

Figure. 1: Compressive Sensing

V. STEP BY STEP PROCESS FOR CS

1. User A calculate SHA3 for each image (I) in GOP for given video, H=SHA (I).
2. These Hashes (H) use as a seed for the random distribution of the Sub-Gaussian Distribution.
3. User A generates sets of matrices Φ which satisfies NSP, RIP and incoherence.
4. Convergent Encryption: User B (try to upload the same video to the cloud) calculates SHA3 for each image (P) in GOP for a given video, H=SHA (P). So here it gives

   H=SHA (I) = H=SHA (P)

5. The cloud will perform deduplication on the sets of the Y matrices, coming from different user/s in order to perform deduplication.
6. The users will discard sets of the matrices X, upload sets of matrices Y to the cloud and keep the seeds (H) in local machine. Since the size of H is nominal as compared to matrix Φ and also much smaller than X, the users will not have to save much on their machines.
7. The CSP will keep only a single unique copy of sets of matrices Y and will keep track of the users sharing these matrices.
8. In order for a user to decompress the video, he/she will ask the CSP for the sets of Y matrices and then by applying the matrix multiplication between Y and Φ (generated by the seeds H), will recover X then grouped together to obtain the video.

VI. SECURITY ANALYSIS

This section discusses the security analysis of the proposed deduplication scheme. The proposed scheme depends on the fact that the user is calculating the SHA3 hash for the each image in GOPs to generate the Sub-Gaussian Distribution for the sensing matrix Φ. A number of weaknesses and attacks had been found on the predecessors of the SHA-2 functions (SHA-256, SHA-512...), so the NIST defined a new standard hash function SHA3, SHA3 is the latest member of the Secure Hash Algorithm family of standards, released on August 5, 2015. In SHA2 hash algorithm the number of rounds was 12 + L, while in SHA3 they increased to 12 + 2L for more protective about security [20]. Also the message padding was changed from a more complex scheme to the simple 10*1 pattern.

Therefore, the probability of a hash collision is nominal. Without the seed/hash of the image, the CSP is not able to generate the sensing matrix Φ from the Y matrix and cannot retrieve the matrix X. The video is therefore secure from a semi-honest CSP.

VII. SYSTEM ARCHITECTURE OF THE PROPOSED SCHEME

In the proposed system, a cross-user cloud storage system is considered where users outsource their data to the cloud storage. Fig 2 presents the system architecture of the proposed scheme, which consists of the following entities:

- User : This is a client who owns the data (Video), and wishes to outsource the data into the cloud storage for the purpose of backup or file-sharing.
- Cloud storage service provider (CSP): This is an entity that offers cloud storage services. It consists of a cloud server and cloud storage.

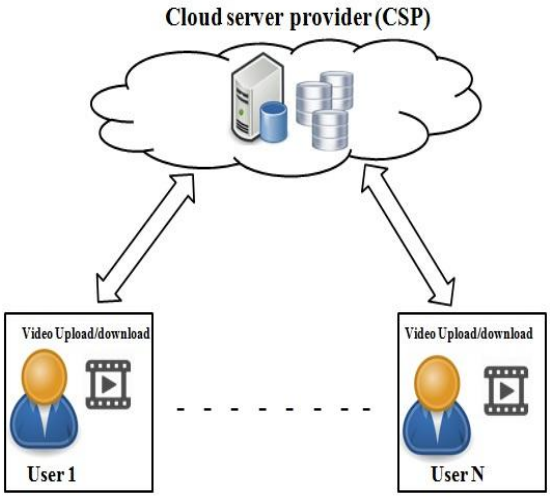

Figure. 2. System architecture of the proposed scheme

Table2. Video Sequences 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 is presented, namely Foreman, Akiyo, Mobile ,Grandma and highway. The videos have been chosen for testing because they belong to different classes of videos [24]. 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.

VIII. IMPLEMENTATION AND RESULTS

The proposed deduplication system is implemented as a Java application, and run on computer equipped with a 2.4 GHz Pentium Dual-Core CPU and 4GB RAM. The test machine runs 64 bit version of windows 7**.** In order to analyze security and efficiency of the proposed scheme, 5 different video sequences are tested on the proposed scheme. The details of these videos are presented in Table 2. The results of experiments compared with the result of two other papers, the first data set taken from experiments in [23] which was for cross-user deduplication using H.264 and hashing SHA-256, the second data set taken from experiment in [15] which was for single-user deduplication using H.264 and SHA-512. The objective of the experiments was to show that using CS for video deduplication yields more efficient results than the previous schemes used H.264. The size of the data to be uploaded will play essential role to achieving optimal efficiency of the scheme. It has been shown that CS performs deduplication more efficiently, allowing the CSP to store less data than when using the previous compression video deduplication schemes using H.264.

Table 3.Comparisim of space saved by using both cross and single user deduplication in H.264 and cross-user deduplication in CS for each GOP in different duplication ratio.

Video sequence	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)		
	H.264 Cross -user by [23]	H.264 Single user [15]	CS Cross -user	H.264 Cross -user by [23]	H.264 Single user [15]	CS Cross -user	H.264 Cross -user by [23]	H.264 Single user [15]	CS Cross -user	H.264 Cross -user by [23]	H.264 Single user [15]	CS Cross -user	H.264 Cross -user by [23]	H.264 Single user [15]	CS Cross -user
Foreman	0.169	0.220	0.253	0.338	0.439	0.456	0.466	0.533	0.712	0.451	0.669	0.850	0.899	0.899	0.899
Akiyo	0.249	0.323	0.488	0.498	0.647	0.976	0.748	0.972	0.999	0.997	1.03	1.12	1.150	1.150	1.150
Mobile	0.618	0.804	0.927	1.236	1.606	1.854	1.850	2.205	2.409	2.015	2.505	2.490	2.750	2.750	2.750
Grandma	0.636	0.827	0.954	1.272	1.653	1.908	1.492	1.939	2.238	1.837	2.388	2.755	2.950	2.950	2.950
highway	1.324	1.722	1.987	2.649	3.444	3.980	3.972	4.231	4.936	5.296	5.630	5.956	6.135	6.135	6.135

Table 3, shows the percentage of increase in the size of both schemes H.264 and CS, H.264 tested in both cases single-user and cross-user deduplication, while the CS is tested in cross-user deduplication only. Cross-user deduplication applied 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. From the results shown in Table 3, it can be observed that the space saved in the cloud is increasing as the size of the file increases, but by using H.264scheme the savings in the space are less than the CS scheme in both single and cross user deduplication but for the case of 100% duplicate were both the schemes offer the same kind of saving. This will consequently reduce the cost for the end user by uploading less data and also reduce the cost to the CSP by deduplication the sets of Yi matrices in each GOPs for different users and keep unique sets for each video. The total data to be uploaded is the size of sets of the Yi matrix generated by multiplying sets of Xi and Φ matrices. The data to be saved by the user for CS scheme is sets of the 256-bit hash value. Sets of the 256 bits are a very small amount of data and almost occupy no major storage space on the part of the user. In CS, there is no loss of information or degradation of video quality.

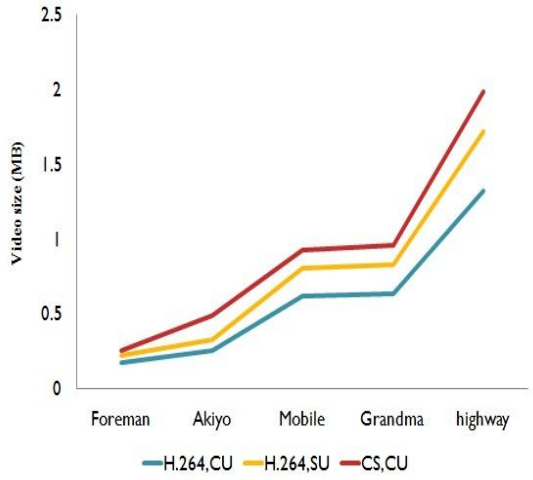

Figure 3. 20% duplicate of GOPs

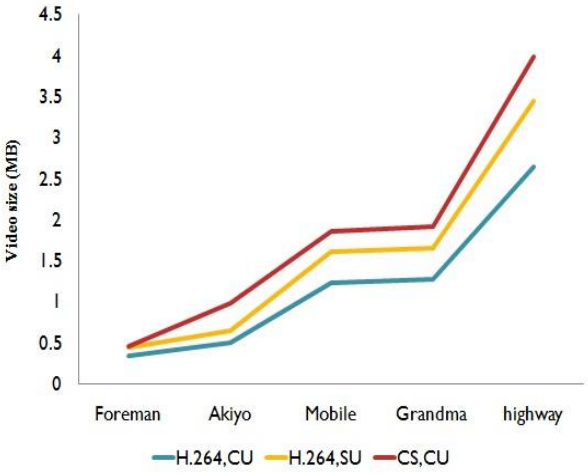

Figure 4. 40% duplicate of GOPs

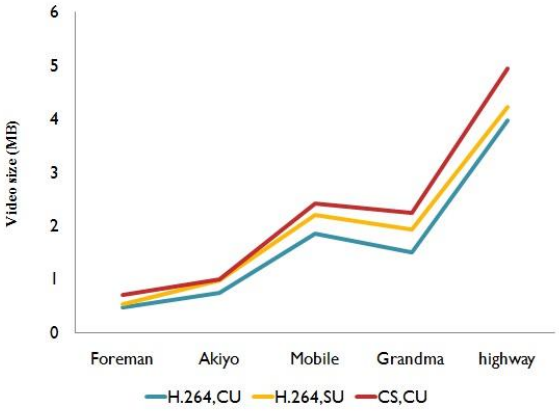

Figure 5. 60% duplicate of GOPs

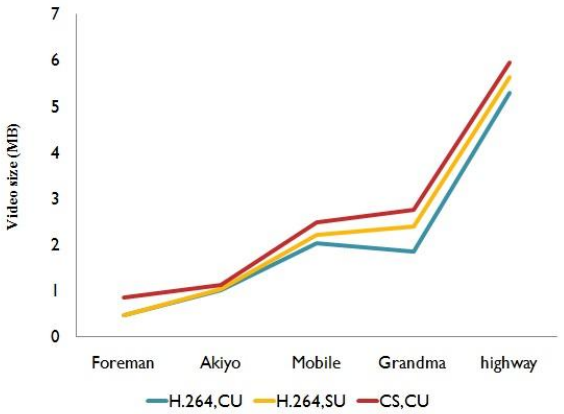

Figure 6. 80% duplicate of GOPs

***CU:Cross-User ,SU:Single-User.**

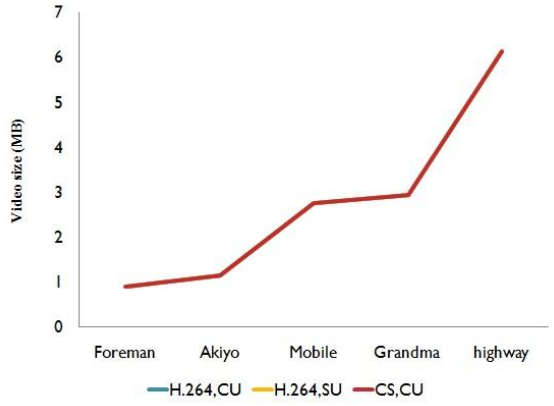

Figure 7. 100% duplicate of GOPs

IX. CONCLUSION AND FUTURE WORK

In this paper, a novel scheme using compressive sensing for performing video deduplication is proposed. Deduplication allows the CSP to remove duplicate videos belonging to different users and save digital storage space. In the proposed scheme, the CSP will charge the users less money and provide them more space. Experimental results showed that the percentage of digital storage space saved by the CSP practicing cross-user deduplication using the proposed scheme 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, there is a possibility that multiple hash tables may be created for different types of files. This would increase the speed of lookup and is also collision free.

As shown in Fig. 3, using CS, CU (Cross-User) scheme achieved biggest amount of space saved in the cloud storage in the case that the CSP practices cross-user deduplication at the GOPs level of 20%. In Fig 4, the CSP practices cross-user deduplication at the GOPs level for40% Fig. 4 and 5 show 60 and 80 % duplicate of GOPs, respectively. Fig. 7 shows 100 % duplicate.

REFERENCES

[1] Opendedup. (2017). [Online]. Available: http://opendedup.org/

[2] D. T. Meyer and W. J Bolosky, "A study of practical deduplication," ACM Trans. Storage, vol. 7, no. 4, pp. 1–20, 2012, doi:10.1145/2078861.2078864.

[3] Dropbox, a file-storage and sharing service. http://www.dropbox.com/.

[4] Google Drive. http://drive.google.com.

[5] MOZY. Mozy, a file-storage and sharing service. http://mozy.com/.

[6] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou. "A Hybrid Cloud Approach for Secure Authorized Deduplication ". In IEEE Transactions on Parallel and Distributed Systems, 2015.

[7] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication" in IEEE Conference on Communications and Network Security (CNS), 2013, pp. 145–153.

[8] Mariv Tello Alonso, Paco Lopez-Dekker, and Jordi J Mallorqu." A novel strategy for radar imaging based on compressive sensing". IEEE Transactions on Geoscience and Remote Sensing, 48(12):4285–4295, 2010.

[9] L. Gan, "Block compressed sensing of natural images" in Proc. Int. Conf. Digital Signal Processing., Cardiff, UK, July 2007, pp. 403–406.

[10] 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.

[11] 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.

[12] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles:- Exact signal reconstruction from highly incomplete frequency information," IEEE Trans. Inf. Theory, vol. 52, no. 2, pp.489–509, Feb 2006.

[13] J. Zhang, D. B. Zhao, C. Zhao, R. Q. Xiong, S. W. Ma, and W. Gao, "Image compressive sensing recovery via collaborative sparsity," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 2, no. 3, pp.380–391, Sep 2012.

[14] E. J. Candes and M. B.Wakin, "An introduction to compressive sampling," IEEE Signal Processing Mag., vol. 25, pp. 21–30, March 2008.

[15] Dr. K. Gangadhara Rao, Dr.B.Basaveswara Rao ,Qutaiba Mumtaz Dawood" Two Phase Approach for copyright protection and Deduplication of Video content in Cloud Using H.264 and SHA-512 " International Journal of Computer Trends & Technology - IJCTT , May 2018, ISSN: 2231-2803.

[16] YONINA C. ELDAR, GITTA KUTYNIOK "Compressed Sensing Theory and Applications" page no.15-26.

[17] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer. "Reclaiming space from duplicate files in a serverless distributed file system". In ICDCS, pages 617–624, 2002.

[18] Andrew B. Watson "Temporal Sensitivity". Sensory Processes and Perception. (1986).

[19] NIST. Nist releases sha-3 cryptographic hash standard. http://www.nist. gov/itl/csd/201508 sha3.cfm, 2016. Online.

[20] V. Kotelnikov. On the carrying capacity of the ether and wire in telecommunications. In Izd. Red. Upr. Svyazi RKKA, Moscow, Russia, 1933.

[21] H. Nyquist. Certain topics in telegraph transmission theory. Trans. AIEE, 47:617–644, 1928.

[22] C. Shannon. Communication in the presence of noise. Proc. Institute of Radio Engineers, 37(1):10–21, 1949.

[23] Fatema Rashid, Ali Miri, Isaac Woungang.A Secure Video Deduplication Scheme in Cloud Storage Environments using H.264 Compression. 2015 IEEE First International Conference on Big Data Computing Service and Applications.

[24] 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.