Journal of
Engineering and
Applied Sciences

MEDWELL PUBLICATIONS
SINCE 2000

Multimedia Image Object Protection in Public Cloud

Ali Mohammed Hameed Al-Saffar
Master of Computer Science, Al-Imam Al-Kadhum College for Islamic Science, Baghdad, Iraq

Key words: Cloud computing, image processing, multimedia object protection, Amazon RDS, AWS

Corresponding Author:
Ali Mohammed Hameed Al-Saffar
Master of Computer Science, Al-Imam Al-Kadhum College for Islamic Science, Baghdad, Iraq

Page No.: 2002-2008
Volume: 15, Issue 8, 2020
ISSN: 1816-949X
Journal of Engineering and Applied Sciences
Copy Right: Medwell Publications

Abstract: Multimedia content is commercially provides over public cloud. Content providers found cloud as a platform for rendering their services. However, they are losing their revenues due to pirated copies made by adversaries. In order to protect multimedia content over public cloud, it is important to have a mechanism for detecting duplicate objects. In this study a framework is proposed for multimedia image object protection in public cloud. The framework has provision for two procedures. The first procedure is reference registration of images into public cloud while the second one is to have a query object and perform matching for detection of pirated objects to trigger protection mechanism. We proposed an algorithm named Cloud Image Object Protection (CIOP) to realize the proposed framework. We collected image dataset known as Caltech 101 for experiments. Amazon AWS is used as public cloud while Amazon RDS is used for object storage. We built a prototype application to demonstrate proof of the concept. The experimental results reveal that the proposed system is capable of protecting multimedia image objects outsourced to public cloud. The results also show the execution time for loading images, signature generation and signature matching.

INTRODUCTION

A new computing paradigm known as cloud computing has emerged with various design objectives shown in Fig. 1. Cloud has specific services such as Software as a Service (SaaS), Platform as a Service (SaaS) and Infrastructure as a Service (IaaS). The design goals of cloud include on-demand self-service, resource pooling, broad network access, rapid elasticity and measured services. Cloud computing has enabled organizations to outsource their data and compute service. Since cloud provides on-demand resource in pay per use fashion, many multimedia content providers started using cloud storage services. When such commercial content is outsourced, possibilities are that they are pirated by adversaries. The pirated or duplicate copies are causing loss to content providers. To overcome this problem, it is essential to have a framework for controlling such misuse of commercial multimedia objects. Many solutions provided in the literature (Susmitha and Babu, 2016; Deepak *et al*., 2016; Gayathri *et al*., 2016; Amirtharathna and Vijayasarathy, 2016) pave way for content protection.

Data such as multimedia image objects are outsourced to cloud IaaS service layer. The storage service of IaaS is responsible to store objects. However, there might be pirated copies in cloud that cause revenue loss to original content providers. In this study, we proposed a framework for protecting multimedia image objects outsourced to cloud. The framework supports both

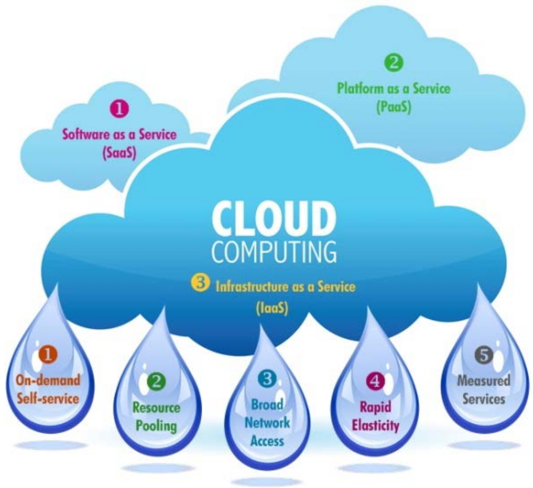

Fig. 1: Cloud computing and its design principles (Calvey, 2013)

object reference registration that includes signature generation and saving objects along with signatures to cloud and signature matching with query objects for verification of illegal copies of outsourced image objects. We proposed an algorithm named Cloud Image Object Protection (CIOP). The algorithm performs operations such as signature generation and matching for performing intended operations of the framework.

Experiments are made with Caltech 101 dataset of images (Greg and Holub, 2006). Original images are outsourced to Amazon EC2 cloud after performing signature generation. Then the original objects are manipulated using software. The modified multimedia image objects are used a query object. Queries are made with 101 categories of images. A prototype application is built to show the utility of the proposed system. Empirical results are observed and evaluated using caougar face category images of Caltech 101 dataset. Our contributions in this study are as follows.

We proposed a framework that includes reference registration, signature matching and signature verification mechanisms. They are meant for storing multimedia image objects and verifying them to protect from piracy.

We proposed an algorithm named Cloud Image Object Protection (CIOP) for realizing both signature generation and signature matching procedures required by the framework.

We built a prototype application to demonstrate outsourcing multimedia image objects and their signatures to Amazon EC2 public cloud and verification of the same with query images that are intentionally inpainted for experiments. The experimental results revealed the efficiency of the proposed framework.

Literature review: Protecting multimedia content in heterogeneous and distributed environment is explored in (Susmitha and Babu, 2016). Signature based identification of multimedia content with cloud assistance is carried out. Multimedia content protection in large scale is studied by (Kanimozhi and Rajalakshmi, 2016) where a Cloud based Multimedia System (CMS) is proposed. Digital signature generation and matching are the two important concepts provided by Deepak *et al*. (2016) for protecting content of multimedia. Hypermedia content protection is explored by Farha and Sreedevi (2016) with reduced computations using cloud computing. A content protection system for different kinds of multimedia objects is explored by Gayathri *et al*. (2016). Kid-tree is the underlying data structure to hold data for processing. Copy detection of video content and its and the advantages of using private cloud to protect multimedia content is studied by Amirtharathna and Vijayasarathy (2016). A survey of cloud based multimedia content protection system is made by Kulkarni *et al*. (2017). As online learning or e-learning became an important platform for education, protecting such content is very important. Towards this end differentially private online learning approach for video recommendations is made by Zhou *et al*. (2015). It was a cloud-assisted video recommendation system that is based on collaborative filtering for bringing about best recommendations.

MapReduce programming paradigm which is in distributed computing environment is studied by Abdelsadek and Hefeeda (2014) for developing a distributed index for tracking and identifying multimedia objects for protecting multimedia content. Encryption and joint fingerprinting are used as part of a hybrid approach by Ye *et al*. (2014) for secure sharing of multimedia content over social networks. A cloud computing platform required by multimedia conferencing applications that are elastic and scalable are studied by Taheri *et al*. (2014). They used IaaS cloud for the empirical study and provided strategies for video conferencing applications. Copyrighted multimedia objects are given legal access to select people. However, the misuse of hem and making pirated copies is the cause of concern. A content protection is provided by NagaKrishna and HemaLatha (2016) for ensuing that copyrighted multimedia objects remain safe and secure.

With multimedia content delivery, it is essential to have Quality of Experience (QoE) perceived by end users. Data fusion and clustering techniques are explored by Baccarelli *et al*. (2014) for achieving required QoE. The innovations in telecommunications such as 3G and 4G networks, it became easier to have multimedia applications. In this context, codifying IP multimedia system is studied by Glitho (2014) for understanding the how and why questions related to it. Signature generation and matching are the two methods explored by Niharika and Sahoo (2016) for protecting multimedia content which is outsourced to public cloud. Signature generation and matching methods employed are used to protect 3D videos. Illegal spreading of multimedia content is the focus of the research by Rajkumar and Kannan (2016) for protecting such content. Traitor tracing protocol is enhanced for ensuring that multimedia content redistribution illegally is prevented. When multimedia objects are stored in cloud or distributed environment, it needs a distributed index for faster retrieval of objects. A distributed index and its utility are studied by Abdelsadek and Hefeeda (2014).

Digital Rights Management (DRM) and media printing are investigated by Huang *et al*. (2010) for protecting rights of multimedia. Identifying media objects that are to be protected and taking care of digital rights using watermarking and encryption approaches. Multimedia search engine known as VertiCut is explored by Qi Chen *et al*. (2015) for effective management of digital media. Safeguarding digital multimedia with a cloud-assisted approach is made by NagaKrishna and HemaLatha (2016). In the literature various approaches are found for protecting multimedia content. However, the protection is inadequate and further research is needed to investigate mechanisms to safeguard all kinds of digital multimedia. In this study, a framework is proposed which is extensible in nature for realizing protection of multimedia.

MATERIALS AND METHODS

Proposed framework: We proposed a framework that can be used by multimedia content owners to protect their media objects from being misused. The framework is divided into two important parts. The first part is reference registration while the second process is verification. The overview of the propose framework is shown in Fig. 2. Multimedia content owner gives image as input. The image is used to generate signature using SHA-1 as use in the proposed algorithm. After generating signature, the signature and original image are outsourced to public cloud. We used Amazon EC2 cloud platform for storage of multimedia image objects.

As shown in Fig. 2, it is evident the content owner can provide query objects for verification process. Once query object is provided, it is subjected to signature generation and signature matching. The signatures due to reference registration available in public cloud are used for matching. The query objects are nothing but original objects inpainted intentionally for object matching evaluation. Signature generation is made with SHA-1 standard for making digest and provide signature for objects uniquely. SHA-1 can provide 160 bit hash value and output named digest which is used in signature generation. Figure 3 illustrates SHA-1 standard.

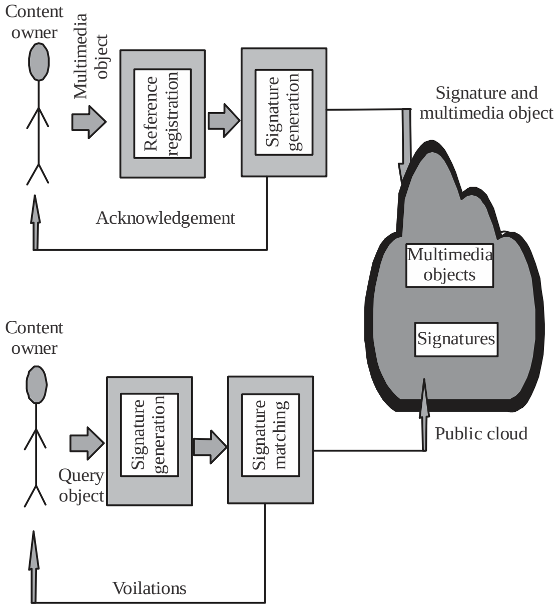

Fig. 2: Overview of the proposed framework for media content protection

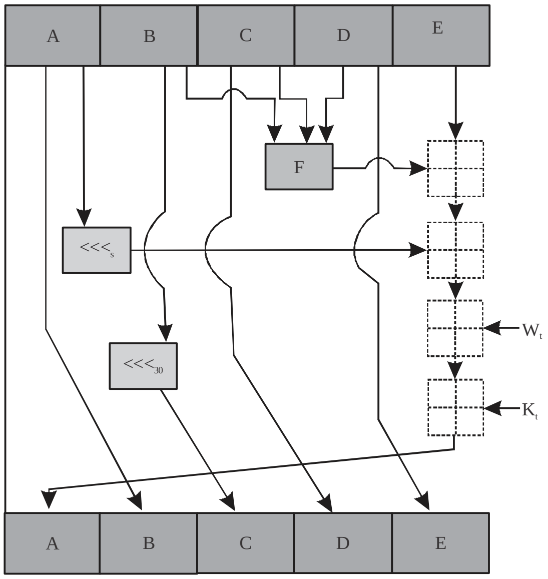

Fig. 3: A single iteration of SHA-1

As presented in Fig. 3, the multimedia object content is denoted as A-E. These are 32 bit word and non-linear function is denoted as F. Once shifts are performed on the inputs, a message digest is generated and referred to a Wt and Kt. This process is repeated for man objects. The digest generated in the underlying signature which is later used in the signature matching operation.

Cloud Image Object Protection (CIOP) algorithm: This algorithm is meant for protecting multimedia image objects outsourced to public cloud. The algorithm takes image dataset, inpainted dataset as inputs and produces signatures of multimedia objects and violation results towards media content protection.

Algorithm 1; CIOP:

```
Algorithm: Cloud Image Object Protection (CIOP)
Input: Image dataset D, inpainted dataset D’
Output: Signatures, violation results (content protection)
Signature generation
1.  For each image in D
2.     Apply SHA-1
3.     Generate message digest md
4.     Generate signature s for image
5.  Save image and s to ClouddB
6.  End For
7.  END IF
Signature matching and protection
8.  Populate signatures S from ClouddB
9.  For each inpainted image img in D’
10.    Follow steps 2-4 to generate signature s for img
11.    IF s is in S THEN
12. found = true
13.          IF found = true THEN
14.            Treat img as pirated
15.            Protect cloud from such img
16.         ELSE
17.            Allow img into the cloud
18.         END IF
19.   END IF
20. End For
```

As shown in algorithm 1, the process involves creation of digest using SHA-1 and then signature generation. The signature matching process needs inpainted images for finding signature similarity to identify duplicate or pirated objects. Once any image is detected as pirated, a protection mechanim is triggered automatically and the image in question is not allowed to get outsourced into public cloud. Thus, the original content owner is protected from loss of revenues.

RESULTS AND DISCUSSION

This section provides experimental setup and results. Experiments are made with multimedia objects such as images. Experiments with other multimedia objects such as videos and audio files for content protection are deferred to our future work. This section provides experimental results related to images as multimedia objects.

Experimental setup: A prototype application is built to have cloud based multimedia object protection. The application demonstrates both reference registration of images and also checking for piracy with object matching mechanism. For doing experiments, image dataset known as Caltech 101 is collected from (Greg and Holub, 2006).

It has images of 101 categories. The proposed system is tested with all categories. However, the experimental results are presented in this study are of cougar face category. Figure 4 shows 10 sample cougar face images.

As shown in Fig. 4, it is evident that the input images are related to cougar face category. They are subjected to inpainting, so as to check the efficiency of the proposed framework in terms of signature generation and signature matching. The original input images are subjected to reference registration in cloud database. Amazon web services is the cloud platform used to make experiments. Amazon RDS with MY SQL is used to store multimedia objects and signatures. The original images are subjected to inpaint using the inpaint software obtained from (Anonymous, 2017). The inpainted counterparts for the original images shown in Fig. 4 are as presented in Fig. 5.

Fig. 4: An excerpt from input images of cougar face category

Table 1: Results pertaining to upload time

Image	Cougar face 1	Cougar face 2	Cougar face 3	Cougar face 4	Cougar face 5	Cougar face 6	Cougar face 7	Cougar face 8	Cougar face 9	Cougar face 10
Upload time (nsec)	6000	5900	6010	6050	5950	6020	6000	6040	5990	6100

As shown in Fig. 5, it is evident that the original image is subjected to inpainting using inpaint tool (Anonymous, 2017) and the inpainting processes followed are polygonal lasso, magic wand, lasso and marker. The original images are given as input to the proposed system for reference registration. Once, the signatures are generated and saved to cloud, their inpainted images are used for experiments. Inpainted object are used as queries to the proposed system. When a query is made its signature is generated and it does match with the original object as much as possible. This is the indication to understand copy paste objects or objects that are pirated with slight or no changes.

Results and evaluation: Experimental results are obtained in terms of time taken for uploading images into the system, time taken for signature generation and matching. Though the dataset contains 101 categories of images and experiment are made with all of them, the results related to 10 select images of cougar face category are presented in this section.

As shown in Table 1, it is evident that the upload time is in nano seconds. The uploading of images is made to prototype application in order to perform further operations.

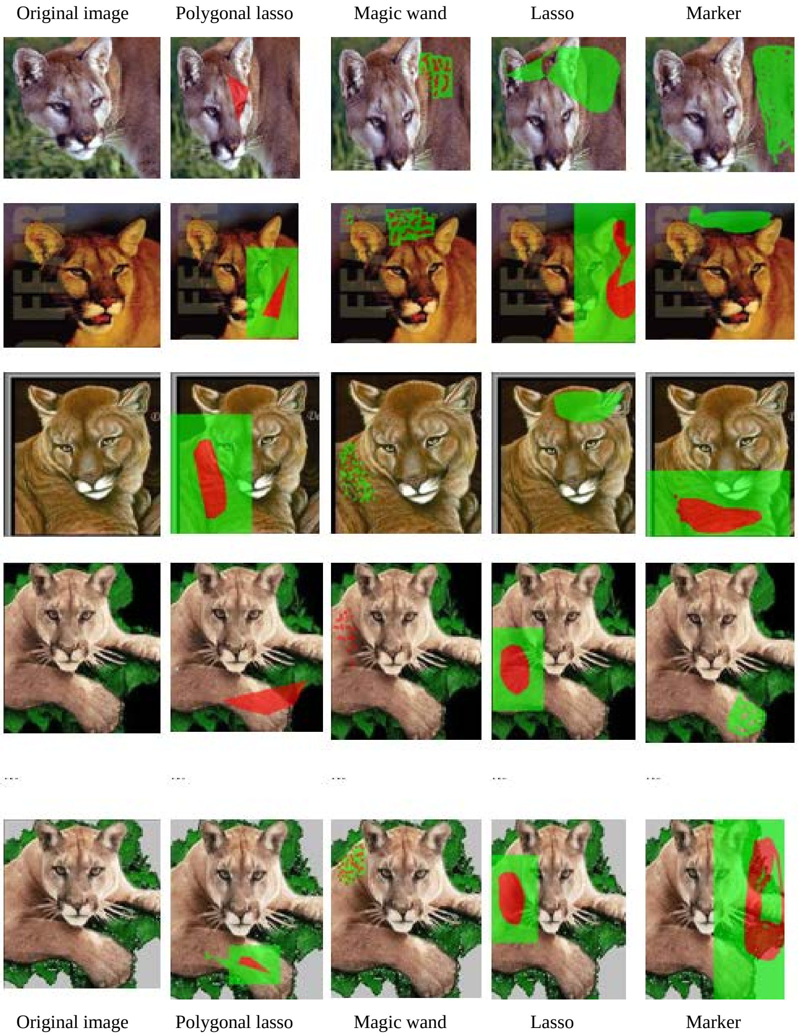

Fig. 5: Inpainted images that are used as query objects

Table 2: Signature generation time

Image	Cougar face 1	Cougar face 2	Cougar face 3	Cougar face 4	Cougar face 5	Cougar face 6	Cougar face 7	Cougar face 8	Cougar face 9	Cougar face 10
Signature generation time (msec)	0.05	0.06	0.07	0.08	0.09	0.1	0.08	0.07	0.06	0.05

Table 3: Signature matching time

Image	Cougar face 1	Cougar face 2	Cougar face 3	Cougar face 4	Cougar face 5	Cougar face 6	Cougar face 7	Cougar face 8	Cougar face 9	Cougar face 10
Signature matching time (msec)	0.1	0.2	0.3	0.4	0.5	0.15	0.25	0.35	0.45	0.48

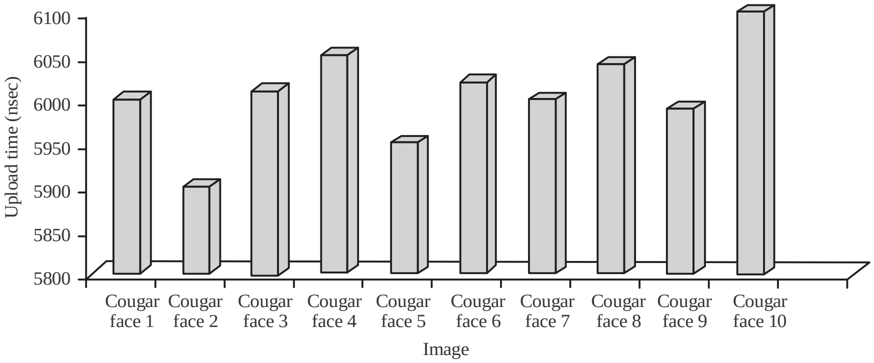

Fig. 6: Upload time taken for each image

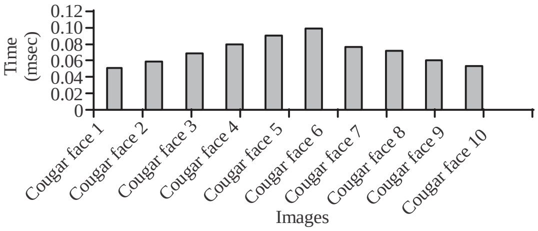

Fig. 7: Signature generation time

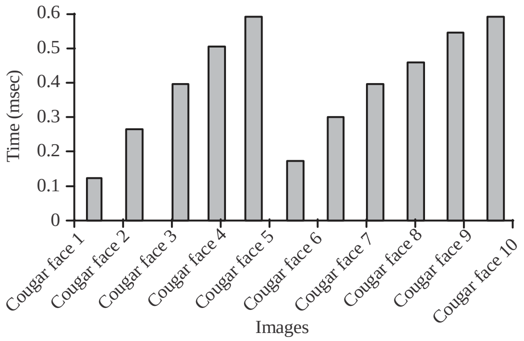

Fig. 8: Signature matching performance

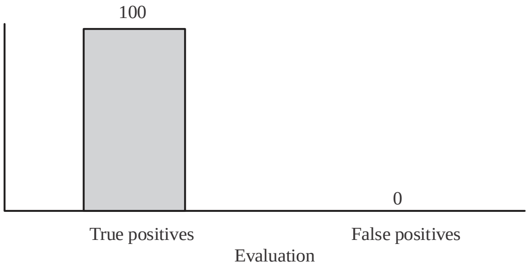

Fig. 9: Evaluation with true positives and false positives

Table 4: Evaluation with true positives and false positives

Parameters	Proposed
True positives	100
False positives	0

As presented in Fig. 6, the image reflects different upload time. The images are uploaded into the prototype application before actually outsourcing to public cloud (Table 2).

As presented in Fig. 7, the signature generation time is observed while making experiments. The results of 10 images are shown where the image took different number of milliseconds (Table 3). As shown in Fig. 8, the signature matching time is presented. The time taken by different images differs. The first image took least time. For each original image, multiple inpainted images are used as query objects to understand the efficiency of the proposed algorithm.

As shown in Fig. 9, it is evident that the proposed system showed 100% true positives. False positives are not reported. It indicates the highest accuracy of the proposed system (Table 4).

CONCLUSION

In this study, we studied protection of multimedia image objects in public cloud. Commercial content owners have been using of late, cloud storage services. Such publicly available content is subjected to duplicate copy or redistribution of intellectual property. In this study, we proposed a framework to solve this problem. The framework is extensible in nature. In this study, it is confined to the protection of multimedia digital image objects. The framework has provision for signature generation for multimedia image objects and also matching. Cloud based solution is provided to realize this.

We proposed an algorithm known as Cloud Image Object Protection (CIOP) to realize the proposed framework. We collected image dataset known as Caltech 101 for experiments. Amazon AWS is used as public cloud while Amazon RDS is used for object storage. We built a prototype application to demonstrate proof of the concept. Results are observed in terms of execution time taken for loading of images, signature generation and matching.

RECOMMENDATION

In future, we extend our framework to support 2D videos, 3D videos and other multimedia objects.

REFERENCES

Abdelsadek, A. and M. Hefeeda, 2014. Dimo: Distributed index for matching multimedia objects using MapReduce. Proceedings of the 5th ACM Multimedia Systems Conference, March 19-21, 2014, Association for Computing Machinery, New York, USA., pp: 115-126.

Amirtharathna, R. and P. Vijayasarathy, 2016. Copy detection of multimedia contents in cloud. Int. J. Eng. Comput. Sci., 5: 16001-16004.

Anonymous, 2017. Inpaint. Wikimedia Foundation, San Francisco, California, USA.

Baccarelli, E., F. Chiti, N. Cordeschi, R. Fantacci, D. Marabissi, R. Parisi and A. Uncini, 2014. Green multimedia wireless sensor networks: Distributed intelligent data fusion, in-network processing, and optimized resource management. IEEE. Wirel. Commun., 21: 20-26.

Calvey, J., 2013. The concept of cloud computing design-principles and paradigms. bodHOST, Edison, New Jersey.

Chen, Q., Y. Liao, C. Mitchell, J. Li and Z. Xiao, 2015. Building a scalable multimedia search engine using infiniband. IEEE. Wirel. Commun., 1: 1-6.

Deepak, N.S.V., M.S. Basha and K. Suresh, 2016. Cloud based protection for multimedia content. Int. J. Inf. Technol., 2: 26-34.

Farha, M. and M. Sreedevi, 2016. An efficient method for protecting hypermedia & reducing computation cost using cloud resources. Int. J. Adv. Trends Comput. Sci. Eng., 5: 77-81.

Gayathri S, M. Priyanka and M. Jaganathan, 2016. Content protection system using matching object for cloud based multimedia. Int. J. Appl. Inf. Commun. Eng., 2: 1-3.

Glitho, R., 2014. Cloudifying the 3GPP IP multimedia subsystem: Why and how?. Proceedings of the 2014 6th International Conference on New Technologies, Mobility and Security (NTMS'14), March 30-April 2, 2014, IEEE, Dubai, United Arab, pp: 1-5.

Greg and Holub, 2006. Caltech 101. California Institute of Technology, Pasadena, California.

Huang, T., Y. Tian, W. Gao and J. Lu, 2010. Mediaprinting: Identifying multimedia content for digital rights management. Computer, 43: 28-35.

Kanimozhi, J.K. and T. Rajalakshmi, 2016. Large-scale multimedia content protection systems. Int. J. Emerging Technol. Comput. Sci. Electron., 23: 12-16.

Kulkarni, V.J., S. Satav and D. Patil, 2017. Survey on cloud-based multimedia content protection. Int. J. Eng. Sci., 7: 4004-4007.

NagaKrishna, L. and D. HemaLatha, 2016. Cloud-constructed combination comfortable security system. Int. J. Eng. Sci. Res. Technol., 5: 730-733.

Niharika, M. and P.K. Sahoo, 2016. Protecting cloud based multimedia content using 3-D signatures. Int. J. Adv. Comput. Tech. Appl. (IJACTA.), 4: 205-208.

Rajkumar, D. and A.R. Kannan, 2016. Illegal multimedia content redistribution protection using enhanced traitor tracing protocol. Int. J. Adv. Res. Biol. Eng. Sci. Technol., 2: 1-8.

Susmitha, B. and B. V. Babu, 2016. An effective and efficient protection system over multimedia using cloud computing. Asian J. Inf. Technol., 15: 3912-3917.

Taheri, F., J. George, F. Belqasmi, N. Kara and R. Glitho, 2014. A cloud infrastructure for scalable and elastic multimedia conferencing applications. Proceedings of the 10th International Conference on Network and Service Management (CNSM'14), November 17-21, 2014, IEEE, Rio de Janeiro, Brazil, pp: 292-295.

Ye, C., Z. Xiong, Y. Ding, G. Wang, J. Li and K. Zhang, 2014. Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks. J. Visual Lang. Comput., 25: 658-666.

Zhou, P., Y. Zhou, D. Wu and H. Jin, 2015. Differentially private online learning for cloud-based video recommendation with multimedia big data in social networks. IEEE. Trans. Multimedia, Vol. 10, No. 10.