International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 6, December 2018, pp. 4204~4211
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4204-4211

A Survey on Multimedia Content Protection Mechanisms

Gottumukkala Hima Bindu[1], Chinta Anuradha[2], Patnala S. R. Chandra Murty[3]
[1,3]Department of Computer Science & Engineering, University College of Engineering & Technology, Acharya Nagarjuna University, India
[2]Department of Computer Science & Engineering, V. R. Siddhartha Engineering College, India

Article Info

Article history:

Received Dec 20, 2017
Revised Jun 4, 2018
Accepted Jul 29, 2018

Keyword:

Cloud-based multimedia content
Multimedia
Multimedia content protection
Video copy detection

ABSTRACT

Cloud computing has emerged to influence multimedia content providers like Disney to render their multimedia services. When content providers use the public cloud, there are chances to have pirated copies further leading to a loss in revenues. At the same time, technological advancements regarding content recording and hosting made it easy to duplicate genuine multimedia objects. This problem has increased with increased usage of a cloud platform for rendering multimedia content to users across the globe. Therefore it is essential to have mechanisms to detect video copy, discover copyright infringement of multimedia content and protect the interests of genuine content providers. It is a challenging and computationally expensive problem to be addressed considering the exponential growth of multimedia content over the internet. In this paper, we surveyed multimedia-content protection mechanisms which throw light on different kinds of multimedia, multimedia content modification methods, and techniques to protect intellectual property from abuse and copyright infringement. It also focuses on challenges involved in protecting multimedia content and the research gaps in the area of cloud-based multimedia content protection.

Corresponding Author:

Gottumukkala Hima Bindu,
Department of Computer Science & Engineering,
University College of Engineering & Technology,
Acharya Nagarjuna University, Guntur, Andhra Pradesh, India.
Email: ghimabindu19@gmail.com

1. INTRODUCTION

Watermarking techniques have been around for content protection or protection of intellectual property in the real world. Watermarking is a process of inserting a distinct pattern into the content of video which is later used for copy detection. The different aspects of watermarking and how it is useful for intellectual property protection on the internet is explained in [1] and digital watermarking schemes for multimedia content protection using different approaches such as asymmetric fingerprinting protocols, zero-knowledge protocols, commitment schemes, and homomorphic encryption in [2]. Interestingly matching techniques complement watermarking techniques. The matching techniques include motion direction, motion matching, ordinal intensity signature, and color histogram signature are explained in [3]. Block cipher algorithm used in [4] for multimedia content protection. Video fingerprinting is also used to identify videos uniquely. Video fingerprint is a vector which can characterize and uniquely identify a video from another video [5]. Full-length video fingerprinting [6] and detection of online abuse of images [7] are two important types of research that play a vital role in protecting intellectual properties. These two incidentally equipped with United State Patents.

Concerning content-based copy detection of multimedia objects, indexing of reference signatures of videos or fingerprints of videos plays a vital role. The recent trends in interactive multimedia computing include multimedia content searching, indexing, visualization, intelligent information extraction, digital

management, multimedia communications, digital signal processing, image, audio and video processing, and multimedia content protection [8]. Multimedia content shared in online social networks (OSNs) is also growing rapidly. Protecting such content has issues and countermeasures as explored in [9]. Digital rights management is another important issue about multimedia content protection. The implementation of novel DRM techniques based on mobile android terminal proposed in [10] and usage of buyer-friendly watermarking protocols in [11] have been proposed to support the protection of copyrighted digital contents.
The remainder of the paper is structured into different sections that provide insights on various techniques used for multimedia content protection.

Table 1. Acronyms

Acronym	Description
HDFS	Hadoop Distributed File System
CBCD	Content-Based Copy Detection
MMMV	Mean of the Magnitudes of Motion Vectors
MPMV	Mean of the Phase Angles of Motion Vectors
DRM	Digital Rights Management
LSH	Locality Sensitive Hashing
SIFT	Scale Invariant Feature Transform
OSN	Online Social Network
M2M	Mobile 2 Mobile

2. VIDEO FINGERPRINTING FOR CONTENT BASED VIDEO IDENTIFICATION

Lee and Yoo (2008) [5] used the concept of video fingerprinting. They proposed a mechanism for content-based video identification using the fingerprinting concept. The overview of the system is presented in Figure 1. It has two important phases known as fingerprint extraction and fingerprint matching. The former is used to obtain a fingerprint from given multimedia object while the latter is used to compare two videos using their corresponding fingerprints.

Figure 1. Overview of video fingerprinting method

The procedure used for fingerprint extraction is illustrated in Figure 2. First of all, the given video is divided into resampled frames and then converted to the greyscale frames. It is done as the grayscale improves the robustness of fingerprint extraction. The resized frames are then partitioned into multiple blocks. Afterward, for each block, the centroid of gradient orientations is computed. Then fingerprint vector is obtained which contains compact features of the video clip which is used to identify video uniquely. Fingerprint matching is an important phase in the proposed system which is responsible for extracting a fingerprint from query video and matches it with that of a video in the database. Their empirical results revealed that the fingerprint matching was able to outperform other features concerning video fingerprinting.

Lu (2009) [12] also explored video fingerprinting for video copy detection. The Metrics used for the mechanism include matching efficiency, low complexity, compact, discrimination, and robustness. Different algorithms are explored namely spatial signatures, temporal signatures, color signatures, transform-domain signatures, and fingerprint matching.

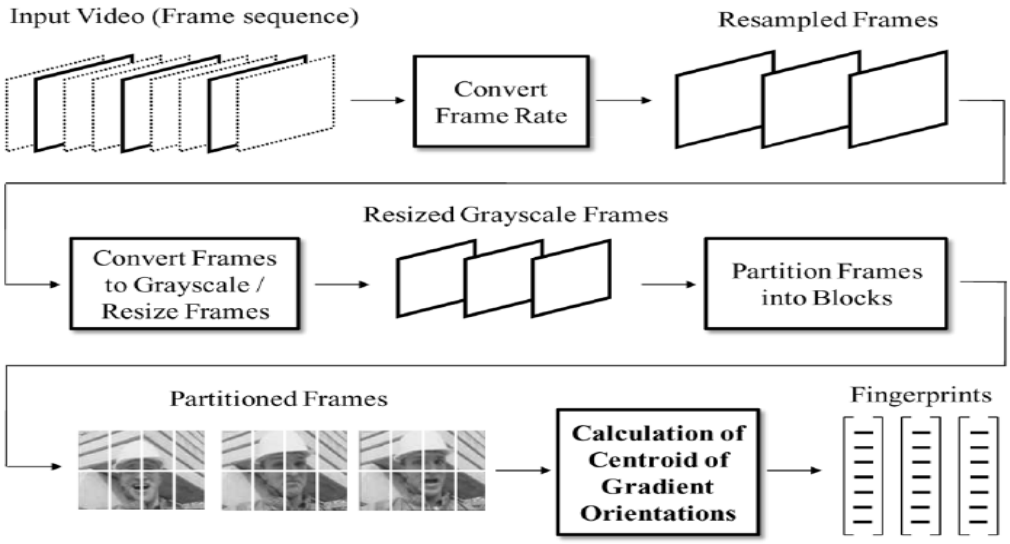

Figure 2. Illustrates the procedure of fingerprint extraction

3. EFFECTIVE AND SCALABLE VIDEO COPY DETECTION

Liu et al. (2010) [13] proposed an algorithm known as content-based copy detection (CBCD) algorithm as shown in Figure 2. The query examples used in this system include either part of reference videos directly or part of reference videos embedded into other videos. As shown in Figure 3, there are two input query video clips. They are used to test the copy detection mechanism employed by using CBCD algorithm. The reference video is flipped in query example 2. Example 1 contains reference video embedded in some region.

The algorithm presented in Figure 4 performs various steps to have content-based copy detection. When query video is given as input, content-based sampling is performed first. Then the query video is subjected to transformation detection and normalization. Finally, SIFT extraction is carried out, and LSH computation is done. These steps are also carried out with a reference video to which the query video need to be compared. Additionally, the LSH indexing is generated for reference video and saved it to the database for reuse. After LSH computation, the query video is subjected to keyframe level query, keyframe level query refinement; keyframe level result merges, video level result fusion, video score normalization and finally CBCD results are generated.

Once the results are generated, they are used to make well-informed decisions. The detection rate and accuracy of the CBCD algorithm showed good performance. The algorithm is scalable as well. Tasdemir and Cetin (2010) [14] used motion vector based features for video copy detection. They were used for reliable verification of signatures about multimedia content as part of CBCD.

Figure 3. Sample query videos (a) Query example 1(b) Query example 2

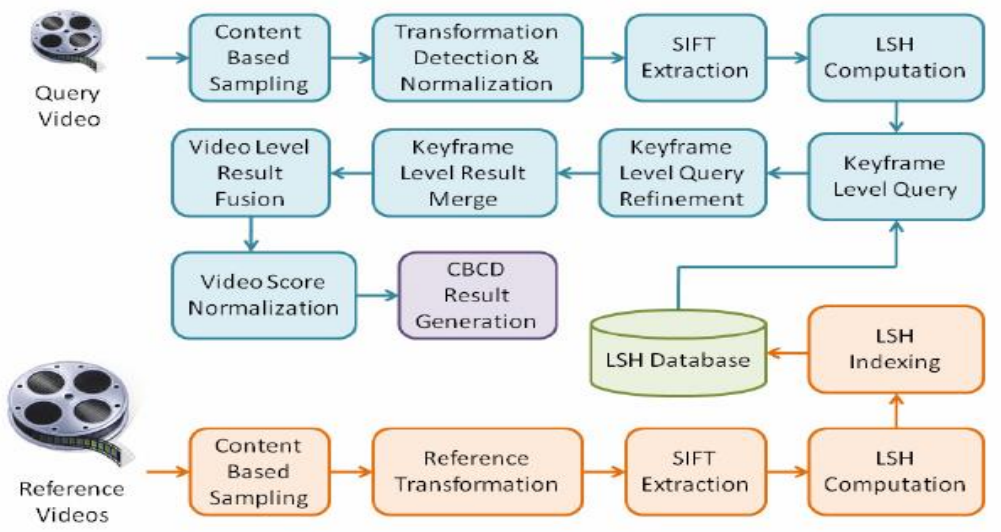

Figure 4. Overview of CBCD algorithm

4. DETECTING 3-D VIDEO COPIES

Khodabakhshi and Hefeeda (2013) [15] proposed a novel content-based copy detection, especially for 3-D videos. First of all the system generates visual signatures for the given 3-D videos. These signatures are maintained in a database. They are known as reference signatures. The query video is then compared against the indexed database references for copy detection. The system is proved to be computationally and storage-wise efficient. They named their proposed system as Spider. The high-level overview of video copy detection system is shown in Figure 5.

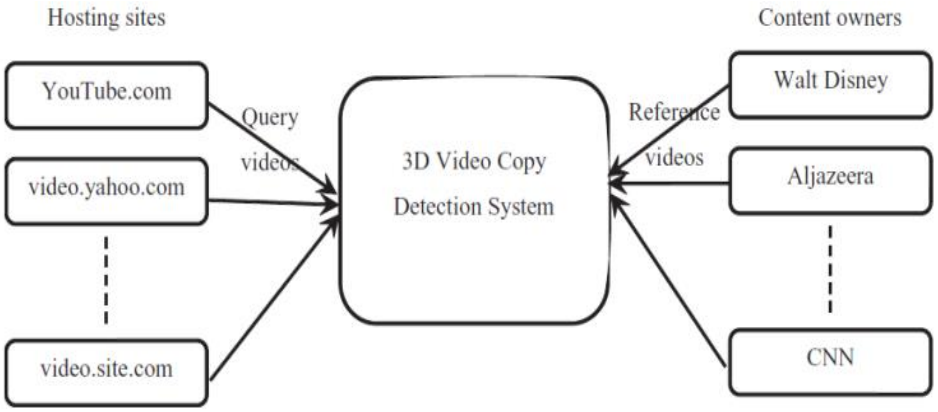

Figure 5. 3D video copy detection system

The people or organizations who own multimedia content are known as content owners. Video hosting sites are websites where videos are hosted. For instance, YouTube is one of the hosting websites. Video copy detection is the process of comparing original video and pirated copy and detecting a copy of the video. The method uses datasets provided by Mobile3DTV, Microsoft, and YouTube. The query videos are further divided into three categories. Type 1 query videos or near duplicate or part of reference videos. Type 2 category are part of reference videos embedded into other videos.

The type 3 videos are the videos that contain no parts of original reference videos. Precision and recall are used to evaluate the system. Ye et al. (2016) [16] focused on mobile to mobile (M2M) communication for secure multimedia content distribution. They proposed a framework for content distribution which is shown in Figure 6. The content protection mechanism is built into a special machine. The special device also provides an index of content to support faster search and identification of videos. The

M2M network can have content distribution capabilities in a secure environment. Delivery of multimedia content over the Internet is explored in [17].

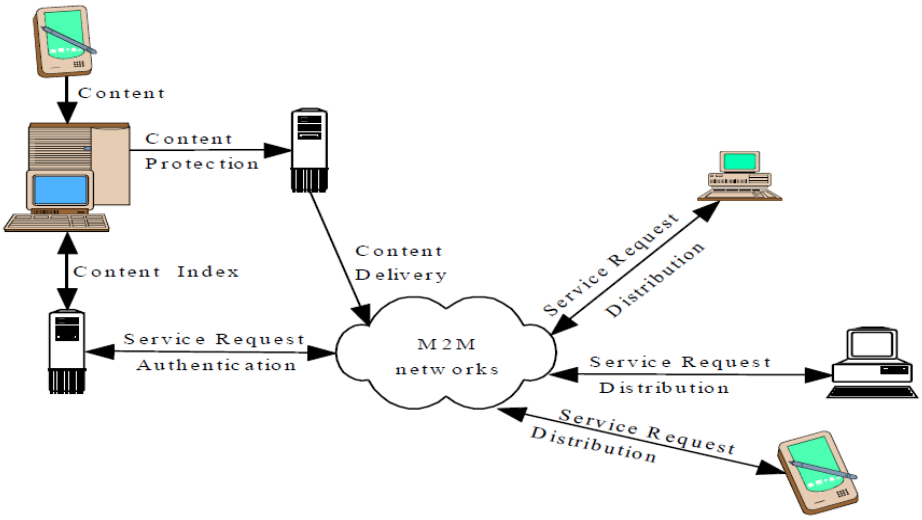

Figure 6. Overview of secure multimedia content distribution framework

5. CLOUD-BASED MULTIMEDIA CONTENT PROTECTION SYSTEM

Hefeeda et al. (2015) [18] proposed a system for large-scale multimedia content protection. It was built for protecting different kinds of media such as music clips, songs, audio clips, images, 2-D videos and 3-D videos. Their system can be deployed either in public or private cloud. They proposed two novel components such as a method for signature generation for multimedia content and a distributed matching engine that is used to protect multimedia objects. The system overview is presented in Figure 8.

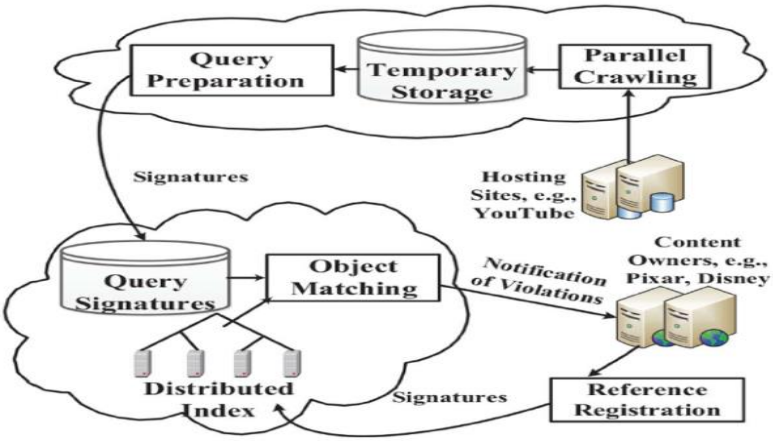

Figure 8. Cloud-based multimedia content protection system

When content owners such as Pixar or Disney hosts new multimedia content over the internet, the content reference registration is made by generating signatures and storing them in a distributed index whereby implementing object matching and query processing. When pirated copies are found over the internet, the query signatures are generated and matched with the signatures stored in the distributed index to detect violations. Wei et al. (2014) [19] proposed a scheme for security and privacy of both computations and storage in the cloud.

5.1. Signature Creation

The system supports different kinds of media for a signature generation. In fact, it supports the creation of composite signature which can have one or more of the elements such as visual signature, audio signature, depth signature, and metadata. The following are the important steps involved in signature generation.

1. Computing visual descriptors for images.
2. Dividing each image into blocks.
3. Matching visual descriptors using Euclidean distance
4. Block disparity computation
5. Compute signature

$$D_i^L\text{-}D_j^R=\sqrt{f_{i1}-f_{j1})^2+\cdots\ldots\ldots\ldots\ldots\ldots+(f_{iF}-f_{jF})^2} \quad (1)$$

$$\sqrt{((x_i-x_j)/W_b)^2+((y_i-y_j)/H_b)^2)} \quad (2)$$

Equations (1) and (2) are used to match visual descriptors and computing block disparity.

5.2. Distributed Matching Engine

The distributed matching engine is made up of object matching and distributed index components. Multimedia objects are characterized by many features containing high dimensions. For instance, an image can be represented by 100-200 SIFT descriptors. In each descriptor, there might be up to 128 dimensions. However, this differs from each multimedia object. A matching engine is constructed that describes object matching logic and distributed index tree that holds signatures of multimedia objects. There are three steps involved in object matching. First of all query data set is partitioned. For each data point, K-nearest neighbors are found. Afterward, application specific object matching is carried out. The precision (3) and average precision (4) are used to evaluate the system by calculating the accuracy of the K-nearest neighbors for a point and over all the points in query set.

$$\text{Precision @ K(p)}=\frac{\sum_{i=1}^{K}\{T_i<=K\}}{K} \quad (3)$$

$$\text{Average Precision @K}=\frac{\sum_{i=1}^{|Q|}\{Precision@K(i)\}}{|Q|} \quad (4)$$

Their empirical results revealed that signature for 3-D videos showed high accuracy regarding precision and recall. Their system is still to be improved to support quick verification of short video segments and live streaming videos for content protection. Similar kind of research is made by Niharika and Sahoo (2016) [20] for cloud-based multimedia content protection system.

6. SUMMARY OF MULTIMEDIA CONTENT PROTECTION METHODS

Table 2 shows a summary of the research that provides insights into different techniques employed for multimedia content protection.

Table 2. Summary of Methods for Multimedia Content Protection

Author & Year	Technique	Advantages	Limitations	Remarks
Hampapur, Hyun, and Bolle (2002) [3]	Sequence matching techniques for copy detection	Detection of copied movie clips	Indexing schemes for parallel convolution are yet to be implemented.	Colour and intensity based signatures are used.
Lee and Yoo (2008) [5]	Novel video fingerprinting method	Performs better than existing ones.	Robustness against transformations is not yet evaluated.	Helps in content-based video identification.
Tasdemir and Cetin (2010) [14]	Vector-based feature set for content-based copy detection (CBCD)	Feature sets represent video for detecting copy detection.	-	Mean of the Magnitudes of Motion Vectors (MMMV) and Mean of the Phase Angles of Motion Vectors (MPMV) are exploited.
Metois et al. (2011) [13]	Detection technique to find an online abuse of images	Characterization of images and thus detection of abuse	-	United Nations Patent

Author & Year	Technique	Advantages	Limitations	Remarks
Saraswathi & Venkatesulu (2012) [4]	Block cipher algorithm	Multimedia content protection with encryption	-	Shows better performance than DES algorithm.
Ioffe (2012) [7]	Full-length video fingerprinting	Characterizes entire duration of the video and supports near-duplicate detection.	-	United Nations Patent
Khodabakshi and Hefeeda (2013) [15]	Novel content-based copy detection for 3D videos.	High precision and recall	-	3D formats of videos are supported.
Wei et al. (2014) [19]	Privacy cheating discouragement and secure computation auditing protocol	Supports secure storage and secure computation as well.	Linear program computation and data mining models are not yet formalized.	A testbed known as SecHDFS is used for the empirical study.
Zhang et al. (2014) [10]	Novel digital rights management (DRM) technique.	Mobile multimedia content is protected using DRM.	-	Protection of copyrighted contents in a mobile environment.
Hafeeda et al. (2015) [18]	Cloud-based multimedia content protection system with signature generation and distributed matching engine.	Supports different types of multimedia content.	Batch processing, support for multi-view plus depth videos are not explored.	The distributed index helps in object matching and query processing.

7. CONCLUSIONS AND FUTURE WORK

Of late multimedia content growing exponentially led to the emergence of the cloud where people in general and multimedia content providers can store and retrieve large volumes of multimedia content. Content providers who are storing multimedia content in public cloud might lose revenues when their legitimate content gets pirated illegally. The rationale behind this is that technological advancements in the computing world made the content duplication and hosting easier. Thus there is every increasing threat to legitimate multimedia content over the cloud. Protecting such intellectual property needs to be given paramount importance. Therefore it is inevitable to have a more sophisticated mechanism that can dynamically protect multimedia content. However, in a distributed environment it is challenging to have computationally intensive operations. In this paper, we make a review of the present state-of-the-art of methods available for multimedia-content protection. The insights of the paper also include opportunities and challenges in the protection of rights of legitimate users of the content. In future, we intend to propose and implement a sophisticated cloud-based mechanism for protecting multimedia content.

REFERENCES

[1] H. E. Suryavanshi, *et al.*, "Digital Image Watermarking in Wavelet Domain," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 3(1), pp. 1-6, 2013.

[2] T. Bianchi and A. Piva, "Secure Watermarking for Multimedia Content Protection: A review of its benefits and open issues," *IEEE*, vol/issue: 30(2), pp. 1-23, 2013.

[3] A. Hampapur, *et al.*, "Comparison of Sequence Matching Techniques for Video Copy Detection," *Storage and Retrieval for Media Databases*, vol. 4676, pp. 194-201, 2002.

[4] P. V. Saraswathi and M. Venkatesulu, "A Block Cipher Algorithm for Multimedia Content Protection with Random Substitution using Binary Tree Traversal," *Journal of Computer Science*, vol/issue: 9(8), pp. 1541-1546, 2012.

[5] S. Lee and C. D. Yoo, "Robust Video Fingerprinting for Content-Based Video Identification," *IEEE transactions on circuits and systems for video technology*, vol/issue: 18(7), pp. 983-988, 2008.

[6] S. Ioffe, "Full-Length Video Fingerprinting," *United States Patent*, pp. 1-11, 2012.

[7] E. Metois, *et al.*, "Detecting Online Abuse In Images," *United States Patent*, pp. 1-10, 2011.

[8] R. Boutaba, *et al.*, "Recent trends in interactive multimedia computing for the industry," *Cluster Computing*, vol. 17, pp. 723-726, 2014.

[9] C. Patsakis and A. Zigomitros, "Achilleas Papageorgiou and Agusti Solanas Privacy and Security for Multimedia Content shared on OSNs," *Issues and Countermeasures, The British Computer Society*, pp. 1-18, 2014.

[10] Z. Zhang, *et al.*, "A novel approach to rights sharing-enabling digital rights management for mobile multimedia," *Springer Science*, pp. 1-17, 2014.

[11] F. Frattolillo, "A Digital Rights Management System Based on Cloud," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol/issue: 15(2), pp. 671-677, 2017.

[12] J. Lu, "Video fingerprinting for copy identification: from research to industry applications," *Media Forensics and Security*, vol/issue: 725402(1), pp. 1-15, 2009.

[13] Z. Liu, *et al.*, "Effective and Scalable Video Copy Detection," *International conference on Multimedia information retrieval* Pages, pp. 119-128, 2010.
[14] K. T. Demir and A. Enis C., "Motion Vector Based Features for Content-Based Video Copy Detection," *International Conference on Pattern Recognition*, pp. 3134-3137, 2010.
[15] M. Hefeeda and N. Khodabakhshi, "Spider: A System for Finding 3D Video Copies," *ACM*, pp. 1-20, 2013.
[16] C. Ye, *et al.*, "Secure Multimedia Content Distribution for M2M Communication," *International Journal of Security and Its Applications*, vol/issue: 10(4), pp. 279-288, 2016.
[17] F. Fund, *et al.*, "Under a cloud of uncertainty: Legal questions affecting Internet storage and transmission of copyright-protected video content," *ACM*, pp. 1-14, 2016.
[18] M. Hefeeda, *et al.*, "Cloud-Based Multimedia Content Protection System," *IEEE Transactions on Multimedia*, vol/issue: 17(3), pp. 1-14, 2015.
[19] L. Wei, *et al.*, "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371–386, 2014.
[20] M. Niharika and P. K. Sahoo, "Protecting Cloud-Based Multimedia Content using 3-D Signatures," *International Journal of Advanced Computing Technique and Applications*, vol/issue: 4(1), pp. 1-4, 2016.

BIOGRAPHIES OF AUTHORS

Mrs. G.Hima Bindu pursuing Ph.D. in the Department of Computer science and Engineering, Acharya Nagarjuna University. She was awarded B.Tech in Information Technology in 2004 and received M.tech in Computer Science and Engineering in the year 2009. Her research interests include Security.

Mrs. Ch. Anuradha was awarded B.Tech in Information Technology from Acharya Nagarjuna University in 2007 and received M.tech in Computer Science and Engineering from JNTU Kakinada in the year 2014. Presently she is working as Assistant Professor in Department of Computer Science & Engineering, V. R. Siddhartha Engineering College Engineering. Her research interests include Image Processing and Data mining.

Dr. P. Sri Rama Chandra Murthy was awarded B.Tech in Computer Science and Engineering from JNTUH in 2005 and received M.tech in Computer Science and Engineering from Acharya Nagarjuna University in the year 2008. He was awarded a doctorate in the year 2013. Presently he is working as Assistant Professor in Department of Computer Science & Engineering, Acharya Nagarjuna University. His research interests include Digital Image Processing, Data Mining, Network Security.