A Survey of Digital Watermarking Techniques for Data Protection in Cloud Computing

Abbas Nna Halima
Department of Computer Science
Federal University of Technology
Minna, Nigeria
Halimanna1983@gmail.com

Mohammed Danlami Abdulmalik
Department of Computer Science
Federal University of Technology
Minna, Nigeria
drmalik@futminna.edu.ng

Solomon Adelowo Adepoju
Department of Computer Science
Federal University of Technology
Minna, Nigeria
solo.adepoju@futminna.edu.ng

Enesi Femi Aminu
Department of Computer Science
Federal University of Technology
Minna, Nigeria
enesifa@futminna.edu.ng

***Abstract* - Recently digital watermarking techniques played an essential role in protecting and authenticating the copyright of multimedia content in a cloud. Based on the literature, there are several digital watermarking techniques used for data protection in cloud computing. However, each of these techniques has its own limitations such as high levels of piracy, theft, and unauthorized distribution of multimedia content. This Survey employs a content-based analysis approach to investigate the watermarking techniques that are more secure, imperceptible, and robust against various kinds of multimedia attacks. The survey shows that the hybridization of watermarking techniques and feature descriptors is more efficient in comparison to a single watermarking technique. This research work concludes that the hybridization technique and use of descriptors are more secure.**

***Index Terms: Digital Watermarking, multimedia contents, feature descriptors, authentication, robustness, hybridization*.**

I. INTRODUCTION

Cloud computing has emerged as one of the most efficient computing paradigms in the world of information technology in recent years. This is due to an increase in parallel, grid-distributed, and other paradigms form of computing [1]. In Cloud, computing customers are offered three basic service models; the SaaS model, the IaaS model, and the PaaS model. The SaaS model which means Software as a service is primarily designed for the end user who has to use the software in performing their day-to-day activities. However, the Platform as a service (PaaS) is primarily designed for developers that require a platform environment to develop their software and application [1]. While Infrastructure as a service (IaaS) is built for network architect development requirement service. User data and information can be stored and accessed via the cloud without the knowledge of data located in the cloud. Security in cloud computing has been frequently raised as one of the most pressing issues in computing. In other to establish ownership authenticity and prevent the issues of data misusing, multimedia information or content can be secure using the watermarking approach. Cloud computing has three categories which include public cloud computing; this cloud computing service are been provided by a third-party body that is built on the internet, this service is accessibly by any customer or users who want to use it by paying for the specific service they are consuming [2]. Secondly, Private Cloud computing services are being provided or accessed via the internet or a private network. In this category, services are offered to only a specific set of users, though a high level of security and privacy is implemented through internet hosting and firewall. Finally, the hybrid cloud service provides a combination of private and public cloud services to users. Within the hybrid cloud, both public and private clouds can be managed independently but applications and data can be distributed or shared among the clouds in the hybridized cloud (private and public cloud) [2].

The massive inventions of digital multimedia products lead to the high demands on authenticity, protection, and security of any digital multimedia content [3]. The potential solution is presented with the inventions of digital watermarking approaches, which tends to secure ownership rights and interest by embedding certain form of information secretly that is only known to the owner into the digital media intended to be secure.

Furthermore, watermarking can be defined as the method of embedding a dual or single watermark item into digital multimedia content such as audio, images, and video content [3]. The three types of watermarking techniques are spatial domain, frequency domain, and hybrid domain. The most common examples of frequency domain watermarking techniques or approaches include SVD (Singular Value Decomposition) and the Karhunen-Loeve Transform (KLT). The spatial domain approaches are basically the initial techniques adopted, in which embedding of the watermarked image can be achieved by modifying the pixels of the image directly [3]. The spatial domain is widely used due to the advantages derived in terms of low computational cost and accessibility to implementation. For example, the LSB (Least Significant Bit), spectrum, and correlation base are the most common spatial domain algorithm. Additionally, there are three types of watermarking systems; blind watermarking, non-blind watermarking, and semi-blind watermarking. Although the original image is not required in the blind watermarking, because the techniques only extract the watermarked image. The blind watermarking approach is

978-1-6654-9370-3/22/$31.00 ©2022 IEEE