Chapter 5
Defending Multimedia Content Embedded in Online Social Networks (OSNs) Using Digital Watermarking

Brij B. Gupta
National Institute of Technology, Kurukshetra, India

Somya Rajan Sahoo
National Institute of Technology, Kurukshetra, India

Prashant Chugh
National Institute of Technology, Kurukshetra, India

Vijay Iota
National Institute of Technology, Kurukshetra, India

Anupam Shukla
National Institute of Technology, Kurukshetra, India

ABSTRACT

In global internet usage, increasing multimedia message, which includes video, audio, images, and text documents, on the web raised a lot of consequences related to copyright. For copyright protection, authentication purpose and forgery detection digital watermarking is the robust way in social network content protection. In this technique, the privacy information is embedded inside the multimedia content like image and video. The protected content embedded inside multimedia content is called watermark-enabled information. To make more effective the process of watermarking, the content encrypted before embedding to the image. Basically, the digital watermarking embedded process implemented in two different domains called spatial and frequency domain. In spatial domain digital watermarking, the watermark information is embedded in the least significant bit of the original image on the basis of bit plane selected and on the basis of the pixels of image, embedding, and detection is performed.

DOI: 10.4018/978-1-7998-2701-6.ch005

INTRODUCTION

As in the social media perspective the pattern of communication with each other in social media has changed after mid-1990. Multiple online social networks like Facebook, Twitter, Instagram, and WhatsApp ease the distribution of user's real-time information between multiple users over the same and different networks. Due to multiple characteristics of online social networks like, ease of use, faster transformation and less expensive, it becomes the significant way of communication and information sharing. Nowadays, almost all the social network users access the news through online channels (Zhang et al., 2017). However, due to the increasing popularity of OSNs, the use of the Internet becomes an ideal way of communication and spreading of fake news. The spreading of fake news in the form of misleading content, fake reviews, fake rumours, advertisements, fake speech regarding politics, satires and many more through images. Currently, fake news is spread faster in social media rather than mainstream media (Sahoo & Gupta, 2020; Sahoo & Gupta, 2018). To protect the multimedia content like images, videos, texts and audios from attackers digital watermarking is the process to hiding and embedding certain information digitally to that content (Sahoo & Gupta, 2019). It is the effective way to protect the rights of the user/author of multimedia content and find whether the content misused/ manipulated by some unauthorized user on that network (Balan et al., 2017; Zedan et al., 2017; Sahoo & Gupta, 2019). The Digital Watermarking is related to the steganography technique in some extent. In that technique we hide the text message behind any multimedia content available. The processes of Digital Watermarking authenticate the status of the owner or author of that multimedia content. In past, different field uses Watermarking technique for protecting the similarity, i.e. watermarks were originally used in paper and subsequently in paper bills (Singh et al., 2012). The popularity of internet in past years has expanded rapidly due to the social networks and their contents like audio, video, images and other personal as well as professional content sharing method. Hence, copying the original content and altering the theme for malicious purpose becomes increases day by day and affect the normal users. Therefore, protecting multimedia content from unauthorized access, digital watermarking is the strongest way (Abraham et al., 2016). In Digital watermarking, the original multimedia content is embedded through signal or data (Li et al., 2019; Li et al., 2018; Gupta et al., 2015). The same principle also used to embed in audio, video and images also (Ansari et al., 2012). The embedded information in original multimedia content is known as watermarked content and that can be extracted and deleted with some specific predefined application and algorithms. The watermarked content may be in the form of image, audio and text etc. As per the digital signal presence in each and every unchanged copy of the original information or content, it behaves as a digital signature for all copies (Verma et al., 2006). The original multimedia content embedded with digital watermarking should be tenured, robust, unperceivable, and comprises of all information about multimedia content ownership. In order to accomplish maximal aegis, the watermark should have these properties 1) It must be protected and undeletable by hacker and attackers; 2) It should be undetectable if analyzed statistically, i.e. encrypted watermark 3) It should be tolerant to compression techniques like lossy 4) It should be tolerant to dissimilar varieties of operations that can be performed on that content; 5) It must be perceptually invisible. The process of Watermarking is categorized into two main categories. The two categories include the spatial domain watermarking and the frequency-domain watermarking (Patel et al., 2013). In spatial-domain watermarking techniques, on the basis of the pixels of image, embedding and detection is performed. Spatial domain watermarking method is a technique in which pixel values of original image are modified for embedding the watermark information in it. This technique is very easy to implement but are not robust against different types of attacks including compression and cropping (Cheng et al., 2004). In order to prevent from different attacks, the watermark is en-