Chapter 31
Integrating Content Authentication Support in Media Services

Anastasia N. Katsaounidou
Aristotle University of Thessaloniki, Greece

Charalampos A. Dimoulas
Aristotle University of Thessaloniki, Greece

ABSTRACT

The chapter investigates content authentication strategies and their use in media practice. Remarkable research progress has been conducted on media veracity methods and algorithms, however without providing that much straightforward tools to users involved in real-world applications. Hence, there is an urgent need for further support content verification by exploiting all the available methods in properly integrated online environments, forming a media authentication network. On-demand training (and feedback) on these technologies is considered of major importance, enabling users to collaborate with media and forgery experts towards adoption, refinement, and widespread dissemination of best practices. Better comprehension of the involved tools and algorithms would propel their broad exploitation in practice, gaining valuable feedback for further improvements. Thus, a continuously updated online repository, containing documented examples, learning resources, and media veracity tools could be adaptively accommodated, better supporting various users and applications needs.

INTRODUCTION

The tremendous evolution of Information and Communication Technologies (ICT) and the low cost of the digital media devices have fueled the widespread expansion of the so-called User Generated Content (UGC). Social networking has become a popular way for users to meet and interact online through text and audiovisual content (photos, sounds, videos, etc.) that is produced and distributed in real time. Traditionally, users share news and multimodal content through social media, while simultaneously discover information on the Web. Among others, trust is considered to be one of the crucial factors of

DOI: 10.4018/978-1-5225-7766-9.ch031

information capturing and dissemination. In the road from Web 2.0 to Web 3.0 and beyond, the quality and credibility of the recorded, shared and broadcasted content is controversial (Ljung & Wahlforss, 2008; Matsiola, Dimoulas, Kalliris & Veglis, 2015). Many (easy to use) multimedia capturing and processing tools (desktop applications and online /cloud services) are currently available and can be exploited literately at any time and place through mobile devices. This "processing at the fingertip" vision familiarizes average users with multimodal media production, processing and management tasks (Dimoulas, Veglis & Kalliris, 2014, 2015).

The domination of digital content over traditional analog media (i.e. films and tapes) has given rise to a number of new information security challenges. Digital content can be processed, intentionally altered or falsified and redistributed relatively easy. This has important consequences for governmental, commercial, social and professional media organizations that rely on digital information (Stamm, Wu & Liu, 2013). Hence, mass communication and journalistic processes can be associated to unwanted content tampering, construction of fake evidences, sharing and propagation of untrue stories. In particular, the universality of "digital news reporting" has turned the evaluation of shared media into a field of prime importance, focusing on the automatic detection of manipulated and misused Web content (Mendoza, Poblete & Castillo, 2010). Its aim is to lay the basis for a future generation of tools that could assist media professionals in the process of verification. According to Figure 1, where the problem definition of the discussed topic is presented, media alteration involves all content types (text, images, audio, video, etc.) that are encountered in today's Multimodal Media Assets (Dimoulas et al., 2014; Katsaounidou, 2016).

Content alteration can be conducted by anyone involved in the media production processes (media professionals, UGC–citizen journalist, etc.), as the bluish arrows in Figure 1 indicate. Once information falsification occurs without being noticed by the users, uncontrolled propagation of untrue stories may appear as a side effect of the contemporary need for timely and immediate informing. Hence, tampered information can be massively shared /propagated by end-users/consumers (greenish-dotted arrows in Figure 1). The outmost target of the current chapter is to describe a collaborating model for overall supporting content authentication through dedicated computerized environments. In this context, users' and journalists' training (and their valuable feedback) holds a key role towards the integration and unification of applicable media veracity services (and their associated learning resources). Thus, algorithms, methodologies and related ground-truth data-sets would be continuously updated, progressed and adapted to the specific needs of the encountered application scenarios.

BACKGROUND

Multimodal items can be evaluated and verified with a variety of methods. In principle, different authentication strategies are associated to various content entities, based on their distinct communication and operation attributes. Context-aware is the simplest authenticity analysis approach that can be applied in most media types, purposing to detect and pull abnormal information out of the content by exploiting human observation and cognition abilities (Silverman, 2013; Katsaounidou, 2016). Missing or unexpected shadows /reflections are common examples in the case of tampered images (Johnson & Farid, 2007; Farid, 2009; Krawetz, 2007). Syntax errors and/or absence of meaning indicate potential tampering in text messaging (Zubiaga & Ji, 2014). Abruptly interrupted background sound, unexpected intonation, and pitch changes form "novelty detection" indicators that reveal possible audio forgery regions (Dimoulas & Symeonidis, 2015; Gupta, Cho & Kuo, 2012; Hua, Zhang, Goh & Thing, 2016; Kotsakis, Mislow,