

Design of Authenticity Identification Scheme for Audio Ownership Protection and Image Tampering Verification

リンバ ウィディアナ チプタサリ

<https://doi.org/10.15017/1398389>

出版情報：九州大学，2013，博士（学術），課程博士
バージョン：
権利関係：全文ファイル公表済



(別紙様式2)

氏 名 : リンバ ウィディアナ チプタサリ

論文題名 : Design of Authenticity Identification Scheme for Audio Ownership Protection and Image Tampering Verification
(オーディオ所有権保護と画像改ざん検証の為の真正性識別スキームの設計)

区 分 : 甲

論 文 内 容 の 要 旨

The advent of the digital era has spread the use of digital multimedia in virtually all areas. Multimedia signal can be easily reproduced and manipulated without any trace of alterations. Constructing a scientific and automatic way for confirming the legitimacy or truthfulness of the structure and/or content of multimedia is an important task, which is the aim of this dissertation. There are two major approaches to multimedia authentication, i.e., active and passive approaches. The former may work in two areas: digital watermarking and signature authentication. In case of digital watermarking, it works by inserting a digital watermark into the host data at the source side, and verifying the watermark integrity at the detection side. In the sense of authentication, the signature is generated by extracting host data features at the source side, and verifying the integrity by comparing the signature at the receiver side. On the contrary, the latter accomplishes data authentication without any prior information. That is, image authenticity is verified without the presence of either digital watermark or signature. Both approaches are discussed and exploited in the thesis.

The thesis fundamentally addresses two main subjects: audio ownership protection and image forensics. The former is usually thought as an active approach, while the latter is referred to as a passive approach. In more details, the organization of the thesis is as follows. Chapter 1 introduces the motivation, problem formulations, and our main contributions. Chapter 2 provides literature reviews of both active and passive approaches. In more details, digital signature, digital watermarking, and trustworthy digital camera are described as related literatures to active approach. As for the passive approach, image forgery detection and image source identification are discussed. Chapter 3 introduces our contribution in the active approach, namely digital audio watermarking through direct feature-based method. Chapter 4 describes on exploiting reference images in exposing copy-paste forgeries. Chapter 5 deals with how to expose geometrical distortion through reference images. To conclude, Chapter 6 summarizes the work and provides research directions.

Numerous ownership protection schemes have been proposed. However, none of these works

provides a formal structure from which the scheme is adopted. This situation arises as our first challenge issue. In Chapter 3, we begin with defining a formal scheme of ownership protection named *direct feature-based method*, as an alternative approach to traditional digital watermarking. Actually, this is not a new method for the researchers in digital signature field. As the traditional approach embeds “digital watermark” into the host data, it may cause distortion, such as quality degradation. Furthermore, trade-off between capacity and other important properties, such as imperceptibility and robustness, emerges as an inherent problem. Direct feature-based provides a solution to overcome such situations. We proceed to propose a resilient audio ownership protection scheme. We exploit index data instead of index field to generate the watermark key so that the number of watermark’s keys is much smaller than in the existing work. We then demonstrate the effectiveness of the proposed scheme against severe distortions. Experimental results indicate that our watermark key’s size is relatively the same as its watermark data while preserving the requirement of watermarking properties. Moreover, the system has maximum imperceptibility and is relatively robust against echo addition, band-pass filtering and re-sampling.

Note that the main purpose of computer forensics is the proper identification and collection of computer evidence. However, all the image forensics’ schemes developed so far have not provided verifiable information on the source of tampering. Thus, the second challenge issue addressed in Chapter 4 is on how to construct a verification scheme to identify the source of tampering. Our preliminary work on passive approach is to study on a common form of manipulation. That is combining parts of the image fragment into another different image to remove objects from the image. Inspired by the digital image correlation concept, we exploit the peak of cross-correlation function to automatically detect the splicing artifacts in any fragment of an image. Experimental results from synthesized splicing experiments state that the scheme can detect most splicing artifacts, with relatively few false positives. However, we observe that high value of peak of correlation coefficient does not guarantee it belongs to a spliced region. Low value of peak of correlation might belong to a spliced region. How to increase detection accuracy becomes the third challenge issue. We then improve our previous work by exploiting pixel-based alignment method adopted from image registration concept. We formulate a tampered image problem as locating the best correlation between the extracted sub-region(s) and their references. The results demonstrate the effectiveness over synthesized images and downloaded images from the web.

To end with, we consider that the image might have occasionally undergone some geometric transformations, such as rotation and scaling. Then, the fourth challenge issue addressed in Chapter 5 is on how to identify the geometric distortions. We exploit distinctive feature descriptor in detecting suspicious regions as well as invariant or sensitive triple feature construction to identify geometric parameters. In our previous work, the spliced artifact identification relies on edge detection technique. Due to this condition, the images which do not introduce any edges are hard to be detected, or might cause fault extraction. We then proposed clustering techniques to identify the tampered region based on distinctive keypoints. We draw the comparison to the existing scheme and it confirms that we obtain a considerable gain both in terms of rotational and scaling accuracy.