Block-based Reversible Fragile Watermarking for 2D Vector Map Authentication

Nana Wang, School of Computer Science and Technology, Jiangsu Normal University, Xuzhou, China

Xiangjun Zhao, School of Computer Science and Technology, Jiangsu Normal University, Xuzhou, China

Han Zhang, Computer and Information Engineering Department, Heze University, Heze, China

ABSTRACT

In this paper, the authors propose a block-based reversible watermarking method for 2D vector map authentication. In the scheme, they divide the features of a vector map into different categories of blocks, calculate an authentication watermark for each block, and embed the watermarks of different blocks using a reversible watermarking method based on virtual coordinates and a fragile watermarking algorithm based on concentric circles. While the block division ensures superior accuracy of tamper localization, the two watermarking methods provide recovery of the original content. Experimental results show that the proposed scheme has good invisibility, reversibility and computational complexity, and can accurately locate malicious attacks such as vertex modification/addition/deletion and feature modification/addition/deletion.

Keywords: 2D Vector Map, Authentication, Concentric Circles, Reversible Watermarking, Tamper Localization

INTRODUCTION

These days, 2D vector maps, the fundamental data of geographical information systems (GISs), have been widely applied in military, civil cartography, urban planning, forestry, etc. These vector geo-spatial data can be easily replicated, manipulated and distributed using powerful available tools and equipment. However, the ease and extent of such manipulations emphasize the need for 2D vector map authentication techniques in applications where verification of integrity and authenticity of the 2D vector map content is essential. The high cost of acquiring these data (Lee & Kwon, 2013; López, 2002; Niu, Shao, & Wang, 2006; Wang et al., 2010; Yan, Li, & Wen, 2011) further underscores this need.
2D vector map integrity and authenticity can be guaranteed through the use of fragile watermarking techniques. Compared with the traditional solution, i.e., digital signatures, fragile watermarking techniques can not only detect but also locate any modification made to the original content. This is especially useful for saving time for retransmission when the rest of the vector map can still be trusted after some tampered data are detected and located.

In most cases of fragile watermarking, the original content are distorted in an irreversible way. However, due to the required high-precision nature of vector maps, modifications to maps are generally undesired. Therefore, reversible fragile watermarking schemes (Shao, Wang, & Xu, 2005; Wang & Men, 2012; Wang & Men, 2013; Zheng, Li, Feng, & Liu, 2010; Zheng & You, 2009), which allow the decoder to recover the original content upon extraction of the embedded authentication watermark, are more appropriate for vector maps.

Currently, research on watermarking for 2D vector maps is mainly focused on robust watermarking algorithms (Doncel, Nikolaidis, & Pitas, 2007; Gou & Wu, 2005; Horness, Nikolaidis, & Pitas, 2007; Jiang, Zhu, Huang, & Ma, 2013; Lafaye, Béguec, Gross-Amblard, & Ruas, 2012; Lee & Kwon, 2013; Ohbuchi, Ueda, & Endoh, 2002; Wang et al., 2010; Yan et al., 2011) for copyright protection or reversible watermarking schemes (Cao, Men, & Ji, 2014; Voigt, Yang, & Busch, 2004; Wang, Zhang, & Men, 2014; Wang, Shao, Xu, & Niu, 2007) for content recovery. Only a few fragile watermarking methods for 2D vector map authentication (Shao et al., 2005; Wang & Men, 2012; Wang & Men 2013; Zheng et al., 2010; Zheng & You, 2009) have been proposed. Shao et al. (2005) divided the vertices into non-intersecting groups and embedded the watermark group by group using Fridrich, Goljan, and Du’s (2001) reversible watermarking algorithm. A drawback of this algorithm is that the tamper localization ability will be ruined if some vertices or features have been added or deleted. Zheng and You (2009) separated the vertices of a 2D vector map into several blocks according to a predefined threshold and embedded the watermark block by block. Because the watermark embedding procedure may shift some vertices from one block to the neighboring blocks, correct watermark extraction may be impossible, especially when the parameters are not properly selected. Another scheme was presented by Zheng et al. (2010), in which the features are divided into different groups and the watermarks are embedded group by group independently. Since the features are traversed according the record number, a feature reordering operation or a feature addition/deletion attack may totally disable the tamper localization capability. To locate malicious attacks accurately and recover the original content, Wang and Men (2012) proposed a reversible fragile watermarking algorithm based on feature marking. The features are divided into groups according to their unique record numbers and the watermarks are embedded using Wang et al.’s (2007) reversible watermarking technique. For achieving good tamper localization performance, a marking method based on vertex insertion is applied to each feature. This scheme can locate tampered features precisely. However, it cannot locate tampered regions. By combining an improved version of Wang and Wang’s (2007) reversible data hiding algorithm and a fragile watermarking method based on vertex insertion, Wang and Men (2013) presented a reversible fragile watermarking scheme for locating tampered blocks in 2D vector maps. But because of the coordinate sorting process during watermark embedding and watermark extraction, its computational complexity is not very low.

To further decrease the computational complexity, in this paper, we propose a block-based reversible fragile watermarking scheme for 2D vector map authentication by exploiting Wang et al.’s (2014) reversible watermarking method and a fragile watermarking algorithm based on concentric circles. In the proposed approach, the features of the vector map are first divided into blocks, each of which contains the same area. According to a predefined threshold, all the blocks are further divided into two categories: normal and complex. After generating an authentication watermark for each block, a normal block embeds the watermark using Wang et al.’s reversible
Related Content

Do Privacy Statements Really Work?: The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce
www.igi-global.com/chapter/privacy-statements-really-work/60975?camid=4v1a

Current Network Security Technology
www.igi-global.com/chapter/current-network-security-technology/60962?camid=4v1a
An Overview on Passive Image Forensics Technology for Automatic Computer Forgery
www.igi-global.com/article/an-overview-on-passive-image-forensics-technology-for-automatic-computer-forgery/163346?camid=4v1a

Telephone Handset Identification by Collaborative Representations
www.igi-global.com/article/telephone-handset-identification-by-collaborative-representations/103934?camid=4v1a