Digital Signal Processing 25 (2014) 224–243

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Perceptual encryption with compression for secure vector map data processing

Bong-Joo Jang [a], Suk-Hwan Lee [b,*], Ki-Ryong Kwon [c,*]

[a] Water Resource Research Division, Korea Institute of Construction Technology, Republic of Korea
[b] Department of Information Security, Tongmyong University, Republic of Korea
[c] Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea

ARTICLE INFO

Article history:
Available online 15 October 2013

Keywords:
Vector map data
Vector compression
Perceptual encryption
Copy detection
Access control

ABSTRACT

With the rapidly rising interest in geographic information system (GIS) contents, a large volume of valuable map data has been unlawfully distributed by pirates. Therefore, the secure storage and transmission of classified national digital map datasets have been increasingly threatened. As the importance of secure, large-volume map datasets has increased, vector map security techniques that focus on secure network and data encryption have been studied. These techniques are required to ensure access control and prevent illegal copying of digital maps. This paper presents perceptual encryption on the vector compression domain for copy protection and access control of vector maps. Our algorithm compresses all vector data of polylines and polygons by lossless minimum coding object (MCO) units and perceptually encrypts using two processes using the mean points and directions of MCOs. The first process changes the position of vector data by randomly permuting the mean points of MCOs, the so-called position encryption. The second process changes the geographic shape by circularly encrypting the directions of vertices in MCOs by the XOR operator. Experimental results have verified that our algorithm can encrypt GIS digital maps effectively and simply and can also improve the compression ratio, unlike general data encryption techniques, and thus, our algorithm is very effective for a large volume of GIS datasets.

1. Introduction

A geographic information system (GIS) is designed to capture, store, manipulate, analyze, and manage all kinds of geographic information. As such, GIS is the emerging system for cartography, statistical analysis, and database technology [1–3]. Many countries have greatly spread the application of geographic information in both the public and the private sector by constructing a GIS frame and network at a national level. In recent mobile applications such as navigation, smart phone, and Wi-Fi, GIS has rapidly grown into a new paradigm of Where 2.0 with Web GIS through Internet mapping, mobile mash-up services, and social communities. The data structure of the geographical dataset, as shown in Fig. 1, consists of spatial data fields and object data fields. The spatial data are classified as vector data and raster data. The former can be displayed as vector graphics, which uses geometrical primitives such as points, lines, curves, and shapes or polygons, whereas raster data appear as an image. Geographical features are often expressed as vectors by considering those features as geometrical shapes.

The security of a geographical dataset encrypts map data or controls user access to prevent damage to or theft of the dataset, which can happen in the integration process with a number of datasets of geographical information. Cases in which second- or third-party consumers illegally distribute datasets established by private or national institutes have been frequently reported. Some countries have invested significant amounts of their budgets to the development and construction of security solutions as a part of an integrated construction project of national geographic information to link systems of institutes.

Looking into recent techniques for geographical dataset security, network security techniques for secure transmission of map data have been researched extensively [4–8]. Researchers have worked on the cryptography-based data encryption of database files or data profiles [9–11] and on the watermarking and hashing of vector maps or raster maps for copyright protection [12–20]. Conventional approaches to dataset security that are based on authentication and watermarking have some limitations. These limitations are as follows. First, the cryptography of data files and profiles increases complexity because of complex encryption algorithms. Some objects that illustrate contour lines in map expression fields, such as houses, roads, and main sewers, can be frequently activated or nonactivated, and the switching of map

* Corresponding authors at: Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea. Fax: +82 51 629 6230.
E-mail addresses: skylee@tu.ac.kr (S.-H. Lee), krkwon@pknu.ac.kr (K.-R. Kwon).

1051-2004/$ – see front matter
http://dx.doi.org/10.1016/j.dsp.2013.09.013

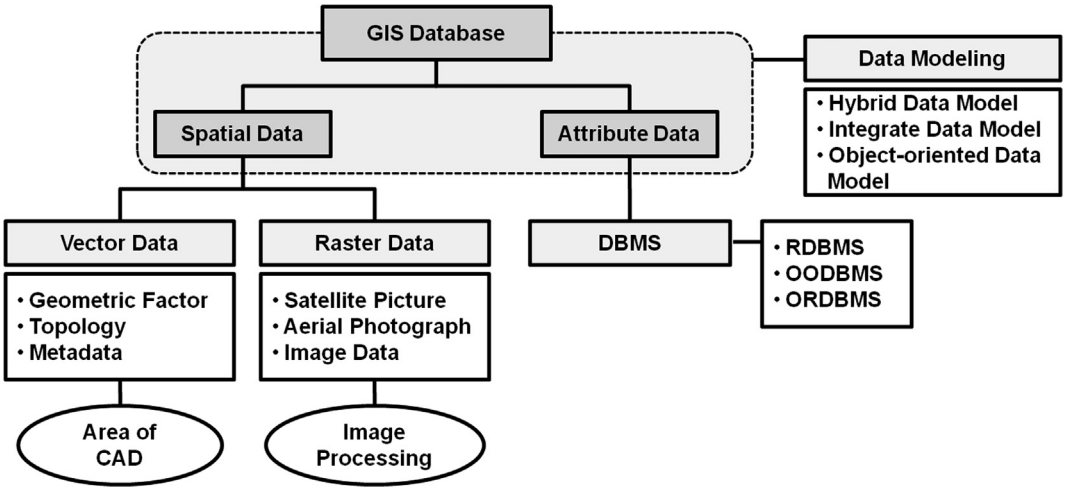

Fig. 1. General data structure of a GIS database.

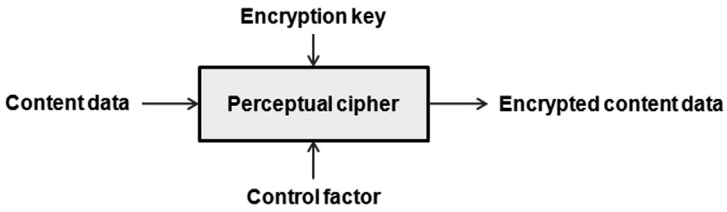

Fig. 2. Concept of perceptual encryption.

expression can occur on the basis of various event types. Thus, because the encryption and decryption of a dataset must always be performed when cases such as the above occur, the flexibility of such a system is very low. In particular, database management systems (DBMSs) based on security techniques [10] are vulnerable to the conversion of data format. Therefore, the security technique must preserve the security of the dataset in various formats. Second, the network security technique cannot preserve security in the case of data leakage in offline or loophole exposure of network administration. Third, the conventional works cannot perform the indexing when layers or objects in an encrypted map are detected and displayed. This indexing is very useful in GIS. Finally, map watermarking, which is the post-processing of security, determines whether pirated map data are illegally copied. In short, it is difficult to create a basic solution for map dataset security.

To compensate for limitations in the conventional approaches described above, we present the perceptual encryption of layer units on vector compression to protect against illegal copying and distribution and to control access of a large volume of map datasets. Our algorithm perceptually encrypts a vector map by using position and direction parameters in vector compression domains that imply lossless hierarchical compression. The main advantages of our algorithm are the high efficiency of perceptual encryption using low-complexity indexing for special or only desired objects in the encrypted map without a decryption process for the total map, as well as the improvement of the compression ratio for a large volume of map datasets.

The remainder of this paper is organized as follows. In Section 2, we describe map security techniques and related works regarding map datasets. In Section 3, we explain the proposed perceptual encryption in detail. In Section 4, we discuss the experimental results, and we conclude the paper in Section 5.

2. Vector map security and compression

A vector map consists of a number of data layers that contain geographical features of roads, railroads, rivers, buildings, and so on, as well as spatial and nonspatial data. Each layer contains object sets of points, lines or polylines, polygons, and characters. Geometric types of points, lines or polylines, and polygons are represented by one or more vertices. In addition, vector maps can be stored and distributed using various formats according to the production environments [21–24]. Despite the various formats, all geometric data contain consecutive vertices of floating points on a 2D plane, and any layer in a map can be generated by a geometric dataset. Most geographical features can be represented by polylines and polygons.

Watermarking and encryption techniques have been studied by many researchers to address the security of the content of the many kinds of vector map data. Vector map watermarking has been extensively researched as a solution for the protection of spatial data since the early 2000s [12–20]. However, because the purpose of vector map watermarking is to verify whether a pirated map has been copied, this seems to be the end step of this security strategy. Therefore, vector map watermarking is not a suitable method for ensuring secure transmission and storage of a map.

Perceptual encryption of multimedia contents degrades the quality of the content according to the security or quality requirements for previewing the secure media content [25]. Fig. 2 shows the concept of perceptual encryption. The control factor handles the quality degradation corresponding to the encryption strength. In general, perceptual encryption is realized by partial encryption algorithms with a format-compliant feature. The focus of most perceptual encryption algorithms has been on images and video in a compressed domain [26–30]. These various perceptual encryption techniques for multimedia were investigated, and it has been found that perceptual encryption techniques for GIS as the vector data, which is an important multimedia tool, have been inadequate