PROTECTION OF GEOSPATIAL DATA: PRESENT APPROACHES AND RESEARCH NEEDS

SangitaZope – Chaudhari[a*] and P. Venkatachalam[b]
[a]Research Scholar, Centre of Studies in Resource Engineering, Indian Institute of Technology Bombay, India, +91-9324204088, sangita.z@iitb.ac.in
[b]Professor, Centre of Studies in Resource Engineering, Indian Institute of Technology Bombay, India, +91-022-5767665 pvenk@csre.iitb.ac.in

KEYWORDS: Geospatial Data, Security, Privacy, Outsourcing, Watermarking

Abstract: Due to rapid growth of distributed network and Internet, it becomes easy for data providers and users to access, manage, and share voluminous geospatial data in digital form. Even though a consistent and reliable means are available for storing, managing and sharing geospatial data, very little attention has been given towards security, access control, and privacy policies. With Internet, it becomes very easy to distribute and copy geospatial data. Therefore, it becomes necessary to protect geospatial data from illegal and unauthorized usage. Security mechanism should be enforced at geospatial data storage, dissemination, and at data retrieval to protect geospatial data from illicit users. In this paper, we define unique security requirements for protection of geospatial data and give an overview on current approaches being used for secure distribution and management of spatial data at storage and dissemination with their limitations and the research challenges.

INTRODUCTION

Geographical Information System (GIS) has been used in commercial and military applications for many years. The main component of GIS is the data. The GIS data has two important properties. First, the effort it takes to put it in a form suitable for use in the GIS applications. This effort increases its cost. Second, in most cases the GIS data may contain confidential information which must be kept away from unauthorized users. For example, GIS layers may include military locations and information like movements and hiding places in a tactical environment. Hence, it is very important to protect the GIS data from two threats. First, since the GIS data is too expensive, we have to prevent illegal duplication and distribution of it. Today, it is too easy to buy some GIS layers, make copies from them and distribute or sell them many times without taking any permission from the original GIS data provider. Second, since as GIS data may have sensitive information, it should not be accessed by unauthorized users. Security for spatial data can be provided at various levels. The first level of security is to provide at database level. If the entire geo-spatial data would be made available by simple collection and integration of data from different repositories, it may possible that data is misused and some privacy violations may occur. As many users are accessing same repository, security measure must be adopted so that users and applications can access data on need-to-know basis only. Access control policies should be enforced to deal with such case.

The second level of security is to provide at distribution/dissemination level. Geographic database contains huge amount of data which need to be distributed to authorized or subscribed customers. One of the approaches is to outsource the data to some authorized service provider who in turn makes it available for authorized customers. The data may be outsourced in encrypted or transformed form. Each of the authorized users uses decryption key provided to them by data owner to decode the data. The second approach is to use digital watermarking for securing both raster as well as vector geospatial data. Digital watermarking is one of the efficient and effective methods to identify legitimate owners and users of spatial data. One can easily trace and prove the unauthorized distribution and reproduction of watermarked data. This paper gives an overview of the methods being proposed by GIS research community for providing security at database level, secure outsourcing of spatial data, and protection at distribution of this data.

SPATIAL DATABASE SECURITY

GIS is widely used in many applications which require multiuser environment, sophisticated database management and robust access control mechanism. As this spatial data must be protected from unauthorized

access in computer and communication systems, it is very crucial and important that only authorized people will have access to database. Database security can be achieved using access control, authentication, auditing, and administration. In database systems it is assumed that authentication of the user has been successfully verified prior to the enforcement of access control policies. (Sandhu and Samarati, 1994)

Atluri and Chun (2007) have developed an authorization system named as Geospatial Authorization System (GSAS). This system uses Geospatial Authorization Model (GSAM) proposed by Atluri and Chun (2004). GSAS allows specifying and enforcing access control policies on large-scale geospatial data based on spatial, temporal and resolution attributes associated with the data objects and the credentials associated with users. GSAS is capable of providing security policies with varying degrees of granularities, from coarse to fine-grained. It supports novel privilege modes like viewing, copying and maintenance related to image manipulations. It also includes view, zoom-in, overlay, view thumbnail, view-annotation, identify animate and fly-by as a privilege.

Traditionally GIS uses block based storage model for storing spatial data. Today in the distributed environment, GIS spatial data is stored based on Object Based Storage (OBS) which gives an integrated solution to both high performance storage services and also data sharing. GIS server, metadata server and storage device are separated and spatial data is organized as a spatial object saved in Object-based Storage Device (OSD). This scheme provides authenticity as well as confidentiality of spatial data (Yanqun and Qianping, 2008). The concept, design and development of a multilevel secure spatial relational data model (MLS/SDM) have been designed and the mandatory security issues in the context of a spatial database system are addressed by Oh and Bae (2004) using spatial class constraints and spatial topological constraints. Access control is designed for various granularity levels like spatial view, spatial layer, spatial tile, and spatial object. Separate spatial class constraints are designed for point, line, and region class. Spatial topology constraints are designed by considering different topological relations like disjoint, equals, covers, covered by, contains, contained by, overlap, union, intersect.

Zeng et al. (2007) adopted certificate-based authentication instead of traditional password authentication in their proposed framework. It is very secure and clients need not require saving their passwords. To guarantee clients authenticity, they introduced Public Key Infrastructure (PKI), which is based on certificates. Along with Role based Access Control (RBAC), role control table is also specified at server side. Whenever user wants to access spatial database, user certificate and roles are transmitted and checked against control table for authorization. Every entity is verified by Registration Authority (RA) and registers his certificate from Certificate Authority Service (CAS). Security Socket layer (SSL) protocol is used during identity authentication and data transmission.

Belussi et al (2004) developed Topological Spatial Data Model (TSDM) model which is a modified version of Layered Spatial Data Model (LSDM). Authorization is specified against map objects at fine granularity level. It also considers spatial representation types and object dimension. Instance, insertion, and schema privileges are assigned on instance of objects and operations executed on them. An access control policy for geographical maps uses object dimension and type of spatial information to support both positive and negative authorization. It grants authorization according to the objects hierarchy and authorizations propagation. Gan (2003) described the access of spatial data through Spatial Data Engine (SDE). SDE manages unstructured spatial data in structured Relational Database Management System (RDBMS). It is an ideal place to make access decisions on spatial data stored in database with respect to spatial semantics. The implementation of SDE-based authorization is very complex and overhead. Also, current SDE does not support access control. One needs to change the source code of SDE to achieve access control.

In addition to above mentioned access control methods; a view based mechanism can also be used to provide access control. Views can be created from the same base table in spatial database according to different security requirements and restrictions. Once the user is authenticated, he gains database account's privileges to the specified view. There is no need to alter the schemas of base tables or add extra tables to store authorization information. This mechanism has the problem of concurrent control. Also, the offensive usage of views can result in redundancy and unnecessary overhead of the access control mechanism, and information leakage through exceptions and errors caused by user-defined functions (Liang, 2005).

Gabillon and Capolsini (2010) used Organization Based Access Control (Or-BAC) model which considers proposed dynamic security rules based on some spatial context to provide access control. Spatial context considered are position of user, zoomed area of interest of user, direction of moving object etc. Compared to other access control models, Or-BAC provides good security as it implements dynamic security rule using

spatial context of object and subject. Bertino et al. (2006) have presented a spatially aware role based access control (GEO-RBAC) which is extension of RBAC. Spatial entities are used to model objects, subject (user) position, and geographically bounded roles. Roles are specified based on position of the user. It deals with both real (physical) and logical position (granularity). The proposed model is divided in 3 components: Core GEO-RBAC which deals with spatial role, role schema, real/logical position, activated/enabled role to be used in subsequent component. Hierarchical GEO-RBAC provides hierarchy of roles schema and roles and are used for both activated and enabled roles. Constrained GEO-RBAC specifies constraints that are helpful in deciding access control policies, different granularities (schema/instance level), dimension (spatial/non spatial), and different verification time (static/dynamic). This model can be extended to support interoperation strategy based multi- domain GEO-RBAC.

DIGITAL WATERMARKING FOR VECTOR DATA

In the field of GIS, most of the research work is focused on digital watermarking for copyright protection which helps for secure distribution of geospatial data. This section provides an overview on vector data watermarking algorithms under spatial and transform domain category.

A. Spatial Domain Algorithm

Vector data can be modeled using features like points, polylines, and polygons. Topological relationship is used to show association between these features. Spatial domain based vector data watermarking approaches use these features and topological relations to embed watermark in vector data. In case of spatial domain, simple watermarks can be embedded in the vector data by modifying the coordinate values or the Least Significant Bit (LSB) values.

Area subdivision methods like Uniform, Quadtree, and Modified quadtree can be used in watermarking process. Modified quadtree method is used by Obhuchi et al. (2002) for experimentation as it gives greater number of vertices for embedding watermark. Vector map is divided into rectangular grid based on the vertex density. If number of vertices is more, algorithm results in good noise resiliency. However, it results in fewer rectangles and hence low chip rate (number of times same watermark is inserted) and affects robustness of the algorithm. Watermark is embedded by displacing group of vertices in rectangular grids. Same Watermark is inserted multiple times in various grids. To extract the watermark, watermarked map is divided in the same way as embedding the watermark, and then the coordinates of the vertices are compared with original map vertices (non-blind watermarking) to extract watermark information. This algorithm provides good resiliency against additive random noise, transformation, vertex insertion/removal, object order scrambling, and cropping attacks. Wang et al. (2009) have adopted a modified quad tree algorithm to divide vector map into different areas. Information of all the points is converted to x and y direction component of the vector set. A key is used to indicate direction of the vector. Then the components are divided into even and odd intervals. Finally, watermark is embedded into x-y components depending on value of watermarking bits. If intervals are large, this scheme produces greater distortion and less robust to noise attacks. To maximize capacity of watermark, adjacent areas can be merged. This scheme provides less accuracy. Even though the robustness is satisfactory for map simplification, interpolation, disarrangement of vertices, geometric transformation, and noise attack, it does not affect extraction of watermark.

In vector map, there is high correlation among the neighbouring vertices of same feature. Polyline feature is used for embedding watermark by Cao et al. (2010). Highly correlated vertices of polyline are grouped together and their median is calculated. Watermark bits are embedded in that median value of each group iteratively. This scheme produces less distortion due to high correlation between the vertices. A blind watermarking scheme reported by Huo et al. (2010) has used polyline/polygon characteristics of map. Length/perimeter is calculated for all polyline/polygon in a map. Considering uniform step (key) of length/perimeter dynamic range, polylines/polygons are arranged in some groups. Watermark is inserted multiple times. Dynamic range of length/perimeter and key used to divide them into groups are required to extract watermark from watermarked data. This scheme is robust against attacks like geometric transformation, object order scrambling, swapping, vertex addition/deletion, and cropping.

In another blind watermarking algorithm, an interior angle is calculated using 3 consecutive points of the object. User specified random table and user id are used as watermarking keys. Watermark is generated using changes interior angle value by random table and user id. Watermark is embedded in to last 2 digits of interior angle.

This method suffers from a weakness that if interior angles are changed, watermark cannot be extracted. It provides good robustness against geometric transformation, noise addition, and vertex addition operations (Kim, 2010). A lossless watermarking algorithm depicted by Men et al. (2010) is based on the global characteristics of vector map. Vertices are categorized as feature points representing polyline basic shape and non-feature points representing polyline details using Douglas-Peucker algorithm. Back propagation neural network is used to determine watermarking parameter. This method fairly deals with simplification and compression attacks. Singular value decomposition is utilized to calculate watermarking parameter for non-feature points. This method is robust against geometric attacks. At detection, the detection keys are obtained through the exclusive OR (XOR) operation between lossless watermarking parameters and copyright image.

B. Transform Domain Algorithm

Similar to images, vector data can be also represented/stored in spatial domain as well as in transform domain. To transfer vector data to its frequency representation, we can use several reversible transforms like DCT, DWT, and DFT. Watermarks can be embedded by modifying transform domain coefficients of coordinates. We start from DFT. There are few algorithms that modify DFT magnitude and phase coefficients to embed watermarks. In the blind watermarking scheme proposed by Tao et al. (2009), phase of DFT is quantized using step size and then watermark is embedded in quantized phase. Step size affects visibility of map data as well as robustness. This method fairly deals with attacks like similarity transformation, Geometric transformation, and format conversion.

DCT based reversible and blind watermarking scheme is proposed by Voigt et al. (2004). It makes use of high correlation property of vertex coordinates from the same feature. A watermark bit is embedded in group of eight point DCT coefficients vertices. This algorithm cannot resist map simplification and interpolation and produces map distortion too. Wang et al. (2011) have adopted the same scheme proposed in by Voigt et al. (2004). They used threshold based error estimation method to control watermarked data distortion. Watermark can be fully recovered under operations like translation, scaling, vertex insertion/deletion, noise addition, distortion, cropping, and object scrambling. Still the algorithm lacks in providing higher capacity, and robustness against rotation attacks.

Li and Xu (2003) have developed wavelet based blind watermarking scheme for vector map protection. Magnitude and phase are calculated from detail coefficients at particular decomposition level and character sequence is generated from magnitude. Watermark bits are embedded into character sequence. The robustness of this algorithm is good enough to deal with attacks like geometric transformation, noise addition. In a non-blind algorithm depicted by Zhu et al. (2008), watermark bits are embedded in low frequency coefficients by applying integer wavelet transform on vector data. This algorithm can effectively resist the attacks like noise, data compression, point deletion and format exchange. Zhang et al. (2010) have proposed an approach which uses Douglas Peucker algorithm to classify vertices as feature and non-feature points. It uses Haar wavelet coefficients of feature points to embed the watermark. Feature points are calculated for each sub region generated by area subdivision process. This method is robust against geometric transformation, addition, deletion, and cropping of points. Also, map distortion is well controlled. This algorithm does not provide good robustness against irregular cropping.

DIGITAL WATERMARKING FOR RASTER DATA

Raster data mostly includes satellite images, digital elevation models, and aerial photos. Lots of research has been done on image watermarking for copyright protection, but very few methods are developed for watermarking of remotely sensed images. Some of the methods proposed for image watermarking can also be applied to remotely sensed images if they fulfil requirements of satellite image watermarking. Here, methods available for watermarking remote sensing images are reviewed.

A. Spatial Domain Algorithm

Chauhan et al. (2000) have proposed a blind watermarking algorithm for copyrighting of satellite images. Watermark is inserted without disturbing vital areas of one's interest. Pixel values are quantized to 0 or 1 depending on Look up Table (LUT). Watermark is embedded in pixels of original image using a mapping in the LUT. To find corresponding position for embedding watermark bit, a prime constant is used. In extraction process, watermark key which is a combination of LUT and prime constant is used. As satellite image is larger, it is possible to embed multiple watermarks into it. Also lookup table can be extended to deal with tri or multicolour watermark using ternary or n-ary sequence instead of 0's and 1's in LUT. Watermark is successfully extracted and it gives good imperceptibility. In this approach no evaluation is done against attack models. A watermarking tool "StegMark" was originally developed for robust and fragile multimedia image watermarking. Robustness is evaluated using cropping, rotation, and compression. "StegMark Geo" is an invisible watermarking solution designed for copyright protection of large-scale, high resolution satellite images. It provides robustness against cropping, resizing, and compression attack (Ho, 2001).

An algorithm proposed by Lu et al. (2005) is based on multistage Vector Quantization (VQ) that embeds both robust watermark for copyright protection or ownership verification and fragile watermark for content authentication or integrity attestation. In the proposed method, the semi-fragile watermark is embedded using index constrained VQ the robust watermark is embedded in the first stage of VQ. Both of the watermarks can be extracted without the original image. The proposed method is robust against JPEG compression, blurring, image enhancement, cropping attacks. Tree structured vector Quantizer based semi fragile watermarking approach is presented by Ruiz and Megias (2011). Watermark bits are embedded by extracting least significant bits of pixels from all bands of multi- and hyper spectral data. This scheme is robust against compression as well as copy and replaces attack.

B. Transform Domain Algorithm

Barni et al. (2002) proposed near-lossless watermarking for copyright protection of remote sensing images. They have used watermarking algorithms using DFT and DWT for still images proposed by Barni et al. (2001). The proposed solution rephrases the near lossless concept by forcing a maximum absolute difference between the original and watermarked image. Error metric can be used to measure spectral distance and defined as:

$$D_c^{m,n} = \max_i \left| x_i^{m,n} - \hat{x}_i^{m,n} \right| \quad (1)$$

Where, x is original image, $\hat{x}$ is watermarked image, (m, n) are spatial coordinates of each pixel and i is its spectral value. In near lossless watermarking, spectral distance between original and watermarked image is minimized causing less quality degradation. This method is evaluated to measure the impact of cropping attack and classification. It is shown experimentally that robustness is less affected by cropping attack. Robustness is good in DWT based scheme than DFT. Classification results for DWT are better than DFT and overall classification results for both DWT and DFT using near lossless watermarking are far better than other conventional watermarking techniques.

Hemalatha et al. (2009) proposed a semi-blind watermarking scheme for remote sensing images. This scheme retains special and spectral information of image. It uses wavelet transform domain to embed watermark. Singular Valued Decomposition (SVD) is applied on any component of wavelet decomposition (A, H, V, or D). SVD matrices are required for extraction of watermark. Stirmark benchmark is used to check robustness of proposed algorithm. Also the attacks like filtering, deletion of attributes, and editing of data are applied using GIS package. This algorithms works well in comparison of other wavelet based algorithms for multimedia image watermarking. In remote sensing environment, analytic integrity is more important than perceptual quality of the data. A scheme using 3- level DWT decomposition is depicted by Ziegeler et al. (2003). Here, only one sub band at each level having maximum root means square value is selected to embed watermark. This scheme is robust against cropping attack. Also classification result is good as compared to other wavelet based schemes. This scheme can be applied to multispectral as well as hyper spectral data.
Ram kumar et al. (1999) also presented a data hiding scheme based on DFT, where they modified the magnitude component of the DFT coefficients. Their simulations suggest that magnitude DFT survives practical

compression which can be attributed to the fact that most practical compression schemes try to maximize the PSNR. Hence using magnitude DFT is a way to exploit the gap in most practical compression schemes. The proposed scheme is shown to be resistant to JPEG and SPIHT compression. A dual domain watermarking technique is proposed for image authentication and image compression (Zhao et al., 2004). DCT domain is used for watermark generation and DWT domain is used for watermark insertion. A soft authentication watermark is used for tamper detection and authentication while a chrominance watermark is added to enhance compression. They use the orthogonality of DCT-DWT domain for watermarking.

OUTSOURCING

There are various techniques available for secure outsourcing of the data. When data is stored and processed out of the territory of its owner, security becomes the first concern. Confidentiality of the outsourced data, correctness assurance of query results, and preserving user's access privacy are the primary requirements of secure data outsourcing. Today, most GIS data providers have a problem of protecting their data from being copied and accessed by unauthorized users.

One of the well-known transformation techniques is simple affine transformation where data owner performs the scaling, rotation, shearing and translation to change actual dataset for outsourcing. This approach is simple but vulnerable to attacks. Yiu et al. (2009) used a transformation which includes Hierarchical Space Division (HSD) In HSD, actual dataset is divided into the Hierarchical Space using kD-tree partitioning and then different transformations are performed on the local regions. Transformation key is shared with trusted users only and service provider can only evaluate the query without seeing actual data. Common attack model is devised to check security. HSD results into secure and an efficient method. Khoshgozaran and Shahabi (2007) utilized space filling curves as one-way transformations to encode the locations of both users and points of interest into an encrypted space and to evaluate a query in this transformed space. The transformed space maintains the distance properties of the original space which enables efficient evaluation of location queries in the transformed space. Subsequently, upon receiving transformed query results, users can reverse the transformation efficiently using the trapdoor information which is only provided to them and is protected from the server. This transformation scheme provides very efficient query processing without compromising privacy. But the result for Location Based Services (LBS) such as nearest neighbour query is approximate.

Yiu et al. (2010) described a transformation approach which protects data privacy but not the user location. There are two types of attacks known as general and tailored attack. In general attack, intruder tries to find the estimation of the original data with brute force techniques but in case of tailored attack, the intruder uses some background knowledge about the data being analysed and tries to estimates data accordingly. If the attacker obtains some background knowledge of mappings between original dataset and transformed dataset, the attacker applies some attack method to estimate the original locations of the objects as the estimated dataset. If the distortionbetween the original dataset and estimated is low, then the method is vulnerable to attacks.

Cryptographic based approaches secure the data by using the power of existing cryptographic techniques available. In Cryptographic Transformation (CRT) the entire dataset is encrypted and then indexed in a B+ tree like structure. Whenever user runs a query, the first node (root) is returned and is decrypted at the user site and then for the next node where the next pointer points to. It goes on recursively until it reaches the leaf node which contains the actual data. Although CRT method results in extra overhead as intermediate node has to be also transferred, it becomes reasonable for large datasets. (Yiu et al., 2009)

Private Information Retrieval (PIR) approaches construct private spatial indexes on top of PIR operations to provide efficient spatial query processing, while the underlying PIR scheme guarantees privacy. There are two location privacy schemes based on hardware-based and computational PIR protocols. The first approach superimposes a regular grid on the data and uses PIR to privately evaluate range and K-Nearest Neighbour (KNN) queries (Khoshgozaran and Shahabi, 2007). The second technique supports approximate and exact nearest neighbour query evaluation by utilizing various 1-D and 2-D partitioning to index the data and then restructuring partitions into a matrix that can be privately queried using PIR (Ghinita et al., 2008). Hengartner (2007) proposed an architecture that uses PIR and trusted computing to hide location information from an un-trusted server. With this approach, PIR is used to prevent the un-trusted location server from learning user locations and trusted computing is used to ensure users that PIR algorithm and other services provided by the server are only performing the operations as intended. In fact, similar to hardware-based PIR, it places a trusted module as close as possible to the un-trusted host to disguise the selection of records. However, the techniques

do not specifically focus on spatial query processing (such as range and KNN) and architecture is not implemented. The PIR protocols are still expensive and require a significant amount of server resources. All database records still have to be processed at the server. Sion (2007) suggests that the cost of privately retrieving database items from the server is significantly higher than sending the entire database to the client. The proposed PIR approaches do not suffer from the privacy vulnerabilities of cloaking, anonymization, and transformation based approaches or the prohibitive communication and computation costs of cryptographic-based techniques.

In another class of approaches like authentic publication, the data owner employs one or more un-trusted data publishers. The data owner employs digests that are bottom-up hashes computed recursively over tree-type structures representing the entire set of objects in the owner's database. These digests are distributed to all clients interested in the owner's data (Gertz et al., 2004). This is done in a secured fashion by using, for example, signing keys. This does not allow the interactive querying. Also the size of the verification object returned may not be linear. The user can verify the returned data with the help of verification object. Similar approach is used to publish relational data over internet by Devanbu et al. (2003). Yang et al. (2008) have opted same approach with little modification for outsourcing of spatial data on location based services. They used combination of MHT and R*-tree. Li et al. (2006) have demonstrated usage of dynamic authenticated index structures on outsourcing. They have compared performance of MHT and extended MHT in terms of fan-out, storage cost, tree construction cost, verification object construction cost, and authentication cost.

RRSEARCH NEEDS

GIS is concerned with spatial data collection, analysis, and their use. These inputs are gathered primarily from topographic/thematic maps, global positioning system (GPS)/ ground based observations, aerial and satellite sensors. Such a digital spatial data generation involves complex and expensive efforts. Also, the dissemination over the network is a complex and massive task in scale and dimension. Many national and international agencies are primarily focusing on coordinated development, use, sharing, and dissemination of geospatial data among wide range of government agencies and offices. While consistent and reliable means to manage, share, and access geospatial data are available, very little attention has been given to address security concerns, such as access control, security, and privacy policies. Use of security mechanism posed at various levels namely geospatial data storage, dissemination, and retrieval of geospatial data from trusted third party could play a significant role in geospatial data environment.

While dealing with geospatial data at dissemination level, geospatial data needs to be protected; otherwise it could result in illegal copy and distribution. Use of digital watermarking for copyright protection of geospatial data is the best solution available to deal with this situation. Geospatial data is modelled by raster and vector models and both of these models have different characteristics. Watermarking algorithm proposed for both are different. Therefore, there is need to evolve methodologies which will be applied to both of these models in an integrated manner. As seen in literature, there are various algorithms available for watermarking using spatial and frequency domain. Each domain has certain limitations. Although spatial domain retains accuracy, it results in weak robustness. Frequency domain gives good robustness but lacks imperceptibility. Therefore to increase robustness while preserving accuracy, it is required to develop integrated watermarking algorithm using different domains and/or hybrid approach. Vector data can be modelled using points, lines, and polygons as a basic feature. Existing algorithms do not differentiate between points, linear and aerial features and also very little attention is given towards consideration of relation among the geospatial objects.

At distribution level, one of the most common attacks applied is cropping attack. In many watermarking algorithms, watermark bits are inserted in consecutive coordinates. Such algorithm, when exploited by cropping attack, watermark may get destroyed and results into unidentified copyright information and hence it's owner. To deal with this, it is necessary to embed watermark bits into random vertex coordinates (or some key point coordinates) instead of consecutive vertex coordinates. Also, same watermark can be inserted multiple times in a vector data to make the algorithm more robust against regular as well as irregular cropping. In existing approaches, while evaluating performance of watermarking algorithm for vector data, the particular focus was only on some common attacks like geometrical transformation, noise, vertex addition/deletion etc. No attempt has been made to check whether topological relationship is maintained or not, which is very important in vector data.

One of the important requirements of raster (remotely sensed/satellite) data watermarking is that it should be near-lossless. This requirement is only satisfied if the watermarked pixel values are extremely closed to the

original pixel values (i.e. within some specified distance). If this requirement is not fulfilled, the percentage of misclassification of watermarked data is more. Also, only few algorithms are available satisfying this constraint and most of them have used wavelet and Fourier transform coefficients for embedding watermark. Therefore, there is a need to develop algorithms which use other frequency domain methods while satisfying mentioned constraint. For raster data watermarking algorithm evaluation, all well-known attacks for image watermarking can be used. However, only few of them (compression and filtering) were used to check robustness of raster data watermarking algorithms. Thus, it is required to consider some more important attacks to evaluate performance of raster data watermarking algorithms.

Geospatial data can be characterized by complex data objects and complex relationship between them. Securing such type of data at storage level is a challenging task and yet not fully understood and developed. There are certain unresolved issues like: (1)Protection of geospatial data using access control mechanism; (2) Deciding access control policy by considering individual layer, individual feature, and components of features; (3) Role of relationship between features in access control policy; (4) Specification and enforcement of content based access control. Also, the subject (user) and the objects (features) used by subject are dynamically and rapidly changing. Thus, it is required to develop a security policy which will solve all cited issues.

Due to voluminous nature of geospatial data, whole data cannot be stored at single server. Also various agencies are dealing with different data formats. According to their usage, geospatial data needs to be outsourced on some trusted servers by applying some modification/transformations. Transformation should be secure and efficient and robust against attack models. Moreover, the time required to perform transformation/inverse transformation should be less so that user can access it instantly. There is a need to develop secure outsourcing approach using efficient transformation mechanism and also a scheme should be developed which will enable authenticated end users to retrieve data of his own interest (for which he is authorized) without exposing other data. Attack models for both of these schemes need to be exploited.

CONCLUSION

Geographical Information System (GIS) represents geographical information in terms of raster as well as vector form. The compilation and management of this geospatial data is expensive and time consuming task. With the fast development of Internet and communication technology, it becomes easy to copy or distribute the geospatial data. Therefore copyright protection, authenticity, privacy, and spatial data source tracing have become important issues.

To deal with such situations : (1) an efficient access control mechanism has to be devised by considering all aspects of GIS data;(2)computationally inexpensive and attack resistant transformation for secure outsourcing is required; (3) robust and invisible digital watermarking needs to be used to protect geospatial data from unauthorized usage at distribution level. Based on review of available schemes, it is observed that there are some unsolved issues like robustness evaluation using various attack models which deals with characteristics of geospatial data, distortion control, and appropriate measures to evaluate geospatial data quality.

REFERENCES

Atluri, V. and Chun, S. 2007.Geotemporal role-based authorization system. International Journal of Information and Computer Security archive, Vol. 1(1/2), pp. 143-168.

Atluri, V. and Chun, S. 2004. An authorization model for geospatial data. IEEE Transactions on Dependable and Secure Computing, Vol. 1(4), pp. 238-254.

Barni, M., Bartolini, F., Cappellini, V., Magli, E. and Olmo, G. 2002. Near-lossless digital watermarking for copyright protection of remote sensing images. International Geoscience and Remote Sensing Symposium, Toronto, Canada, pp. 1447 – 1449.

Barni, M., Bartolini, F., Magli, E., Gabriello, O. and Zanini, R. 2001. Copyright protection of remote sensing imagery by means of digital watermarking. In Proceedings of SPIE conference on Sensors, Systems, and Next-Generation Satellites, Toulouse, France, pp. 550-565.

Belussi, A., Bertino, E., Catania, B., Damiani, M. and Nucita, A. 2004. An authorization model for geographical maps. In proceedings of the twelfth annual ACM international workshop on Geographic information systems, Washington D.C., U.S.A., pp. 82-91.

Bertino, E., Catania, B., Dmiani, M. and Perlasca, P. 2006. GEO-RBAC: A Spatially Aware RBAC. ACM Transactions on Information Systems and Security, pp. 1–34.

Cao, L., Men, C. and Li, X. 2010. Iterative embedding-based reversible watermarking for 2D-vector maps. In Proceedings of 17th IEEE International Conference on Image Processing, Hong Kong, pp. 3685-3688.

Chauhan, Y., Gupta, P. and Majumder, K. 2002. Digital Watermarking of Satellite Images. In Proceedings of 3rd Indian Conference on Computer Vision, Graphics and Image Processing, Ahmedabad, India, pp. 235-240.

Devanbu, P., Gertz, M., Martel, C. and Stubblebine, S. 2003. Authentic Data Publication over the Internet. Journal of Computer Security, Vol. 11(3), pp. 291 – 314.

Gabillon, A. and Capolsini, P. 2010. Dynamic Security Rules for Geo Data. Data Privacy Management and Autonomous Spontaneous Security, LNCS, Vol. 5939, pp. 136-152.

Gan, Q. 2003. Realization of Total-relationship Spatial Database Based on SDE. Surveying and Mapping of Sichuan. Vol. 26(02), pp. 59-61.

Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C. and Tan, K. 2008. Private queries in location based services: anonymizers are not necessary. In proceedings of the ACM SIGMOD International Conference on Management of Data, Vancouver, Canada, pp. 121-132.

Gertz, M., Kwong, A., Martel, C., Nuckolls, G., Devanbu, P. and Stubblebine, S. 2004. Databases that tell the Truth: Authentic Data Publication. IEEE Data (base) Engineering Bulletin, Vol. 27(1), pp. 26-33.

Hemalatha, T., Joevivek, V., Sukumar, K. and Soman, K. 2009. Robust Watermarking of Remote Sensing Images without the Loss of Spatial Information In Proceedings of 10th ESRI India User Conference, Noida, India, Vol. 1(2), pp. 1-8.

Hengartner, U. 2007. Hiding location information from location-based services. In proceedings of International Conference on Mobile Data management, Mannheim, pp. 268-272.

Ho, A. 2001. Robust Copyright Protection of Satellite Images Using a Novel Digital Image-In-Image Watermarking Algorithm. International Geoscience and Remote Sensing Symposium, Sydney, Australia, pp. 1194-1196.

Huo, X., Seung, T., Jang, B., Lee, S. and Kwon, K. 2010. A Watermarking Scheme Using Polyline and Polygon Characteristic of Shapefile. In Proceedings of International Conference on Intelligent Networks and Intelligent Systems, Shenyang, China, pp. 649-652.

Kim, J. 2010. Robust vector digital watermarking using angels and a random table. Advances in Information Sciences and Service Sciences, Vol. 2(1), pp.79-90.

Khoshgozaran, A. and Shahabi, C. 2007. Blind evaluation of nearest neighbour queries using space transformation to preserve location privacy. In proceeding of 10thACM International Conference on Advances in Spatial and Temporal Databases, Boston, MA, USA, pp. 239-257.

Liang. 2005. Study on view-based security model for database. Sun Yatsen University Forum, Vol. 3, pp. 134-137.

Li, Y. and Xu, L. 2003. A blind watermarking of vector Graphics images. In Proceedings of 5th International Conference on Computational Intelligence and Multimedia Applications, Xi'an, China, pp. 424-429.

Li, F., Hadjieleftheriou, M., Kollios, G. and Reyzin, L. 2006. Dynamic Authenticated Index Structures for Outsourced Databases. In Proceedings of ACM SIGMOD International Conference on Management of data, Chicago, Illinois, USA, pp. 121 – 132.

Lu, Z., Xu, D. and Sun, S. 2005. Multipurpose image watermarking algorithm based on multistage vector quantization. IEEE Transactions on Image Processing, Vol. 14, pp. 822-831.

Men, C., Cao, L., Li, X. and Wang, N. 2010.Global Characteristic-based Lossless Watermarking for 2D-Vector Maps. In Proceedings of International Conference on Mechatronics and Automation, Xi'an, China, pp. 276-281.

Oh, Y. and Bae, H. 2004. MLS/SDM: Multi-level Secure Spatial Data Model. Computational Science and Its Applications, LNCS, Vol. 3043, pp. 222–239.

Ohbuchi, R., Ueda, H. and Endoh, S. 2002. Robust watermarking of vector digital maps. In Proceedings of IEEE International Conference on Multimedia and Expo, Lusanne, Switzerland, Vol. 1, pp. 577-580.

Ramkumar, M., Akansu, A. and Alatan, A. 1999. A Robust Data Hiding Scheme For Images Using DFT. In Proceedings of International Conference on Image Processing, Kobe, Japan, Vol. 2(1), pp. 211-215.

Ruiz, J. and Megias, D. 2011. A novel Semi-fragile forensic watermarking scheme for remote sensing images.International Journal of Remote Sensing, Vol. 32(19), pp. 5583-5606.

Sandhu, R. and Samarati, P. 1994. Access control: principles and practice. IEEE Communication Magazine, pp. 40-48.

Sion, R. 2007. On the computational practicality of private information retrieval. In proceedings of the Network and Distributed Systems Security Symposium, San Diego, California, USA, pp. 87-96.

Tao, S., Dehe, X., Chengming, L. and Jianguo, S. 2009. Watermarking GIS data for digital map copyright protection. In Proceedings of 24th International Cartographic Conference, Santiago, Chile, pp.1-9.

Voigt, M., Yang, B. and Busch, C. 2004.Reversible watermarking of 2D-vector data. In Proceedings of Multimedia and Security Workshop, Magdeburg, Germany, pp. 160-165.

Wang, X., Huang, D. and Zhang, Z. 2011. A DCT-Based Blind Watermarking Algorithm for Vector Digital Maps.Journal of Advanced Materials Research, Vol. 179(180), pp.1053-1058.

Wang, C., Wang, W., Wu, B. and Qin, Q. 2009. A watermarking algorithm for vector data based on spatial domain. In Proceedings of 1st IEEE International Conference on Information Science and Engineering, Nanjing, China, pp. 1959-1962.

Yang, Y., Papadopoulos, S., Papadias, D. and Kollois, G. 2008. Spatial Outsourcing for Location-based Services. In Proceedings of 24th IEEE International Conference on Data Engineering, Cancun, Mexico, pp. 1082-1091.

Yanqun, Z. and Qianping, W. 2008. Security Model for Distributed GIS Spatial Data. In proceedings of International Symposium on Information Science and Engineering, Shanghai, pp. 641 – 645.

Yiu, L., Ghinita, G., Jensen, C. and Kalnis, P. 2009. Outsourcing Search Services on Private Spatial Data. In proceedings of twenty fifth IEEE International Conference on Data Engineering, Shanghai, pp. 1140 – 1143.

Yiu, M., Ghinita, G., Jensen, C. and Kalnis, P. 2010. Enabling search services on outsourced private spatial data. The International Journal on Very Large Data Bases, 19(3), pp. 363-384.

Zeng, Y., Wei, Z. and Yin, Q. 2007. Research on Spatial Database: A Secure Access mechanism. In proceedings of Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, pp. 2174-2178.

Ziegeler, S., Tamhankar, H., Fowler, J. and Bruce, L. 2003. Wavelet-Based Watermarking of Remotely Sensed Imagery Tailored to Classification Performance. In Proceedings of IEEE Workshop on Advances in Techniques for Analysis of Remotely Sensed Data, Greenbelt, MD, USA, pp. 259-262.

Zhu, C., Yang, C. and Wang, Q. 2008. A watermarking Algorithm for Vector Geo-spatial Data based on Integer Wavelet Transform. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Beijing, Vol. 37(B4).

Zhao, Y., Campisi, P. and Kundur, D. 2004. Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images. IEEE Transactions on Image Processing, Vol. 13(3), pp. 430-448.

Zhang, L., Yan, D., Jiang, S. and Shi, T. 2010. New robust watermarking algorithm for vector data. Wuhan University Journal of Natural Sciences, Vol. 15(5), pp. 403-407.