JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1165 - 1169
https://publishoa.com
ISSN: 1309-3452

Study on Approaches for Geospatial Data Security

Prof. Prajakta Bhangale[1], Dr. Shubhangi Vaikole[2]

[1] Research Scholar,
Computer Engineering Department, Datta Meghe college of Engineering,
Mumbai.
bprajakta11511@gmail.com

[2]Associate Professor
Computer Engineering Department, Datta Meghe college of Engineering,
Mumbai.
slv.cm.dmce@gmail.com

ABSTRACT

Geospatial data is very sensitive data. The GIS data model should provide make sensitive dataset available to authorized users only and preserve the access for insensitive data from same database to general users. To secure sensitive data from any unauthorized modifications and maintain its confidentiality, a strong encryption method with limited resources should be developed. Available encryption techniques for GIS data security are dealing with encryption technologies for GIS data based on watermarking, symmetric key cryptography techniques, and chaotic maps etc. which are useful for copyright protections. Geospatial data is used widely for many data sensitive applications like defence management, power grids, business decision making, tracking of events and activities using IoT devices etc. These systems are all vulnerable to various cyber-attacks, intrusions. It leads to incorrect information and affects business decisions

Keywords: Cryptography, Security, Geospatial data, vector data, raster data, Lightweight Cryptography.

I. INTRODUCTION

A GEOGRAPHIC INFORMATION SYSTEM (GIS) IS A COMPUTER PROGRAMME THAT SAVES AND DISPLAYS INFORMATION ABOUT THE EARTH'S SURFACE. THE GEOGRAPHIC INFORMATION SYSTEM (GIS) DEPICTS STREETS, BUILDINGS, AND VEGETATION. THIS ALLOWS PEOPLE TO IDENTIFY, EVALUATE, AND COMPREHEND PATTERNS AND CORRELATIONS MORE QUICKLY.

There are mainly two categories in geospatial data vector data and raster data. Vector data uses X and y coordinates to represent lines, polylines, polygons which represents map features. Raster data consist of pixels. They are stored in the form of image file. Like digital satellite images, digital aerial photographs etc.

The GIS data has two key characteristics.

- We must ban illicit duplication and distribution of GIS data since it is too expensive.
- GIS data contains a variety of confidential information that must be protected against unwanted access.

Encryption technologies for GIS data based on watermarking, symmetric key cryptography techniques, and chaotic maps for vector and raster data are all available encryption strategies for GIS data security. All of the techniques outlined above do not meet all of the requirements for reliable security with low resources.

II. ISSUES AND REQUIREMENT OF GIS DATA SECURITY

Existing systems explored for Raster Data encryption have most of the research done for maintaining copyright protection in the geospatial domain, more research can be done for achieving robust security for data. Also execution time and quality for existing cryptographic algorithms could be improved for GIS data security. Vector data encryptions are very crucial due to data sensitivity and widely used in resource.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1165 - 1169
https://publishoa.com
ISSN: 1309-3452

Many researchers have provided solutions to this by watermarking techniques for vector and raster data which is useful for copyright protection, ownership etc., and vector based algorithms are developed using location based services is able to provide security with limited resources in devices such as mobile devices but security may get compromised as RC6 algorithm used is vulnerable to statistical attack ,differential attacks due to its iterative statistical weakness in its round function.

III. RELETED WORK

To secure geospatial data over communication phase various methods are proposed. Following summary will give idea about various technologies invented by researchers.

A. VECTOR DATA ENCRYPTION TECHNIQUES

Vector map encryption is crucial, work proposed by Giao Phan [1] provide new efficient technique. It selects polyline layer from GIS data DP, SF and LA algorithms for defining breakpoints of objects randomization in key using SHA512 and 2D chaotic maps. DP algorithm has drawback of self intersection problem. DP algorithm, monotonic chain and dichotomy solves problem of self intersection. These methods can be used to improve performance for encryption.

Geospatial data encryption also achieved by GPT system [2].The algorithm proposes a new method, For location-based encryption error correcting codes key computation and randomized by mixing key with random parts of extension field, use a public key cryptosystem. The data is encrypted using a private key, which is then XORed with a geo lock based on the intended receiver's location and decryption time. This XORed data is then encrypted with asymmetric key encryption. The first key is obtained at the receiver's end by decoding with the private key. The session key is created by XORing the output with the geo lock, which is calculated with the same function as the sender. This session key will be used to decrypt the data. the data. It calculates unique parity matrix for each user, so improves security. It is public key cryptography technique, so time required is more than symmetric encryption techniques.

AES and the secret key used for encryption of feature vertices of the backbone object. Using SHA-512 hashing algorithm secret key is calculated and used to with user’s key input. This secret key K computes a set of random numbers by the Gaussian distribution is used to encrypt features encryption using AES or DES. Random Gaussian distribution algorithm is used for backbone object randomization in method is specified for vector data security [3].It does not change and increase the size of the encrypted file hence also prevents data loss. Thus more randomness high is the security. It is measured in terms of entropy where entropy is sum of entropies of random variables.

Vector watermark is embedded in low frequency coefficients HH, HL[4].Watermark is embedded multiple times to increased robustness. Watermark extraction is achieved by applying DWT on original and watermarked data. This method is robust against noise, up scaling, downscaling, translation ,format exchange, coordinate addition, coordinate deletion, cropping(25%and 40%)attacks but less robust to compression attack with normalized coefficient (NC) almost equivalent to 1 except for compression where it is 0.90. This method can be useful for copyright protection and copy control of digital images but sustainability for forgery attack, Collusion Attacks, still needs to be verifiable. The technologies used in vector map digital watermarking are analyzed and classified [5]

The Vector data encryption for drone security is proposed by Giao Pham et.al [6]. The proposed algorithm is based on the geographical features of raster data from geospatial data. Selective encryption in the frequency domain of discrete cosine transform is performed on geometric objects. This algorithm is very efficient for large volume data.

For Vector data security, many researchers worked on various methods for watermarking .In this method watermark is embedded by changing vertex coordinates within some error tolerance [7].These algorithms are vulnerable to compression and deletion attacks.

Bang, N.V et al has other approach of vector data security by selecting and encrypting objects of polyline-polylines layers by chaotic map generated key set. It creates two key sets one is generated by SHA512 hashing of users password and other key set is generated by chaotic map. This gives enhanced security to vector data. This selective encryption reduces computation overhead and time This security could be improved by key set from combination of two chaotic map function.[8].also key sensitivity analysis results shows that slight change in keysets causes incomprehensible data

which consequently enhances security. This algorithm further can be modified by reducing no of objects selected so to reduce computation to great extent.

One of the research proposes vector watermarking using discrete cosine transform, disc. These methods are used for copyright and fragile to noise attack. To overcome this drawback various methods based on ciphers were developed.[9]

Latest work by Na Ren et.al has introduced new watermarking technique by combining zero watermarking and blockchain. This method eextracts the feature points by vector map line and compressed surfaces. The angle sequence of the feature points is XORed operation is with copyright image. As a output we get multiple zero watermarks. Experiments show that the proposed algorithm completely resists translation, rotation, and scaling attacks and has good robustness to compression, cropping, and adding attacks. Also NC value obtained is always equivalent to one. [10]It achieved copyright protection for the lossless vector map.

B. RASTER DATA ENCRYPTION TECHNIQUES

Security of raster data is obtained by watermarking technique. In this watermark is embedded in low frequency coefficients of wavelet transforms [11]. In this Arnold's permutation is used for watermark embedding.2-D DWT is applied on each channel of host raster image till third level. From this third level components LL3 and HH3 coefficients are selected for embedding the watermark. To get the watermarked raster inverse DWT is applied as last step. Exactly reverse procedure is applied to extract watermark. With this method, efficient results are obtained compared to previous papers for various geometric and non-geometric attacks for raster images of geospatial data. Robust watermark has ability to resist regular malicious attacks, and used to confirm the ownership of document, distributor and authorized clients for data. Fragile watermark is less robust and mainly used to provide the authenticity and integrity of the data.

One of the researches works presents security of GIS data using Visual Cryptography technique for raster images by generating two shares from image [12]. It mainly focuses on secure transmission of raster maps and the computation-free encryption scheme of raster maps. Encoding is done in the Block-wise encoding is done by generating shares block wise and imposed with equal sized secret block. With this feature pixel expansion is eliminated therefore improving quality of visual perception. Here vector data security is not addressed and it works only for greyscale images .Also, in VC method more the number of shares more security we achieve so here security could be compromised easily as only two shares are used. This method could be further improved to apply for high resolution raster images.

M. Lianquan et.al. Suggested Digital watermarking algorithm based on DCT and DWT, these algorithms are vulnerable to compression and deletion attacks [13].

Also other watermarking approach using AES and RSA is studied for both raster and vector this data [14].This method uses two levels of AES cryptography and one level of RSA cryptography. Original raster image encrypted with AES 128 bit and least significant bits are used to embed checksum which can be verified at receiver side. Composite function calculates composite image. Composite and encrypts image together encrypted using RSA and sent over the network. While decrypting data exactly reverse procedure carried out. This technique combine advantages of both symmetric and asymmetric encryption hence achieves high security. This technique was not tested with real time data so practical implementation and its performance comparison is not possible.

The method propose by Y Dakroury et.al uses AES and RSA with digital watermarking techniques that can be applied both raster and vector data.[15] For AES key generation, uses salt, iteration count, and password in key derivation functions .For RSA, 512, 1024 or 4096 bits key is used. Password is encrypted with private key of RSA to create watermark and that watermark is embedded in image using predefined seed. Decryption module uses 256-bit AES in counter mode. Iteration count is crucial factor; more no. of iterations gives more stronger key so difficult to crack such information. To improve the performance different asymmetric algorithms could be applied for final stage to make system more random and secure.

IV.INVESTIGATION AND ANALYSIS

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1165 - 1169
https://publishoa.com
ISSN: 1309-3452

Various research papers give varying results for respective technology for raster and vector data encryption. Following table shows basic comparison of the results with raster data.

Following table shows summarized

TABLE I. COMPARISON OF EXISTING SYSTEMS FOR RASTER DATA ENCRYPTION

Author& Ref No.	**Average PSNR**	**Features**
Lijing Ren et.al [7]	49.52	Size invariant, Quality improvement Computation free technique
Sangita Zope et.al[11]	53.87	robust against scaling, cropping and rotation attack.

For vector data methods discussed in previous section, performance is measured on basis of different parameters like entropy, time taken for loading encrypted images, max-error based on no of selected objects from vector maps, MSE for watermarking technique. This watermarking technique results are degraded with increased embedding power and is not robust against compression attack [11].Method invented by Giao phan et.al [2] is used to encrypt randomly vertices of objects like polygons and polylines depicts high key sensitivity to achieve immense security for vector data in comparison with watermarking techniques.

Existing systems explored for Raster Data encryption have most of the research done for maintaining copyright protection in the geospatial domain, more research can be done for achieving robust security for data. Also execution time and quality for existing cryptographic algorithms could be improved for GIS data security. Vector data encryptions are very crucial due to data sensitivity and widely used in various resources.

India has identified shortcomings in the country's widespread use of GIS, which must be addressed as part of the process of developing a National GIS. GIS is technology-driven, but it also needs to be decision-driven. This means that all types of decision makers, including governments, businesses, and people, should be able to use GIS data and apps to solve problems. The Geographic Information System (GIS) will be critical to modern governance and nation-building. While achieving this goal, one crucial feature of GIS data is, it is very sensitive which thereby calls to address key issues associated with using and sharing confidential geospatial data."

The research work should focus mainly on achieving robust security for raster data and vector by using a combination of chaotic functions, genetic algorithms and other efficient encryption methods.

V.CONCLUSION

Geospatial data is accessed widely for various applications all over the world. It is expected to ensure security, authenticity and availability of data on limited resources devices also. So here we propose secure GIS data with less computing power and with robust security over communication networks by using efficient techniques for encryption for vector and raster data. The proposed work will aim to contribute research towards attaining an improved security for geospatial data using lightweight cryptography algorithms for vector and raster data, which will reduce the use of high power computation resources, thereby limiting resources required for security.

REFERENCES

[1] Gian Pham" Vertices random selection for vector map data in encryption process" Volume 2; Issue 4; July-

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1165 - 1169
https://publishoa.com
ISSN: 1309-3452

August 2021; Page No. 823-826
[2] Eraj Khan, Abbas Khalid, Arshad Ali*, Muhammad Atif, Ahmad Salman Khan" Geo Security using GPT Cryptosystem" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 2, 2020
[3] Giao N. Pham , Son T. Ngo , Anh N. Bui , Dinh V. Tran , Suk-Hwan Lee and Ki-Ryong Kwon , " Vector map random encryption algorithm based on Multiscale simplification and gausian distribution" ISPRS Int. J. Geo-Inf. 2019, 9, 4889
[4] Sangita Zope-Chaudhari, Parvatham Venkatachalam, Krishna Mohan Buddhiraju,"Copyright protection of vector data using vector watermark" IGARSS 2017.
[5] M. Voigt and C. Busch. "Feature-based watermarking of 2D-vector data". In Proc. of SPIE International Conference on Security and Watermarking of Multimedia Content, Santa Clara, CA, USA, 2003, pp.359-366
[6] Gian Pham, Kwang-Seok Moon, Suk-Hwan Lee, Ki-Ryong Kwon "GIS Map encryption algorithm for Drone security based on geographical features"
[7] Liangbin Zheng, Yulu Jia, Qun Wang,"Research on Vector Map Digital Watermarking Technology" 2009 First International Workshop on Education Technology and Computer Science
[8] Suk-Hwan Lee, Ki-Ryong Kwo. Bang, Kwang-Seok Moon, Sanghun Lim," Selective Encryption scheme for vector map data using chaotic map" Journal of Korea Multimedia Society Vol. 18, No. 7, July 2015(pp. 818-826)
[9] I. Kitamura, S. Kanai, and T. Kishinami. "Copyright protection of vector map using digital watermarking method based on discrete Fourier transform". In Proc. of IEEE International Geosciences and Remote Sensing, Sydney, NSW, Australia, 2001, pp. 191-193.
[10] Na Ren,Yazhou Zhao,Changqing Zhu ,Qifei Zhou, Dingjie Xu," Copyright Protection Based on Zero Watermarking and Blockchain for Vector Maps" ISPRS Int. J. Geo-Inf. 2021, 10, 294. https://doi.org/10.3390/ijgi10050294
[11] Sangita Zope-Chaudhari, Parvatham Venkatachalam,"Robust Copyright protection of raster images using wavelet based digital watermarking "IGARSS 2014.
[12] Lijing Ren "A Novel Raster Map Exchange Scheme Based on Visual Cryptography"HindawiAdvances in Multimedia Volume 2021, Article ID 3287774, 7 pages
[13] M. Lianquan and Y. Qihong. "A digital map watermarking algorithm based on discrete cosine transform". Journal of Computer Applications and Software, 2007, pp. 146-148
[14] Monika Bansal and Akanksha Upadhyaya," Three-Level GIS Data Security: Conjointly Cryptography and Digital Watermarking" Springer Nature Singapore Pte Ltd. 2018 M. U. Bokhari et al. (eds.), Cyber Security, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_24
[15] Y Dakroury, IA El-Ghafar," Protecting GIS data using cryptography and digital watermarking"IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010
[16] R. Ohbuchi, H. Ueda, and S. Endoh. "Robust watermarking of vector digital maps". In Proc. of IEEE International Conference on Multimedia and Expo., Lusanne, Switzerland, 2002, pp. 577-580.