SECURE OUTSOURCING OF TREND SURFACE ANALYSIS

Salih Demir & Bulent Tugrul*
[1]Ankara University, Department of Computer Engineering, Golbasi, Ankara, Turkey

ABSTRACT
Data has been collected for analysis purposes by governments, companies, and institutions. Data analytics is used to discover precious knowledge from huge amount of data. Spatial analysis is one of the main components of GIS tools. Spatial analysis is the process of manipulating of spatial data to reach knowledge. Spatial interpolation methods are employed to build prediction models for unmeasured points. Spatial interpolation methods play a crucial role for many engineering and financial disciplines. Trend Surface Analysis (TSA) is one of the most applied and dependable spatial interpolation methods. TSA, basically, searches the best fitted polynomial expression for the given data set. Such calculations may require so much time, computing and storage capacity. In recent years, there is a new trend to transfer these kinds of burdens to cloud servers which are dedicated to give computing and storage services. However, data is one of the most valuable assets of institutions. Therefore, privacy of each party becomes more critical. Data owners try to hide their data from both clients and cloud servers. The clients want to get a prediction value without disclosing the coordinates where it may invest its money and time. Our study proposes a secure solution in this framework. We examine our solution thoroughly in terms of accuracy and security.

Keywords: *Cloud computing, Outsourcing, Security, Spatial interpolation, Trend surface analysis,*

1. INTRODUCTION

Data is collected for variety of purposes by governments, companies, and institutions. Storing vast amount of data does not reveal any valuable information. Data should be analyzed to extract knowledge. Governments use social media data to collect intelligence about evil-minded people. Health records are examined to find a treatment for an incurable disease. Mobile or Internet service providers explore their customers' usage statistics to offer them new campaigns. Otherwise, they may lose their loyal customers to competitors. Statistics and data mining methods can be employed to analyze such datasets. Analyzing complex and huge amount of data requires so much storage and computing capacity.

Scientific computations require so much time, storage and computation power by nature. Recent trends show that there is a shift from server-client architecture to cloud computing. Cloud computing allows low-capacity (in terms of memory, CPU, and battery) users to move their data and necessary computations to high-capacity cloud servers to reduce time and money costs. However, users must take the privacy of their data into consideration. Governments have been approving laws to protect the privacy of their citizens against misuse. Therefore, private data cannot be stored publicly in cloud servers. Storing the data in encrypted form may provide confidentially of private data. However, it makes difficult to compute related analysis functions. Secure multi-party computation (SMC) or privacy-preserving methods allow transferring private data between users and cloud servers.

Spatial analysis allow data analyst to explore patterns and relationships that are captured in spatial data. Similarly, spatial interpolation methods (SIM) analyze and describe spatial variability using statistical, mathematical and geographical principles. Li and Heap [1] classified 25 commonly applied methods based on their features. They categorized all SIMs in three different sets: non- geostatistical, geostatistical and hybrid methods. Kriging, a geostatistical method, is the far most famous and applied one. However, Inverse distance weighted (IDW), Nearest neighbors (NN) and Trend surface analysis methods are considerably used in many engineering studies. TSA seeks the best (according to least squared error) polynomial expression to fit spatial data. It has two different choices: local and global. Local TSA uses only the neighbor points where a prediction is asked. On the contrary, global TSA use the entire data set.

In traditional spatial interpolation architecture, there are two parties; Data owners and Clients. Data owner has all the necessary data to build a prediction model. It stores, manages and computes spatial data to give services to clients. Clients request predictions from data owners for its future investments. As seen, in traditional architecture there is no privacy concern from the perspectives of both parties. In real life, both parties may behave in a malicious manner. Data owner may share the coordinates where the clients are planning to make an investment with competitors of the clients. A solution that considers the privacy of both parties is necessary for spatial interpolation analysis.

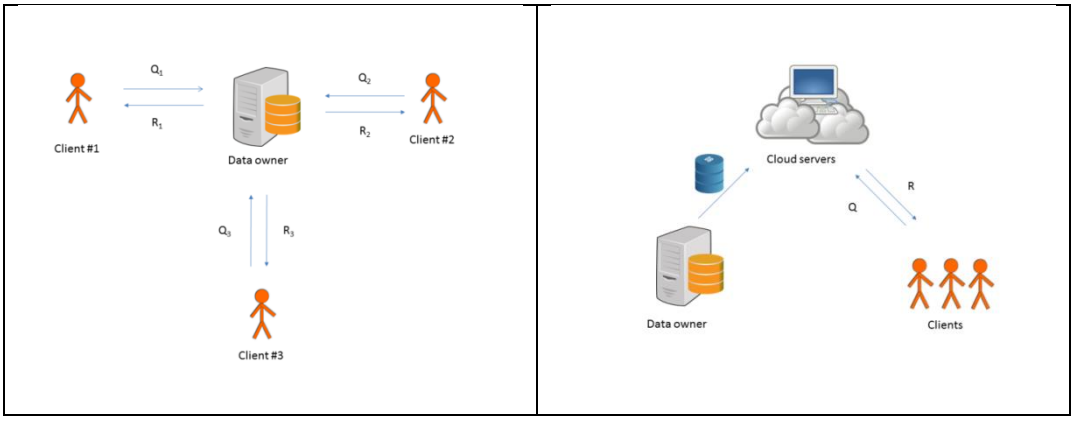

Figure 1. Traditional vs Cloud computing spatial interpolation architecture

The paper is organized as follows; Sect. 2 investigates related studies about TSA and SMC in the literature. Essential methods used in our proposed solution are briefly explained in Sect. 3. After presenting our solution, we analyze our solution in terms of privacy and accuracy. The paper is finalized with conclusion and future work section.

2. RELATED WORK

Client-server architecture has been widely used for more than two or three decades. Recently due to low cost and less maintenance requirements of cloud computing, IT professionals try to change their infrastructures. Cloud computing allows outsourcing hardware resources to third-party companies and can provide services (IaaS, Paas and Saas) for huge data and scientific computation at lower costs [2]. Yiu et al. [3] proposed how to enable outsourcing of similarity search techniques for sensitive data. Their solution is a compromise between efficiency and privacy. Zhou et al. [4] came up with a solution which is a new scheme to conduct secure k-nn query over encrypted data located in cloud servers. Their solution protects both data owners' and clients' private data from cloud servers.

SMC introduced by Yao [5] is defined as how to compute a joint function without revealing distrusting parties' (two or more) private inputs to each other. SMC protocols must assure both privacy and correctness properties. SMC protocols are based on either secret sharing or garbled circuit construction. Ben-Or et. al [6] and Chaum et al. [7] proposed solutions based on secret sharing. However, Yao offered a binary circuit design for two-party SMC. Micali et al. [8] extended two-party scheme to multi-party scheme. After the introduction of SMC, the first studies laid out theoretical principles. Bogetoft et al. [9] gave an example of first practical implementation of SMC based protocols. Since then, SMC protocols have been implemented in many different scenarios; Auctions, E-Voting and Data Mining.

A Geographic Information System (GIS) captures, stores, processes and visualizes spatial data to reveal relationships, patterns and trends using a computer system. Advancements in computer and surveying engineering enable to apply GIS principles to variety of disciplines. A general GIS tool should perform these tasks; Input, Manipulation, Management, Query, Analysis, and Visualization. One of the methods of analysis task is spatial interpolation. Spatial interpolation is defined as predicting a value for a target location within same region of measured points [10]. There are a variety of spatial interpolation methods. Nearest Neighbors (NN) IDW, Kriging, and TSA are examples of widely known and applied methods [1]. The author studied IDW and Kriging [11-14] methods under the light of protecting the privacy of users. The scientists and data owners can apply the proposed methods, if they have privacy concerns.

Oldham and Sutherland [15] introduced TSA for the first time. Watson [16] described essential principles of TSA. Since then, scientist applied TSA with other spatial interpolation methods to compare their results. Luo et al. [17] applied TSA and six other spatial interpolation methods to construct surfaces created by wind speed data collected from England and Wales. Obasi et al. [18] extended calculation of the constants in the TSA equation to get a more simplified form of the matrices. Pellitero et al. [19] develop a software tools to reconstruct the 3D surface of palaeoglaciers. They applied many spatial interpolation methods and TSA as well.

3. BACKGROUND

3.1. Trend Surface Analysis

Li and Heap [1] compares spatial interpolation methods according to their features. There are many ways to classify spatial interpolation methods. One of them is whether they are local or global predictors. Local methods use only data in the region of interest to produce a prediction. On the other hand, global methods use entire data collected from the region to build a prediction model. TSA utilizes a polynomial expression according to least squares criteria. A second degree polynomial equation can be used to relate geographic variables (x and y) to spatial variation [20].

$$z = a_0 + a_1x + a_2y + a_3x^2 + a_4y^2 + a_5xy \quad (1)$$

Higher degree equations can be employed to represent more complex data. The coefficients (a_0, a_1, a_2, a_3, a_4, a_5) can be calculated in the same manner as in regression analysis. Sen [20] presents the required calculation to find the coefficients.

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{bmatrix} = \begin{bmatrix} 1 & \bar{x} & \bar{y} & \overline{x^2} & \overline{xy} & \overline{y^2} \\ \bar{x} & \overline{x^2} & \overline{xy} & \overline{x^3} & \overline{x^2y} & \overline{xy^2} \\ \bar{y} & \overline{xy} & \overline{y^2} & \overline{x^2y} & \overline{xy^2} & \overline{y^3} \\ \overline{x^2} & \overline{x^3} & \overline{x^2y} & \overline{x^4} & \overline{x^3y} & \overline{x^2y^2} \\ \overline{xy} & \overline{x^2y} & \overline{xy^2} & \overline{x^3y} & \overline{x^2y^2} & \overline{xy^3} \\ \overline{y^2} & \overline{xy^2} & \overline{y^3} & \overline{x^2y^2} & \overline{xy^3} & \overline{y^4} \end{bmatrix}^{-1} \begin{bmatrix} \bar{z} \\ \overline{xz} \\ \overline{yz} \\ \overline{x^2z} \\ \overline{xyz} \\ \overline{y^2z} \end{bmatrix} \quad (2)$$

The left-hand side of the equation corresponds the coefficients of the trend surface equation. The right-hand side of the equation consists of averages of the variables in the data set.

3.2. Secure Matrix Multiplication Protocol (SMMP)

Secure matrix multiplication protocol was proposed by many researchers [21, 22]. We prefer to employ the protocol which has the same architecture as in matrix inversion protocol described in the next subsection presented by Nassar et al. [23]. The matrices (A and B) are additively broken into two halves which should satisfy $A = A_1 + A_2$ and $B = B_1 + B_2$ and each part is stored in two non-colluding cloud servers. Their protocol is based on:

$$AB = (A_1 + A_2)(B_1 + B_2) = A_1B_1 + A_1B_2 + A_2B_1 + A_2B_2 \quad (3)$$

Assume that matrices A_1 and B_1 are stored by CS_1, similarly matrices A_2 and B_2 stored by CS_2. The first additive term of (3) $A_1 B_1$ can be computed by CS_1 without help of CS_2. Additionally, the additive last term $A_2 B_2$ can be computed by CS_2 alone. The remaining terms A_1B_2 and A_2B_1 can be calculated with the help other cloud servers. SMMP requires 4-matrix transfers in the best case (8 in the worst case) between cloud servers.

3.2. Secure Matrix Inversion Protocol (SMIP)

Computing inverse of a matrix is a very common operation in engineering and scientific equations. Secure Multi-party Computation (SMC) which is a sub branch of information security enable to calculate an output of a function using private data of two or more parties without disclosing their private inputs. Nassar et al. [23] proposed a secure matrix inversion protocol. Their solution divides the matrix A into two separate matrix A_1 and A_2 where $A_1 + A_2 = A$. Each part (A_1 and A_2) is stored in two non-colluding cloud servers. None of the server can learn the private matrix A.

$$A^{-1} = A_1^{-1}(A_1^{-1} + A_2^{-1})^{-1}A_2^{-1} \quad (4)$$

If the right hand side is inverted,

$$(A_1^{-1}(A_1^{-1} + A_2^{-1})^{-1}A_2^{-1})^{-1} = A_2(A_1^{-1} + A_2^{-1})A_1 = A_2A_1^{-1}A_1 + A_2A_2^{-1}A_1 = A_2I + IA_1 = A_2 + A_1 = A \quad (5)$$

SMIP requires three non-colluding servers to conduct such calculation. A_1^{-1}, $A_2^{-1}$and $A_1^{-1} + A_2^{-1}$ are stored in three different servers respectively. Inverse of Matrix A can be calculated using secure 3-matrix multiplication protocol described in their study. They achieve 3-matrix multiplication protocol in three different ways; Additive splitting, Homomorphic encryption and Shamir's secret sharing. Additive splitting solution requires 8-matrix transfers between cloud servers.

3.3. Homomorphic Encryption

There are two different kinds of encryption methods. The first kind called symmetric (private) encryption methods which use the same key for both encryption and decryption functions. Symmetric methods utilize confusion and diffusion operations to produce cipher-text from plain-text and key. The second kind is called asymmetric (public) encryption methods. These methods employ complex modular arithmetic operations to provide confidentiality service

between communicating parties. Homomorphic encryption algorithms based on asymmetric cryptography allow performing arithmetic calculations without decrypting cipher-texts. There a few scheme that shows such properties. Paillier [24] cryptosystem is one of the examples of such algorithms. It satisfies homomorphic addition and multiplication of plaintexts. Basically multiplying two cipher-texts is equal to summation of corresponding values in plaintexts.

$$D(E(m_1, pk) \cdot E(m_2, pk)(mod\ n^2)) = m_1 + m_2\ (mod\ n) \quad (6)$$

The multiplication property can defines as a cipher-text raised to a constant k is equal to the product of the corresponding values in plaintexts and the constant.

$$D(E(m_1, pk)^{m_2}\ (mod\ n^2)) = m_1\ m_2\ (mod\ n) \quad (7)$$

4. PROPOSED SOLUTION

Firstly, we want to identify to goals that a secure outsourcing protocol must present.

- *Correctness*: If all parties involved in the protocol follow the steps honestly, the output will be the same as in traditional scheme.
- *Privacy*: Private data of all parties must be protected from ineligible users.
- *Efficiency*: Efficiency in terms memory, communication and computation may be affected due to protocols used to satisfy privacy. However, the cost must be at acceptable level.

As described in Introduction section there are three parties which want to establish a secure prediction model on their private data.

- *Data Owner (DO)* gathers and stores spatial data from a specific territory.
- *Cloud Servers (CS)* has sufficient storage and computing capacity to process spatial data and offers prediction services to clients.
- *Clients (C)* can be investors or researchers who need a prediction value for a specific coordinate within the territory in interest.

Our solution follows the steps explained below;

I. DO encrypts all values (x_i, y_i, z_i) with his secret key and sends to one of the CS (CS_1) which manages communication between other servers. Encryption with DO's key provides confidentiality which means that only DO can decrypt and read the values in cipher text form. Therefore, CS_1 cannot learn any input due to encryption.

ID	x	y	z
1	x_1	y_1	z_1
2	x_2	y_2	z_2
3	x_3	y_3	z_3
…	…	…	…
n	x_n	y_n	z_n

Table 1a. Spatial data table owned by DO

ID	x	y	z
1	$\xi_{DO}(x_1)$	$\xi_{DO}(y_1)$	$\xi_{DO}(z_1)$
2	$\xi_{DO}(x_2)$	$\xi_{DO}(y_2)$	$\xi_{DO}(z_2)$
3	$\xi_{DO}(x_3)$	$\xi_{DO}(y_3)$	$\xi_{DO}(z_3)$
…	…	…	…
n	$\xi_{DO}(x_n)$	$\xi_{DO}(y_n)$	$\xi_{DO}(z_n)$

Table 1b. Encrypted spatial data table stored by CS

II. CS_1 applies addition and multiplication properties of Paillier system to form the necessary matrices to calculate the coefficients of polynomial expression and sends them back to DO.

III. DO owns the necessary key to decrypt the values in matrices. DO divides matrices B and C into two halves ($B = B_1 + B_2$ and $C = C_1 + C_2$) as described in SMIP protocol and sends each halve to two non-colluding cloud servers. Cloud servers cannot build prediction model with the halves they have. Servers need the other halves to build a prediction model based on TSA.

IV. The coefficients of polynomial expression can be computed after multiplying $(B_1 + B_2)(C_1 + C_2)$ with SMMP.

V. The client encrypts the coordinate value (x_p, y_p) where it needs a prediction with his private key [$\xi_C(1)$, $\xi_C(x_p)$, $\xi_C(y_p)$, $\xi_C(x_p^2)$, $\xi_C(y_p^2)$, $\xi_C(x_p y_p)$] and sends them to CS.

VI. CS_1 calculates "$a_0^{\xi_C(1)} * a_1^{\xi_C(x_p)} * a_2^{\xi_C(y_p)} * a_3^{\xi_C(x_p^2)} * a_4^{\xi_C(c)} * a_5^{\xi_C(x_p y_p)}$," with Paillier cryptosystem which is equal to "$a_0 + a_1 x_p + a_2 y_p + a_3 x_p^2 + a_4 y_p^2 + a_5 x_p y_p$" in plaintext and sends the cipher text to the client.

VII. The client possesses the required decryption key to open and get the final prediction value for the coordinate (x_p, y_p).

5. ANALYSIS OF THE PROPOSED SOLUTION

5.1. Supplementary cost analysis

In traditional spatial interpolation methods, DO gathers, stores, and computes data to produce a prediction value for the location requested by a client. However, traditional methods do not provide privacy for both of the parties. SMC and Privacy-preserving methods can be applied to provide security services. On the other hand, these methods may increase computation, communication and storage costs.

5.1.1. Computation cost analysis

All necessary computation should be done by DO in traditional system. If cloud computing is preferred due to efficiency and economic reasons, cloud servers should do all necessary computations. Cloud servers take the burdens of building a prediction model from DOs, however, a significant concern about privacy remains. Our proposed solution offers a privacy preserving solution for DOs, CSs and clients. SMC protocols and homomorphic encryption allow us to present such solution. As expected, these methods increase total number of computations to offer a secure outsourcing prediction service to community. Spatial interpolation services are not hard real time systems unlike automation systems. Therefore, minor delays when producing prediction does not affect all parties. DO must encrypt all spatial data table to send CS. CS must use multiplication operation instead of addition to find aggregate values of matrices using encrypted values. Multiplications require more time than addition operations. DO must decrypt two matrices which are parts of TSA equation and apply secret sharing schemes to divide them into two shares. CSs must apply SMIP and SMMP protocols to find coefficients described in Eq. (1). The client encrypts target coordinate (x_p, y_p) with its key and gets [$\xi_C(1)$, $\xi_C(x_p)$, $\xi_C(y_p)$, $\xi_C(x_p^2)$, $\xi_C(y_p^2)$, $\xi_C(x_p y_p)$]. Therefore it must call encryption function six times. CS computes $a_0^{\xi_C(1)} * a_1^{\xi_C(x_p)} * a_2^{\xi_C(y_p)} * a_3^{\xi_C(x_p^2)} * a_4^{\xi_C(c)} * a_5^{\xi_C(x_p y_p)}$ which is corresponding to final prediction value in cipher-text. The client must call decryption function using the key known by only it to get prediction value in plain-text.

5.1.2. Communication cost analysis

Transferring all data to the cloud servers increases communication costs. The spatial data table in encrypted form must be sent to one of the CSs. The engaged cloud server computes the matrices in encrypted form used in TSA and sends back to the DO. Two matrices (B_1 + B_2 and C_1 + C_2) are generated according to secret sharing principles by DO and sent to CSs. As described in Nassar et al. [23], these matrices must be transferred to other cloud servers to run SMMP and SMIP. Therefore our solution creates 1 x (size of spatial data table) + 12 x (size of matrices) (best case) (matrices are far smaller than data table) additional communication between CSs and DO.

5.1.3. Storage cost analysis

If there is no privacy and efficiency concern, all spatial data and matrices are stored in DO's servers. However our solution which offers both privacy and efficiency uses more storage capacity. Additionally, an encrypted form of the spatial data table must be stored in one of CSs. TSA requires two matrices to compute coefficients of the polynomial expression, but three times more capacity (by cause of SMMP and SMIP protocols) needed for our solution. Therefore our solution requires 1 x (size of spatial data table) + 4 x (size of matrices) (best case) additional storage capacity (matrices are far smaller than data table).

5.2. Accuracy Analysis

Some of the Privacy-preserving Data mining methods which are employed to hide private data may worsen the accuracy of the prediction models. Agrawal and Srikant [25] proposed Random data perturbation techniques to protect private data of users. Simply, a random noise produced according to a distribution is added to original data sets. Kargupta et al. [26] showed that the original data can be estimated from perturbed data using spectral filter techniques. Therefore, in our solution, we prefer to use homomorphic cryptosystem and secret sharing methods. Both of the methods are deterministic which implies that the final prediction value of the traditional scheme and our solution will be same. The parties involved in secure outsourcing of TSA will build a prediction model with the same accuracy. Additionally, privacy of all parties is assured.

5.3. Privacy Analysis

As we claimed, a secure outsourcing protocol must assure correctness, privacy, and efficiency. In order to demonstrate that our solution keeps the privacy of all parties, we should prove that nobody's private data is not disclosed to unauthorized parties.

- DO encrypts spatial data set with the key known by only itself before sending to CS. Therefore, cipher text stored in servers cannot be read by any CSs. Even if the transaction line between DO and CSs are tampered, malicious parties cannot get useful information.
- The encryption method which has homomorphic properties allow CS to build and compute necessary matrices required for TSA. The matrix values are aggregation of spatial data, therefore, CS or malicious parties cannot estimate corresponding measurement value for a specific location from the matrices.
- Furthermore, the matrices are partitioned into halves (not essentially equal parts) using secret sharing schemes. CSs must behave maliciously to learn matrices however this behavior will damage their reputation and trustfulness. To emphasize, even if they behave maliciously they will learn only values inside matrices, not any specific spatial data.
- The client sends the coordinate value in encrypted (uses the key known only by client) form to CSs. Our solution allows CSs to compute final prediction value in cipher text form. Therefore, DO, CSs and any other third parties cannot learn the location where the client needs a prediction value.

From the statements explained above, we can conclude that our solution fulfils privacy requirements of a secure outsourcing protocol.

6. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a framework how to achieve a secure outsourcing of TSA which is one of the fundamental spatial interpolation methods used by scientist. We employed secure matrix multiplication and inversion protocols which are studied in many studies. We chose solutions introduced by Nassar et al. [23] due security and efficiency reasons. Furthermore, we employed Paillier homomorphic cryptosystem to transfer and compute sensible inputs of data owners and clients. After illustrating the details of our solution, we analyzed it in terms supplementary cost, accuracy, and privacy. We conclude that supplementary cost of our solution is negligible, accuracy of both traditional scheme and secure outsourcing of TSA are same and privacy of all parties is assured. Our future direction will study remaining spatial interpolation methods in the same architectural perspective. As mentioned in related work section, SMC protocols of Kriging and IDW are published by authors. However, scientist may want to use other spatial interpolation methods to compare their results.

7. ACKNOWLEDGEMENTS

This work was supported by the Ankara University Scientific Research Projects under Grant [BAP- 15B0443011].

8. REFERENCES

[1] J. Li, A.D. Heap, Spatial interpolation methods applied in the environmental sciences: A review, *Environmental Modelling & Software*. **53**, 173-189 (2014).
[2] J.R. Vacca, "Cloud Computing Security: Foundations and Challenges", CRC Press (2016).
[3] M.L. Yiu, I. Assent, C.S. Jensen, P. Kalnis, Outsourced similarity search on metric data assets, *IEEE Transactions on Knowledge and Data Engineering*. **24**(2), 338-352 (2012).
[4] L. Zhou, Y. Zhu, A. Castiglione, Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner, *Computers & Security*, (2016).
[5] A.C. Yao, Protocols for secure computations, *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science* (1982).
[6] M. Ben-Or, S. Goldwasser, A. Wigderson, Completeness theorems for non-cryptographic fault-tolerant distributed computation, *Proceedings of the twentieth annual ACM symposium on Theory of computing* (1988).
[7] D. Chaum, C. Crépeau, I. Damgård, Multiparty unconditionally secure protocols, *Proceedings of the twentieth annual ACM symposium on Theory of computing* (1988).
[8] S. Micali, O. Goldreich, A. Wigderson, How to play any mental game, *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC* (1987).
[9] P. Bogetoft, I. Damgård, T.P. Jakobsen, K. Nielsen, J. Pagter, T. Toft, A practical implementation of secure auctions based on multiparty integer computation, *Financial Cryptography*. **4107**, 142-147 (2006).
[10] P.A. Burrough, M.D. Rachael, L.D. Chriotopher, "Principles of geographical information systems", Oxford University Press (2015).
[11] B. Tugrul, H. Polat, Estimating Kriging-based predictions with privacy, *International Journal of Innovative Computing, Information and Control*. **9**(8), 3197-3209 (2013).
[12] B. Tugrul, H. Polat, Privacy-preserving inverse distance weighted interpolation, *Arabian Journal for Science and Engineering*. **39**(4), 2773-2781 (2014).

[13] B. Tugrul, H. Polat, Privacy-preserving kriging interpolation on partitioned data, *Knowledge-Based System.* **62**, 38-46 (2014).
[14] B. Tugrul, H. Polat, Privacy-Preserving Kriging Interpolation on Distributed Data, *International Conference on Computational Science and Its Applications* (2014).
[15] C. Oldham, D. Sutherland, Orthogonal polynomials: Their use in estimating the regional effect, *Geophysics.* **20**(2), 295-306 (1955).
[16] G.S. Watson, Trend-surface analysis, *Mathematical Geology*. **3**(3), 215-226 (1971).
[17] W. Luo, M. Taylor, S. Parker, A comparison of spatial interpolation methods to estimate continuous wind speed surfaces using irregularly distributed data from England and Wales, *International journal of climatology*. **28**(7), 947-959 (2008).
[18] A. Obasi, A. Onwuemesi, O. Romanus, An enhanced trend surface analysis equation for regional–residual separation of gravity data, *Journal of Applied Geophysics*. **135,** 90-99 (2016).
[19] R. Pellitero, et al., GlaRe, a GIS tool to reconstruct the 3D surface of palaeoglaciers, *Computers & Geosciences*. **94**, 77-85 (2016).
[20] Z. Sen, "Spatial modeling principles in earth sciences", Springer (2009).
[21] M.J. Atallah, N. Konstantinos, J.R. Rice, E.E. Eugene, Secure outsourcing of scientific computations, *Advances in Computers*. **54**, 215-272 (2002).
[22] X. Lei, X. Liao, T. Huang, F. Heriniaina, Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud, *Information sciences*. **280**, 205-217 (2014).
[23] M. Nassar, A. Erradi, F. Sabri, Q.M. Qutaibah, Secure outsourcing of matrix operations as a service, *2013 IEEE Sixth International Conference on Cloud Computing* (2013).
[24] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, *International Conference on the Theory and Applications of Cryptographic Techniques* (1999).
[25] R. Agrawal, R. Srikant, Privacy-preserving data mining, *ACM Sigmod Record*. **29**(2), 439-450 (2000).
[26] H. Kargupta, et al., Random-data perturbation techniques and privacy-preserving data mining. *Knowledge and Information Systems*. **7**(4), 387-414 (2005).