Development of Security Stamp for Desktop Spatial Data Modification in Unrestricted Access Platform

RMM Pradeep[1#] and NTS Wijesekara[2]
[1]*Department of Information Technology, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka*
[2]*University of Moratuwa, Moratuwa, Sri Lanka*
[#]pradeep@army.lk

Abstract— *One of the challenges of the Desktop Spatial Data Security is when computing with tools developed with unsecured software. Modifications are often required especially in geographical databases, because of the continuous changes that take place in soil, slope, land cover and parcel boundaries. Therefore data security measures need to incorporate in mechanisms that enable the users to recognise the authenticity of the modified data. In the present work a new concept for data security is incorporated to validate the modification to a land use planning tool developed with the use of off-the-shelf GIS software. This concept incorporates a two-dimension security stamp using both the spatial attributes and non-spatial attributes of the geographic dataset, which in a unique encrypted identity for the corresponding user or user group. The security stamp developed using this concept was incorporated to a Geographic Storm-water Management Tool and tested for its success. This success was evaluated based on the probability of error occurrence in the stamp value. The security stamp enables pinpointing the data modifications that had been carried out without authority, enabling the users to avoid using security-breached data. The proposed concept identifies the changes incorporated to spatial data whether they are unintentional or intentional, hence falls into the category of "Responsible Citizen" tools.*

Keywords— *Unsecured GIS Software, Desktop Spatial Data Security, Digital Security Stamp*

I. INTRODUCTION

A. Background

Spatial data represents information about the physical location, characteristics and shape of geometric objects. These objects can be point features representing locations, line and polygon entities representing countries, roads, lakes etc. Furthermore the relationships between the geographic entities are usually stored as coordinates and topology ((ESRI, 2015), (MSDN, 2015)). The Geographic Information System (GIS) is a computer system that can be used to capture, store, query, analyse and display spatial data. In a GIS the associated spatial data are independent from the GIS software

B. Literature Review

Due to this independent thematic nature of spatial information, they are usually captured and manipulated by different organizations and are shared among the users (Morris, 2013). For an example, soil data are maintained by soil conservators, elevation and land cover information are prepared by survey department while land parcel data boundary data are maintained by local governments. These data are then shared for practical applications. But the absent of controllability over the data ownership, data originating organization may face difficulties when such user change the information and start to share the data set informing it is the original dataset (Sebake & Coetzee, 2013). Most of the research works on this issue are attempt to build either access control security or privacy of the spatial information in the same way they are used in relational or unstructured data sets ((Atluri & Chun, 2004), (Bertino et al., 2008), (Lin et al., 2008), (Sasaoka & Medeiros, 2006)). Nevertheless no research could be found on spatial data protection mechanism on protecting or auditing other than based on access control mechanism.

C. Requirement of Research

Present day off-the-shelf desktop GIS software such as ArcGIS, QGIS and Grass do not provide any inbuilt data security. Hence once a data layer is created with these GIS software it is not possible to track the changes other than carrying out a time consuming matching with the original data.

This security issue becomes one of the considerable challenges in spatial decision support systems, especially when the land ownership is involved in the associated changes. Therefore any intentional or unintentional changes of a spatial data would affect the ownership and this could be advantages or disadvantages. Hence, the requirement is to develop a data security mechanism

that enables the users to recognise the authenticity in GIS systems using desktop software.

D. Objective

The objective of the present work is to develop a new concept for data security which validates the spatial data modification in a land use planning tool that is an extension to the off-the-shelf GIS software.

D. Research Question and Hypothesis

It needed to research the data level conceptualization, creation, implementation and validation of spatial-oriented mechanism to track the unauthorised modifications. The present work believe that using a two-dimensional security stamp for each feature of the spatial data which generated using spatial and non-spatial attribute; can achieve data level security.

II. METHODOLOGY

A. Land Use Planning Tool

The most commonly used GIS software in Sri Lanka is ArcGIS (Wijesekera & Peiris, 2008), while the most valuable land information for the public are associated with individual properties. In case of stormwater generation due to land parameter changes, the most prominent is the urban land development by means of soil, land cover and elevation change. Perera & Wijesekera (2010) identified that the three most important parameters of a land parcel in case of stream flow generation are slope, soil and land cover. The other land parameter is important for a GIS is the shape. The overall methodology of the case study is shown in the Figure 1.

Accordingly the tool development was carried out to combine land parcel modification and stream flow generation concepts which working within the ArcGIS environment. Literature citing of GIS data security would not be found. Instead several guidelines on general databases were utilized to obtain the thinking trend in data security. ((Lin et al., 2008), (Thi et al., 2014), (Hu et al., 2014), (Malik & Sharma, 2011))

In this work a tool was developed as an extension to ArcGIS, to incorporate modifications to slope, land cover and soil which influence the surface runoff generation whilst the urbanization. The tool computes the changes in runoff generation due to land modifications using Rational Method and Unit Hydrograph concepts and allows users to incorporate a detention pit to control the Stormwater reaching the urban drainages and control the urban flash floods.

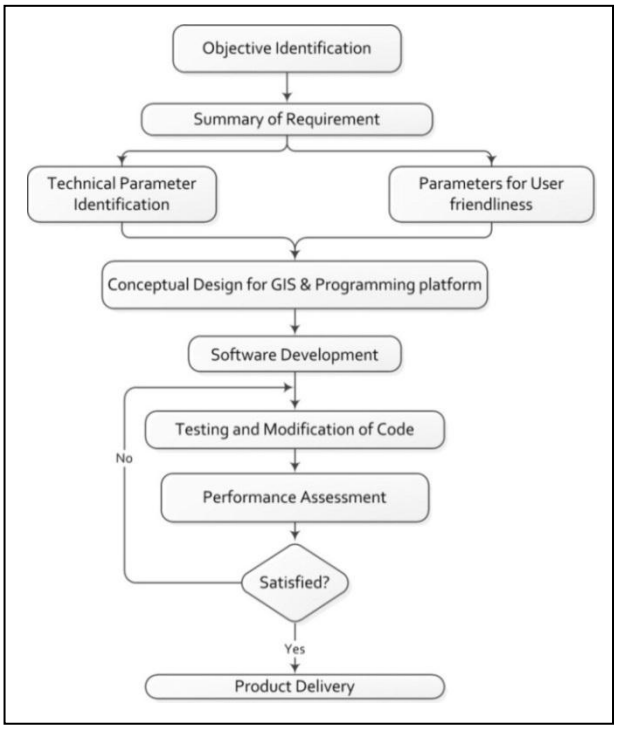


Figure 1: Overall Methodology

B. Achieving Spatial Data Security

The tool design incorporated two security considerations. The first concern is to secure the Tool from unauthorised access. The second is to embed a security stamp for manipulation of spatial data within the tool. As the tool is intended for spatial data security then security stamp design looked at imprinting the characteristics of spatial data.

1) Control the Access: Securing the tool was done by incorporating user credentials. Since the desktop GIS software does not contain security feature, it is necessary to seek a secure mechanism for storage (ArcGIS, 2015). In this tool, desktop database Microsoft Access and its encryption capability is utilized to store the user credentials. Based on Discretionary Access Control (DAC) the security of the tool was developed as shown in the Figure 2.

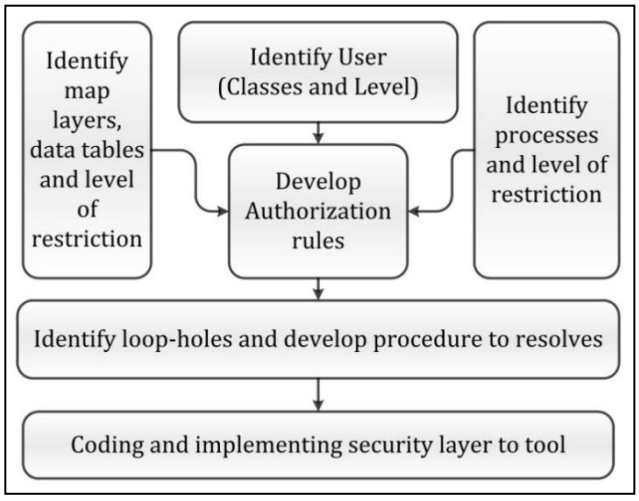


Figure 2: Concept of DAC Security Development

Two levels of users were identified as Administrator and Power User. Only administrator level users are permitted to generate the stamp value. When any other user incorporates modifications to the layers via the tool, a stamp value is automatically generated and stored. This component in the design is expected to look after the first security concern.

2) Inform the Security Breaches: For the second concern, tool was designed to inform the spatial data security breaches. The tool embeds the facility to keep the authenticated users informed about unauthorised changes in the spatial layers and to highlight the affected features

C. Security Stamp Algorithm

In the developed tool, an algorithm was developed to generate security stamp. This algorithm performs mathematical functions with spatial data (area and coordinates of centroid) and non-spatial data (assessment number and postal address) of features.

The mathematical function uses parameters combining their floating point values and ASCII codes to generate "Code Value" and then save as an attribute named "validate" in the spatial data set. The associated main steps are shown in the Figure 3.

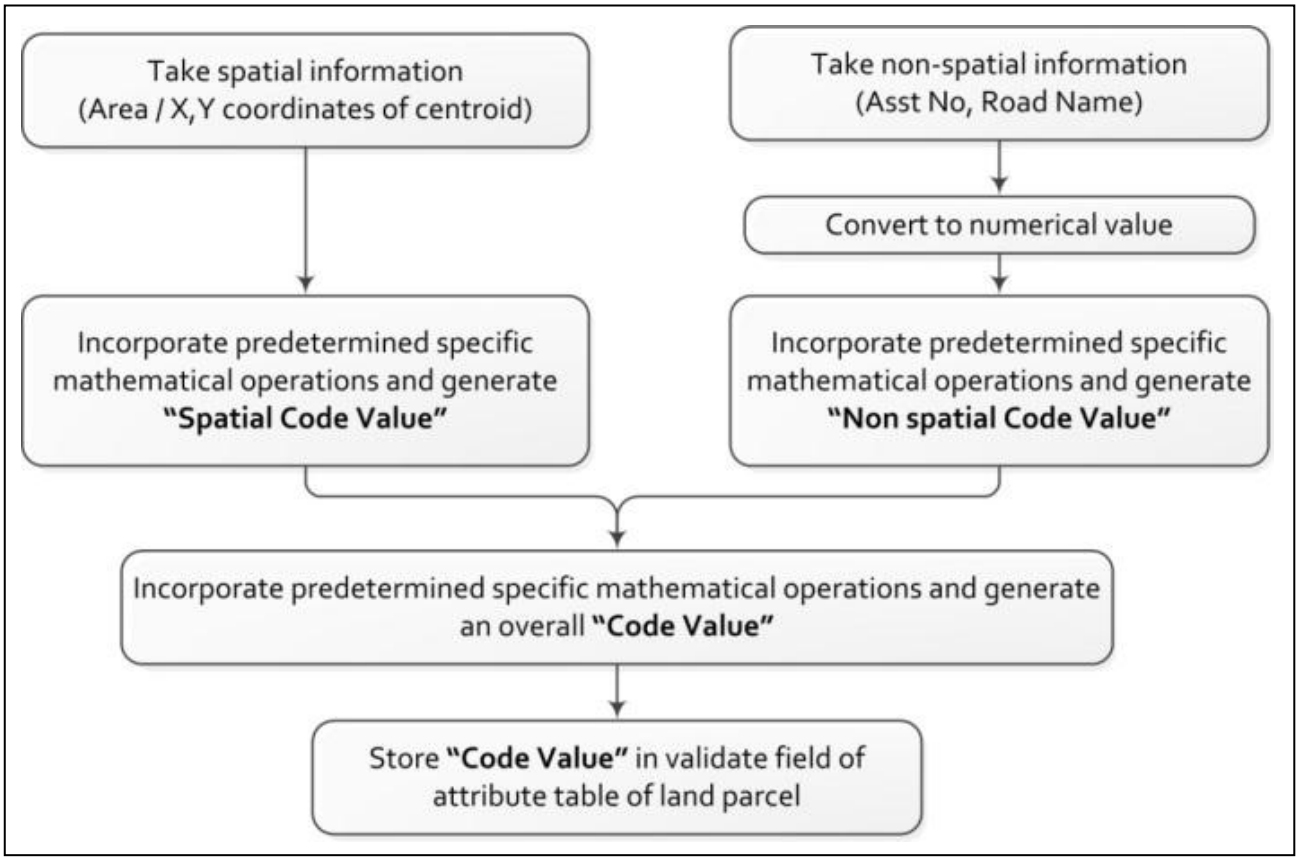


Figure 3: Stamp Value Generation Algorithm

At each execution the tool computes the stamp value using the geographic features and then compare with the "Validate" column. The mismatches point to unauthorised modifications carried out to the data layers without the use of the designed tool. Then it generates a message to inform the user to retrieve a fresh copy from the original (authenticated) data set and overwrite the manipulated data. The developed Visual Basic code for validation is as follows:

```
'loop for each feature of the table
Do While Not pFeat Is Nothing
   'retrieve size of the land parcel
   Set pArea = pFeat.Shape
   'i calculated using feature non-spatial attributes
   (ID,'Assessment number, road name)
   'and spatial attribute(area)
   i1 = Tan(pFeat.Value(fFid))
   i2 = Asc(pFeat.Value(fasstNo))
   i3 = Len(pFeat.Value(froadNAme))
   i4 = Sqr(pArea.Area)
   i = i1 + i2 - i3 * i4
   'get the centroid value of the land parcel
   cXY = pArea.Centroid.x + pArea.Centroid.y
   'combine centroid with non-spatial attribute
   '(feature ID)
   OutPut = Log(cXY) / Log(pFeat.Value(fFid)
   'generate final coded value
   i = i + Sqr(OutPut)
   calVal = Round(i, 8)
   'get the existing recoded value at field "Validate"
   dbVal = pFeat.Value(fValidate)
   'verify the values
   If pFeat.Value(fValidate) <>
                        pFeat.Value(fChkVal) Then
      'if does not match set the flag of unauthorised
      'access
      validateOK = False
      'Call the function to highlight the feature
      fun_HighlightFeature(fFid)
   End If
   'move to next feature
    Set pFeat = pValFeatureSet.NextFeature
Loop
```

D. Stamp Value Verification

A comprehensive study was done to verify the correctness of stamp value comparison. 1405 land parcels from the Sri Lanka Survey department's land parcel layer for Thimbirigasyaya Ward of Colombo Municipal Council, Sri Lanka were used for this activity.

To evaluate the spatial value generation capability, altogether 50 random land parcels were modified on three occasions and compare the pre and post stamp values as in Table 1.

The security stamp value need to have sufficient resistance to the possibility of guessing. In tool testing, this aspect was evaluated by analysing the correlation of the stamp value with spatial information or non-spatial information which were utilised in the stamp value generation. Then it evaluated the level of correlation between 1405 land parcels' stamp values and attributes.

III. RESULTS

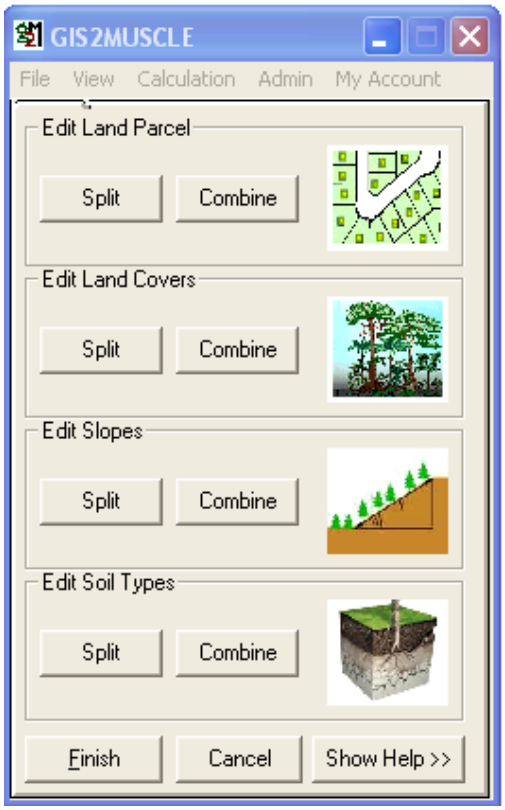


Figure 4 : GIS2MUSCLE Main Interface

The developed tool for land use planning was named as, Geographic Information System to Manage Urban Stormwater Considering Land Enhancement (GIS2MUSCLE). The tool is an easy to use tool compatible with ArcGIS versions from 9.0 to 9.3. The tool demonstrates the security incorporation to an off-the-shelf general use GIS software and independent spatial data. (Figure 4).

The tool facilitates two level users, Administrator and Power User with added functions to the Administrator (Figure 5).

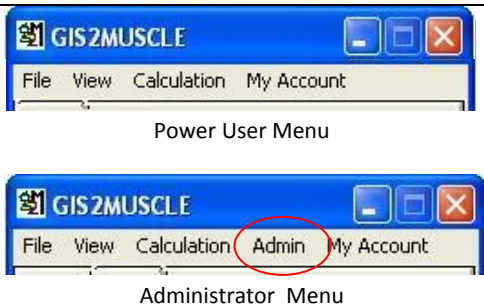


Figure 5 : Administrator and Power user Menu

Based on the spatial data security manipulation, the Administrator is given the rights to place new stamp values ("Encode Layer") to either existing or new spatial data layer and check the stamp value for validity in any time("Check for Validity") as shown in the Figure 6.

The generated stamp values are stored in the "Validate" attribute of the Land Parcel Layer (Figure 7).

Figure 6 : Administrator menu item for stamp manipulation

FID	Shape *	ID	ASST_NO	ROAD_NAME	Validate
0	Polygon	0	117	Havelock Road	-405.668091
1	Polygon	0	0	Vacant Lot	-185.777754
2	Polygon	0	40	Thimbirigasyaya Road	-376.837281
3	Polygon	0	56	Thimbirigasyaya Road	-383.652255
4	Polygon	0	83	Havelock Road	-47.658765
5	Polygon	0	17	Thimbirigasyaya Road	-108.133028

Figure 7 : Attribute table of the Land Parcel Layer of Thimbirigasyaya Ward of Colombo MC

Except that the tool able to display an error message and highlights features which are modified without authority when logon to the tool or at the access of "Check for Validity" menu item (Figure 8).

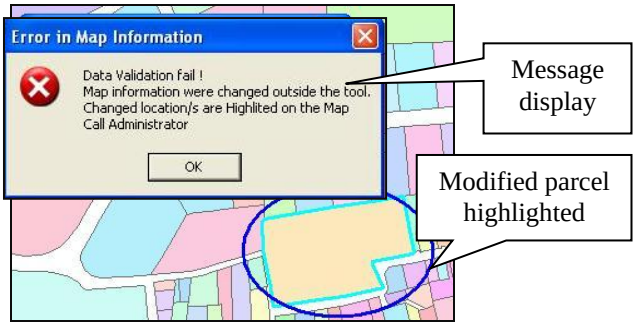
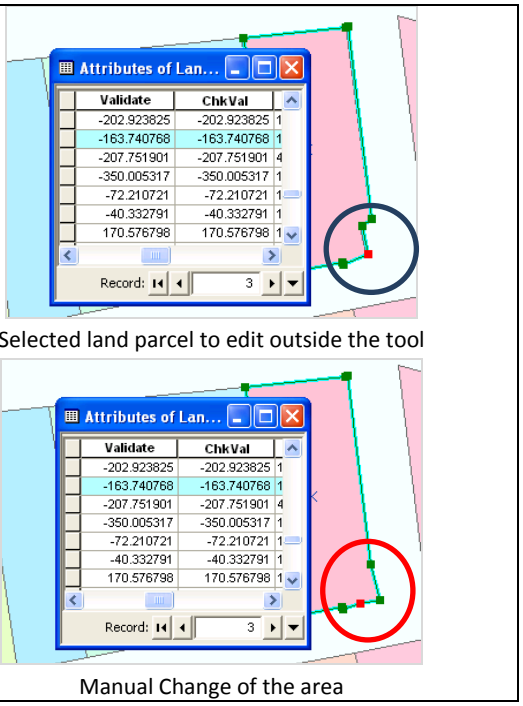


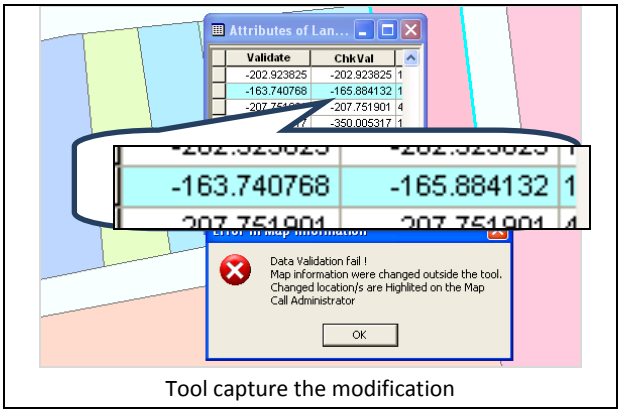
Figure 8 : Notification of Modifications Outside the Tool

Further evaluation result shows the application of the security algorithm with 100% accurate stamp value generation (Table 1). A sample land area modification steps screen shots are shown in the Figure 9.

Table 1. Sample Modification verification

Modification to geospatial data	No of random land parcels	Identification with security stamp disparity
Non spatial values	15	100%
spatial values	15	100%
Combination of spatial and non-spatial values	20	100%
Total	50	100%





Tool capture the modification

Figure 9 : Capturing of the unauthorised land area modification

When it consider the attributes' correlation with the stamp values, it observed, a presence of very weak uphill or downhill linear relationship except the area parameter as shown in the Table 2. Distribution of the stamp values over the Area, ASCII of Assessment Number, ASCII of Road Name, X coordinate of Centroid and Y coordinate of Centroid are shown in the Figure 10, 11, 12, 13 and 14.

Table 2. Correlation between stamp value and value used to generate stamp value

Parameter	Correlation with stamp value
Area	-0.865565049
x Coordinate	-0.013764352
y coordinate	-0.192503765
Assessment Number	0.054177663
Road Name	0.075696388

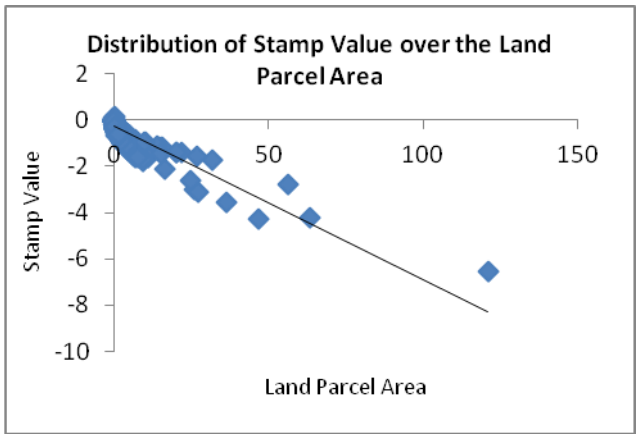


Figure 10: Distribution of stamp value over Land Parcel Area

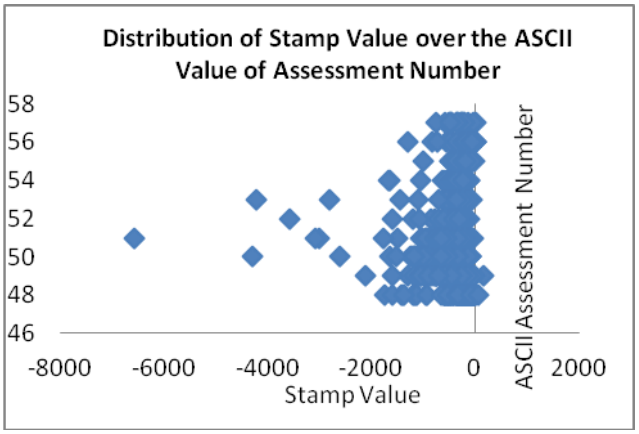


Figure 11: Distribution of stamp value over ASCII – Asst No

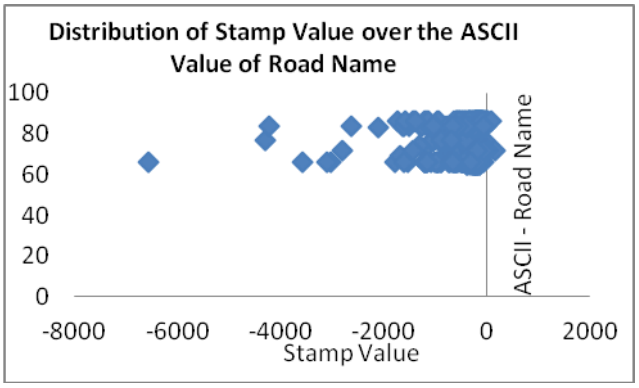


Figure 12: Distribution of stamp value over ASCII – Road Name

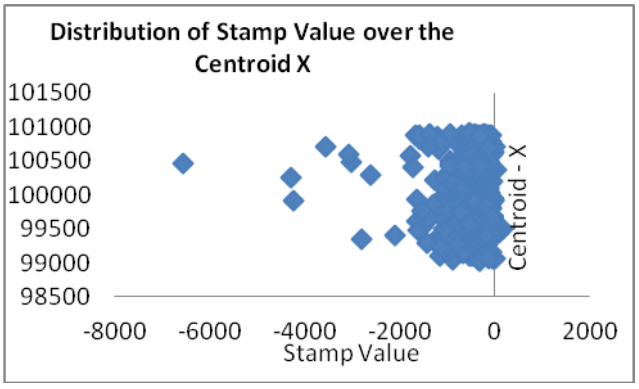


Figure 13: Distribution of stamp value over X-Coord of Centroid

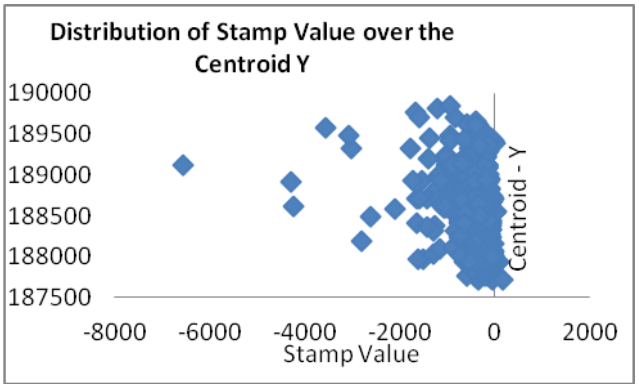


Figure 14: Distribution of stamp value over Y-Coord of Centroid

IV. DISCUSSION

The present work proposes a model for desktop spatial data security and demonstrates by developing a land use planning tool. The model proposes a security stamp to be generated based on the spatial and non-spatial and record the value in the attribute table of the each feature.

In the work, it used a simple mathematical algorithm to generate the stamp value and study shows the correctness of the stamp value over the modifications. Nevertheless, it observed a strong liner correlation between stamp value and Area of features which increases the probability of guessing the stamp values. However this would be minimised by improving the stamp value generation algorithm.

V. CONCLUSION

The present work able to demonstrate the capability of providing spatial data security using spatial and non-spatial attributes of the data.

The proposed concept's major feature is, it does not prevent editing spatial data but recognises pilferage and warns the users though its capability to identify the intentional or unintentional modifications made. Then through this concept a value is given to all the users and shows them they are responsible citizens.

Finally it expects this model opens a new research area that is security for spatial data in unrestricted access platform.

REFERENCES

ArcGIS, 2015. *ArcGIS for Desktop Best Practices*. [Online] Environmental Systems Research Institute, Inc. Available at: http://doc.arcgis.com/en/trust/security/arcgis-desktop-best-practices.htm [Accessed 12 May 2015].

Atluri, V. & Chun, S.A., 2004. An Authorization Model for Geospatail Data. *IEEE Transactions on Dependable and Secure Computing*, I(4), pp.238-54.

Bertino, E., Gertz, M., Thuraisingham, B. & Damiani, M.L., 2008. Security and Privacy for Geospatial Data:Concepts and Research Directions. In *SPRINGL '08 Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*. NY, USA, 2008. ACM.

ESRI, 2015. *GIS Dictionary*. [Online] Available at: http://support.esri.com/en/knowledgebase/GISDictionary/term/spatial%20data [Accessed 1 June 2015].

Hu, V.C. et al., 2014. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. Standards and Guidelines. Maryland: National Institute of Standards and Technology U.S. Department of Commerce.

Lin, J., Fang, Y., Chen, B. & WU, P., 2008. Analysis of Access Control Mechanisms for Spatial Database. In *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences.* Beijing, 2008. International Society for Photogrammetry and Remote Sensing.

Malik, M. & Sharma, A.K., 2011. Data Security and Access Control for Geospatial Database sets Using Novel StegoHash Algorithm. *IJCA Special Issue on Network Security and Cryptography NSC*, Number 2, pp.4-10.

Morris, S., 2013. *ISSUES IN THE APPRAISAL AND SELECTION OF GEOSPATIAL DATA*. Online Resource. Washington, D.C: National Digital Stewardship Alliance.

MSDN, 2015. *Spatial Data (SQL Server)*. [Online] Available at: https://msdn.microsoft.com/en-us/library/bb933790.aspx [Accessed 1 June 2015].

Perera, K.R.J. & Wijesekera, N.T.S., 2010. Identification of the Spatial Variability of Runoff Coefficient of Three Wet Zone Watersheds of Sri Lanka for Efficient River Basin Planning, Environmental & Water Resources Institute (EWRI) of American Society of Civil Engineers. In *3rd*

International Perspective on Current & Future State of Water Resources & The Environment. India, 2010.

Sasaoka, L.K. & Medeiros, C.B., 2006. Access Control in Geographic Databases. In J. Roddick et al., eds. *Lecture Notes in Computer Science: Advances in Conceptual Modeling - Theory and Practice*. Berlin : Doi: 10.1007/11908883_14 (Springer). pp.110-19.

Sebake, M.D. & Coetzee, S., 2013. Address Data Sharing: Organizational Motivators and Barriers and their Implications for the South African Spatial Data Infrastructure. *International Journal of Spatial Data Infrastructures Research*, VIII, pp.1-20.

Thi, K.T.L., Thi, Q.N.T. & Dang, T.K., 2014. An Enhanced Access Control Model for GIS Database Security. *ASEAN Engineering Journal Part D*, III(No 1), pp.40-51.

Wijesekera, N.T.S. & Peiris, T.C., 2008. The Status of RS/GIS/GPS Application in Sri Lanka – A Survey of Public Private and Non Governmental Organizations. *Engineer Journal of the Institution of Engineers*, (Special Issue on Geoinformatics Applications), pp.1-10.

BIOGRAPHY OF AUTHORS

RMM Pradeep is a lecturer at General Sir John Kotelawala Defence University. He received his B.Sc. Degree in Management Information Systems from the University of Ireland. He also holds a M.Sc. degree in Geoinfomatics from the University of Moratuwa. He is interested in the field of Engineering Application Development and Information Security.