Integration of the Visual Authentication of Spatial Data with Spatial-Temporal Class Taxonomies for Advanced Spatial Authentication Modeling to Create *Pretty Good Security*

*Vert, G., **Gourd, J., *Iyengar, SS.
*Dept. of Computer Science, LSU, Baton Rouge, LA 70809
**Dept. of Computer Science, LaTech, Ruston, LA 70809

e-mail: gvert12@csc.lsu.edu

Abstract **–** Due to the criticality of spatial data in decision making processes that range from military targeting to urban planning it is vital that transmission of spatial data be authenticable and secure. Cryptographic methods can be utilized for this purpose, however they can be relatively slow, especially when encrypting voluminous quantities of data such as is found with spatial data. Previously a promising and fast method of low overhead spatially based visual authentication has been developed. This method considered the angular and temporal relationships of spatial object data. It was initially shown to be extremely fast and easily extended to an intuitive visual algebra that makes it easy for a human being to identify modifications to data such as deletion, movement or additions of spatial objects. Additionally, work was done to taxonomically classify spatial objects based on their spatial and temporal properties. This paper integrates the two approaches to i) introduce a new concept in security that of *pretty good security* ii) potentially dramatically increase the speed of the authentication method on top of the visual signature authentication methods developed previously. The approach integrates the notion of spatial and temporal taxonomic relationships when determining what key spatial objects should be authenticated.

1.0 INTRODUCTION

Spatial data sets or maps get transmitted over the Internet all the time for planning processes and decision-making support ranging from resource management to urban planning [1,2,3,8,11]. This highlights the need to create techniques to protect and secure the transmitted spatial data. Authentication is a method of determining whether a data item has been modified. It enables computers at the receiving end to verify the contents of the message. [4, 5] Authentication can range from simple functions such as using passwords to very complicated identifiers. Advanced approaches to authentication may increase the amount of authentication needed based on the perceived risk associated with accessed resources. This is referred to as risk based authentication.

In this paper an approach to authentication based on determining what is important to authenticate based on spatial temporal category relationships is presented. A previously developed visual method for authentication of spatial data is integrated with taxonomically based spatial-temporal classifications to improve the authentication speed of the visual authentication method. This method can create ultra fast authentication where only relevant parts of the spatial data based on taxonomic relationship are authenticated. The result is defined as *pretty good security* and has the potential to be considerably faster than currently existing methods.

1.1 Background

Encryption is a widely utilized method to authenticate and protect data. There are many encryption techniques available and commonly used such as systematic encryption, and Public-Key encryption. When one considers the application of such methods to spatial data there are several questions that must be considered:

- cryptographic algorithms tend to be designed to work on relatively small amounts of data and thus can be computationally expensive.
- when considering the application to spatial data, the question often becomes which data needs to be encrypted and thus does all data need to be encrypted.

Very little work appears to have been done on the development of authentication methods based on properties describing spatial data. This has became the motivation for the development of a new method for doing spatial data authentication inspired from the concepts of biometrics. This approach utilizes taxonomically related classes of spatial information to select subsets of spatial objects and a visualized mathematical model to generate a geometric signature for the data sets that can be used for authentication and can visually point to modified objects in a spatial dataset. The approach is based on the spatial and temporal properties of objects. The result is a method that can be ultra fast and selective in what is authenticated.

2.0 PREVIOUS WORK

In previous work, the notion of visual authentication of spatial objects has been developed [6]. Additionally, the concept of spatial taxonomic classes of objects was defined based on their temporal and spatial properties defined in other work [12,13,14]. This section presents an overview of this work to set the grounds for their unification into an authentication scheme based on the integrations of the ideas.

The question of how to identify spatial objects for authentication signatures is based on research similar to the classification categories of Peuquet [2]. Our research extended this previous work to classify spatial objects based on the effect time has on them. That means every object was studied with respect to time, and what changes can occur to that object due to time. We define the term degree of temporality as being how long it takes an object to change its spatial geometry and define this concept as:

$$\textit{Degree of temporality} = \frac{\Delta\ \textit{Spatial Geometry}}{\textit{Time}}$$

From this definition, we derived the following classifications for objects:

- temporal continuous (TC) – an object whose degree of temporality and attributes change continuously
- temporal sporadic (TS) – an object whose degree of temporality and attributes change in an unpredictable fashion
- static (S) – an object that has no change in degree of temporality or attributes
- Static-temporal (ST) – an object that is typically static, but may—under certain situations—have changes in degree of temporality and attributes

The following presents a sample summary of some spatial objects and how they may fit into these classifications.

Static	***Stati c-Tem poral***	***Temporal-Continuous***	***Temporal-Sporadic***
Ocean	Sea	Ice Mass	Port
Island		Desert water	Land
Rocks		Shore	Farm
Forest		Sand	Park
Summit		Silt	University
Mounta in		Clay	Parcel data
Hill		Bushes	Corral
Valley		Lake	Dam/Weir
		River	Mines

Table 1. Temporality classification of the taxonomy

3.0 USING A VISUAL GLYPH TO AUTHENTICATE SPATIAL DATA

Visual authentication can be a fast method to create an authentication signature compared to encryption because the algorithmic complexities of trigonometric mathematics are simpler than encryption algorithms. The following section therefore presents the development of a visual authentication method that can be applied to spatial data.

3.1 Spicule Visualization Tool

Takeyama and Couclelis have shown that GIS layering abstraction of a location is equivalent to a set of multiple attributes [9]. So, the map can be looked at as a 3D-set of layers on top of each other. In this 3D paradigm of layered spatial data, the Spicule can be utilized to create a mathematical signature for authenticating spatial data by mapping the tips of vectors on the Spicule to the unique spatial objects identified from the taxonomy. The signature that can be generated using this approach becomes an n-tuple which can be visually subtracted using the Spicule to detect changes in the spatial data.

The Spicule was developed [6,7] as a tool for detecting intrusions on computer systems of malicious software and individuals. It is a visually based glyph that has a strong mathematical foundation based in linear algebra. As a research tool, it is still being investigated for application to a wide area of pattern recognition problems. One of the interesting properties of the Spicule is that it has a simple but powerful algebra that allows rapid visualization and detection of changes in data sets that the Spicule has been mapped onto [6,7]. Thus the mathematics of the Spicule can be utilized to authenticate and detect changes in the relative geometries of spatial objects

To illustrate the Spicule concept consider Fig. 1 and Fig 3. In these figures one observes a ball floating in 3-D space. This ball has—attached to its circumference—vectors that can be mapped onto objects in 3-D space such as spatial objects found in spatial data. As an example, the tip of H vector may be mapped onto the specific intersection of a street system that has been classified as a static temporal object. The Spicule has a variety of different vector types, each with its own unique properties. In the figure, a new type of vector is defined. This vector is based at the equator of the Spicule's main ball and has the head of the vector mapped to spatial objects in a data set. When considering this scheme it is fairly straight forward to see that such a mapping can create a series of vectors each with a unique mathematical description of orientation, angle and direction. This descriptive information constitutes the authentication signature for the transmitted spatial data.

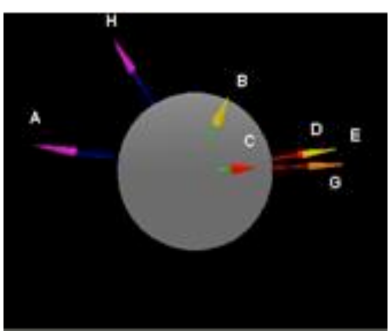

Fig. 1, Sample Spicule glyph

In Fig. 2, an example of how a Spicule might map onto significant spatial features found in various GIS data layers is shown. In this illustration, layer one may represent a street system, layer two may represent the distribution of forested areas, and layer three may represent houses. Each vector on the Spicule has a unique set of descriptive attributes such as vector magnitude, vector angular orientation, and location of a vector on the 3-D central ball. A vector's descriptive orientation can then become a signature of the spatial object it has been mapped onto [10].

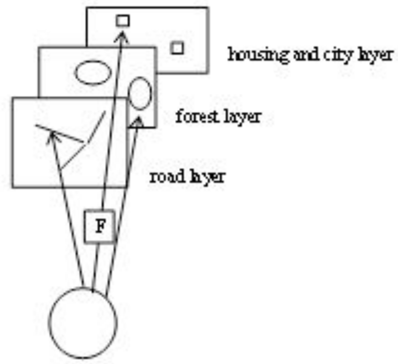

Fig. 2, Sample mapping of Spicule glyph to features in GIS spatial data

The current form of descriptive signature equation is given by:

$V = V_1 + V_2 + \ldots Vx$

Where Vx is given as:

Vx = (|Vx|, elevation, equatorial location)

where:

|Vx| - magnitude
elevation - angular degree's above horizontal
equatorial location - angular degree of vector tail when mapped on the Spicule ball

This signature creates a unique description of the orientation of a spatial object within the 3D data space.

In this scheme a vector pointing from the center of the Spicule, at the origin, to each point or spatial object selected from the taxonomic spatial temporal plot to create a signature. The n-level data layers shown in Fig. 2 are initially proposed to be placed at one vertical unit apart from the Spicule layer. So, the first layer points will have coordinates of (x, y, 1), the second layer points' coordinates will be (x, y, 2), and the third layer points' coordinates will be (x, y, 3). Based on this the vector attributes for each authentication point in the three layers will be:

$$Mag_i = \sqrt{x^2 + y^2 + i^2} \qquad (1)$$

where:

i is the data layer number.
x, y are point original coordinates.
Mag_i is the magnitude of the vector from (0,0,0) to a point in layer i .

$$Sin\theta_{ei} = \frac{x}{\sqrt{x^2 + y^2}} \Rightarrow \theta_{ei} = Sin^{-1}\frac{x}{\sqrt{x^2 + y^2}} \qquad (2)$$

$$Sin\theta_{vi} = \frac{i}{\sqrt{i^2 + y^2}} \Rightarrow \theta_{vi} = Sin^{-1}\frac{i}{\sqrt{i^2 + y^2}} \qquad (3)$$

Equations (2) and (3) are used to calculate the equator and the vertical angles respectively,

where:

i is the data layer number.
θ_{vi} is the vertical angle degrees for a vector from (0,0,0) to a point in layer i .
θ_{ei} is the equator angle degrees for a vector from (0,0,0) to a point in layer i .

The collection of attributes and angles for all authentication vectors forms a two-dimensional matrix that is used ~~as~~ for the authentication signature and the Spicule visualization authentication process (Fig. 5).

The signature calculation process is done when a spatial dataset is requested to be transmitted over the internet. Table 2 shows a sample calculated vector matrix.

Object ID	Layer	Mag_i	θ_{vi}	θ_{ei}
1	3	7.68	66.8	18.43
2	2	16.31	42.51	4.76
		. .	. .	. .
n	i	29.22	51.95	3.18

Table 2. Sample calculated vector matrix

At the receiving end, the same process to create a signature matrix from the received spatial dataset was applied. By visualizing the mathematical *difference* between the received spatial data sets matrix and the transmitted matrix, as shown in Fig. 3, it can be determined if the dataset has been intercepted or altered during transmission. If no modifications have been made, the result is a featureless, smooth ball. In Fig. 3 the resulting vector points to an object that has been modified.

4.0 COMPARATIVE AUTHENTICATION SIGNATURE GENERATION PERFORMANCE

Spatial data may be protected for transmission by encryption or by the generation of a signature using MD5, SHA or RIPEMD. In order to compare the performance of the spatial signature approach to that of above traditional methods a test suite was set up on a PC running at 2.4ghz with a P4 processor. The Crypto++ package was utilized for comparison with timing figures measured down to the millisecond. Crypto++ has a program called Cryptest that may be called with command line switch to encrypt symmetrically, decrypt and generate SHA, MD5 and RIPEMD160 digests. The comparative speeds from this initial performance testing are shown in table 3.

Test Type	Pass 1 (10x)	Pass 2 (10x)	Pass 3 (10x)
Shell	63.00	58.00	57.00
Encrypt (symmetric)	126.60	123.4	121.90
Decrypt (symmetric)	115.60	123.5	121.90
MD5/SHA/RIPEMD	67.20	67.20	64.00
Spatial Authentication	< .01 millisecond	< .01 millisecond	< .01 millisecond

Table 3 Average performance comparison of Spatial Authentication versus Symmetric encryption, SHA, MD5, RIPED (milliseconds) on test data

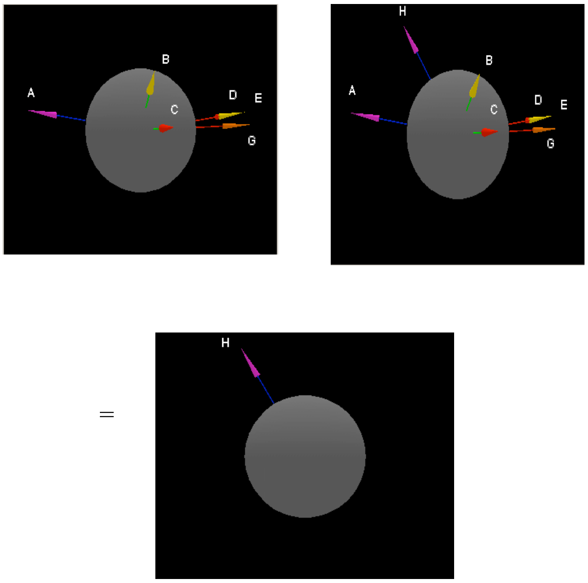

Figure 3. Visualization of authentication signature: Template form (left) – Authentication form(middle) = Change form indication H has been added to the transmitted data set generating the Authentication form

5.0 SELECTIVE AUTHENTICATION

Not all spatial or temporal objects need to be authenticated. This is due to the fact that some objects may not have a strong relationship to objects in another taxonomic class. For instance, static objects may not be related to objects that are continuously changing. This observation leads to the notion that i) authentication can be done based on taxonomic classes of objects that are of interest to a user, ii) partial authentication can reduce the already fast authentication speeds from the visual approach. This term is referred to as *pretty good security*. The selection of what is authenticated becomes a function of the *relationship among objects* and thus can be defined by the user and is a subject for further research.

Such an approach is suggested via the implementation of a similarity matrix that has the following format:

	S	ST	TC	TS
S	1	.75	.5	.25
ST	.75	1	.75	.5
TC	.50	.75	1	.75
TS	.25	.50	.75	1

Table 4, Similarity matrix of taxonomic classes utilized for object authentication

where the taxonomic classes are abbreviated as defined previously. In the above matrix, a hierarchy of relationships among classes defined in the spatial-temporal taxonomy are defined. A value of one indicates absolute relationship and lower values indicate less relationship. This hierarchy can then be utilized to determine by a user what objects (from Table 1) in a spatial data set should be authenticated using visual signatures. For example, if a user wants to only visually authenticate objects that are Static (S), such objects {ocean, islands, rocks,..} would be used in the visual authentication process. Whereas if a user wanted to authenticate all objects that are greater than or equal to .75 (a high degree or relation) then the objects in the ST and S classes would be authenticated. The result is that a user can select to authenticate only highly related objects and thus increase the already fast authentication times shown previously for the visual authentication method. In this similarity matrix the class relations are split evenly due to there only being four classes at the present in the spatial-temporal taxonomy. However, this approach in the future should be studied to determine better adaptive schemes for given security situations that might be applied to the similarity matrix.

6.0 CONCLUSION AND FUTURE WORK

The integration of the visual authentication method with taxonomic classes can provide for dramatic increases in the speed of authentication based on the new notion of authentication of only spatial-temporal objects that are related. This concept is referred to as *pretty good security*. This work builds on previously defined research topics in the area of spatial authentication. The level of confidence in the authentication is left up to the user and should be the subject of future empirical work. Other work could involve the study of dynamically changing relationship values, how they might be defined dynamically and the effect on speed. Additionally, this method has terrific potential in the newly developing paradigm of a global information system based on spatial temporal relationships among data objects and global contextual processing.

REFERENCES

[1] ESRI Data & Maps, Media Kit. 2002. Esri ArcGIS. www.esri.com

[2] "An Introduction to Geographical Information Systems", by Ian Heywood, Sarah Cornelius,

and Steve Carver. Second Edition, 2002. Prentice Hall.

[3] Environmental Modeling Systems, Inc. WMS 7.1 Overview. http://www.ems-i.com/WMS/WMS_Overview/wms_overview.html

[4] William Stallings. 2003. Network Security Essentials, Applications and Standards. Prentice Hall.

[5] Charlie Kaufman, Radia Perlman, Mike Speciner. 2002. Network Security, Private Communication in a Public World. Prentice Hall PTR.

[6] Vert, G. Yuan, B. Cole, N. A Visual Algebra for Detecting Port Attacks on Computer Systems, Proceedings of the Intl. Conf. on Computer Applications in Industry and Engineering (CAINE-2003), November 2003, Las Vegas, NV, pp 131-135.

[7] Alexandria Digital Library Feature Type Thesaurus. University of California, Santa Barbara. Version of July 3, 2002. http://www.alexandria.ucsb.edu/gazetteer/FeatureTypes/ver070302/index.htm

[8] Introduction to ArcView 3.x. ESRI Virtual Campus, GIS Education and Training on the Web. http://campus.esri.com/

[9] Takeyama, M., and Couclelis, H., 1997, Map dynamics: integrating cellular automata and GIS through Geo-Algebra. *International Journal of geographical Information Science* 11: 73-91.

[10] Jensen, C.S., and R. Snodgrass. 1994. Temporal Specialization and Generalization. *IEEE Transactions on Knowledge and Data Engineering* 6(6): 954-974.

[11] Onsrud, H.J., and G. Rushton. 1995. Sharing Geographic Information. Center For Urban Policy Research, New Brunswick, N.J. 510pp.

[12] Guimaraes, G., V.S. Lobo, and F. Moura-Pires. 2003.A Taxonomy of Self-Organizing Maps for Temporal Sequence Processing. *Intelligent data Analysis* 4:269-290.

[13] Heaton, Jill. Class lecture. University of Nevada, Reno. 08/23/2004.

[14] Calkins, H. W.; Obermeyer, N. J.; Taxonomy for Surveying the Use and Value of Geographical Information. *International Journal of Geographic Information Systems* V. 5, N. 3, July-September 1991, pp. 341-351.