Signing individual fragments of an RDF graph of unique Bulgarian bells

Galina Bogdanova
Todor Todorov, Nikolay Noev

Institute of Mathematics and Informatics, BAS

Signing individual fragments of an RDF graph of unique Bulgarian bells

The aim of the presented article is to study signing of RDF graph fragments in semantic web.

This paper is upgrade of our work on archive of unique Bulgarian bells, which is part of the project "Research and Identification of Valuable Bells of the Historic and Culture Heritage of Bulgaria and Development of Audio and Video Archive with Advanced Technologies" (BELL).

- To accomplish this we have to:
  - develop semantic web and ontology of digital resources of BELL project;
  - signing RDF graphs fragments in semantic web of bells.

- The main tasks of this work are:
  - indexing the media resources in digital archive;
  - making an ontology using OWL, RDF technology;
  - applying a sign in fragments of an RDF graph.

Signing individual fragments of an RDF graph of unique Bulgarian bells

- Some previous work:
  - 2004 - 2009, work on BELL project;
  - 2006, G. Bogdanova, T. Trifonov, T. Todorov, and Ts. Georgieva, Methods for Investigation and Security of the Audio and Video Archive for Unique Bulgarian Bells;
  - 2007, G. Bogdanova, T. Todorov, Ts. Georgieva, Algorithms for security and analization of experimental multimedia archive;
  - 2008, T. Berger, T. Todorov, Improving the Watermarking Process With Usage of Block Error-Correcting Codes;
  - 2008, G. Bogdanova, Ts. Georgieva, Using Error-correcting Dependencies for Collaborative Filtering;
  - 2009, G. Bogdanova, T. Todorov and N. Noev, Organization and Security of the Audio and Video Archive for Unique Bulgarian Bells.
- Some related papers:
  - 2003, J. Carroll, Signing RDF graphs;
  - 2005, G. Tummarello, C. Morbidoni, D. Kourtesis, F. Piazza and P. Puliti, Toward MUI: Ontology assisted global identification of Audio Resources;
  - 2005, G. Tummarello, Ch. Morbidoni, P. Puliti and F. Piazza, Signing individual fragments of an RDF graph.

Signing individual fragments of an RDF graph of unique Bulgarian bells

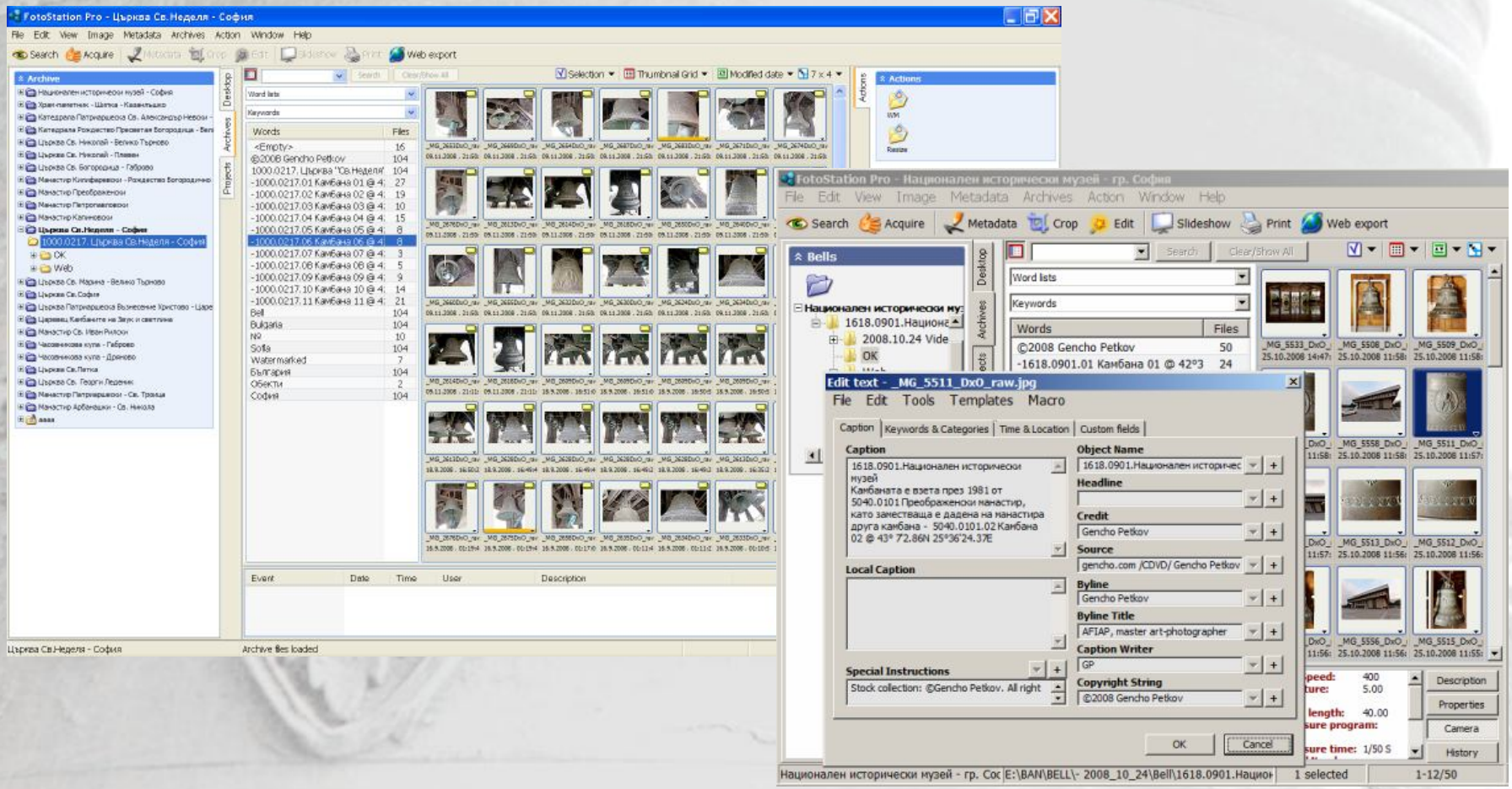
The archive of BELL contains:

- Digital data
  - More than 3 000 digital records with added digital steganographic sign (invisible watermark);
  - including photo pictures, video clips, audio records;
  - technical data, historical references, passports, diagrams etc.

- Organization of the BELL archive:
  - Tree file structure;
  - Digital files format, parameters, coding;
  - Specific signature for file name;
  - Additional META textual data for indexing of media files:
    - Title (name of subject);
    - Creator (name of digitalizer);
    - Description (additional data);
    - Date (date of creation);
    - Type (type of media);
    - Format (file format, codec and parameters);
    - Identifier (geographic coordinates);
    - Rights (owner of property rights).

Signing individual fragments of an RDF graph of unique Bulgarian bells

Fully functional BELL archive with added META data, actions and security settings:



Signing individual fragments of an RDF graph of unique Bulgarian bells

Semantic web

- The **Semantic Web** is an opportunity to redefine, or perhaps to better define, all the content and applications on the Web. It is mainly used to describe the model and technologies proposed by the W3C.

  These technologies include a variety of data interchange formats and notations such as:

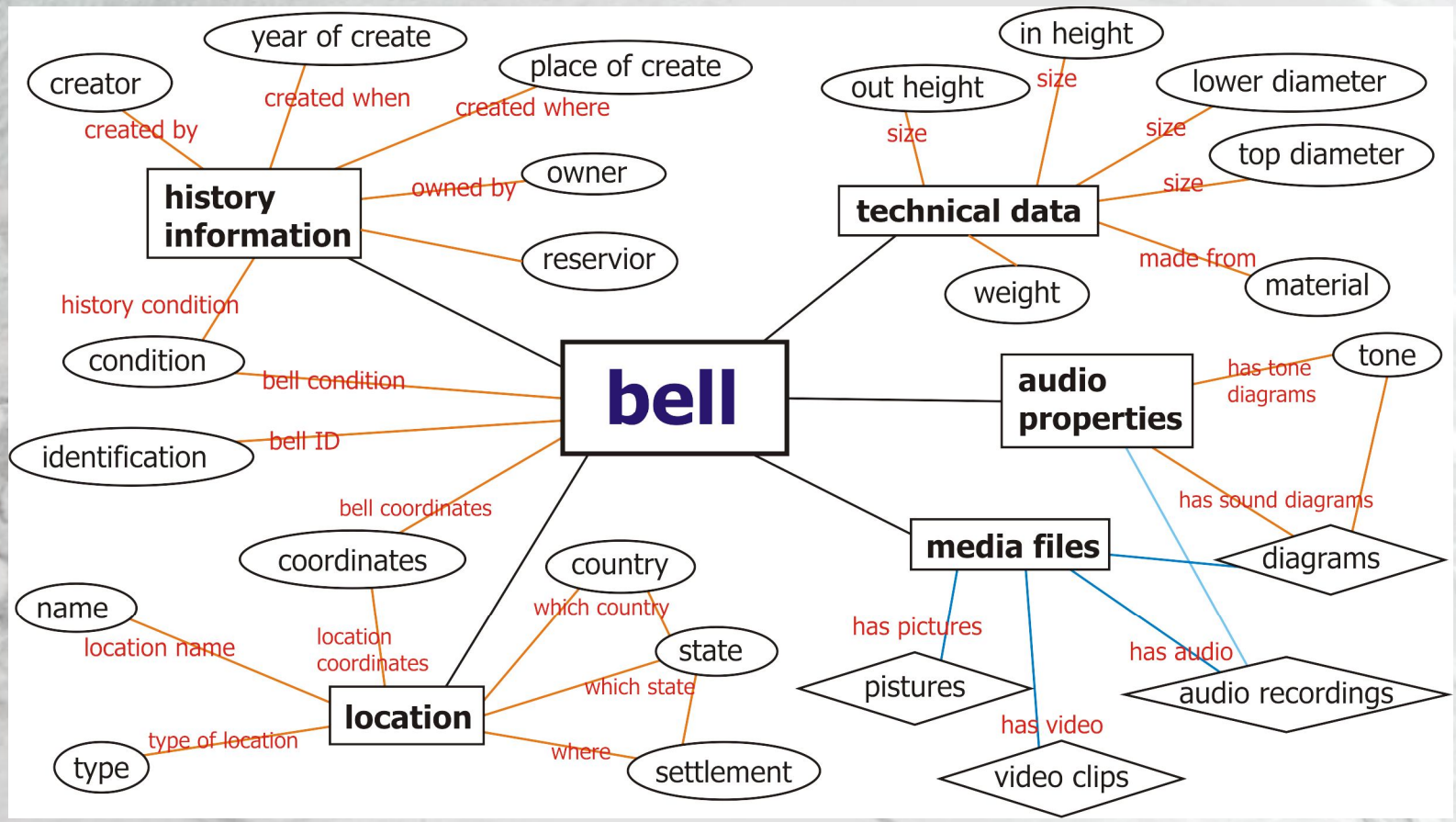
  – RDF – Resource Description Framework;
  – RDFS – RDF Schema;
  – OWL – Web Ontology Language.

  All of which are intended to provide a formal description of concepts, terms, and relationships within a given knowledge domain.

  The data described by an **ontology** in the OWL family is interpreted as a set of "individuals" and a set of "property assertions" which relate these individuals to each other. An ontology consists of a set of axioms which place constraints on sets of individuals (called "classes") and the types of relationships permitted between them. These axioms provide semantics by allowing systems to infer additional information based on the data explicitly provided.

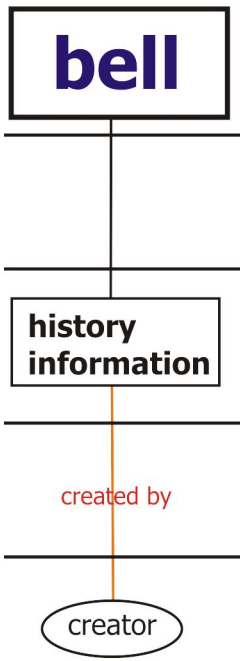
Signing individual fragments of an RDF graph of unique Bulgarian bells

The basic ontology schema of annotation, that we use to define a bell content:



Signing individual fragments of an RDF graph of unique Bulgarian bells

Some basic definitions used in building ontology:



Description	RDF Declaration of resources
main ***bell*** resource linked with property ***history information***	«**RDF:Description** RDF:ID="*bell*"» «**RDF:type RDF:resource**="*#bell*"» «**/RDF:Description**»
connection between ***bell*** resource and ***history Information*** property	«**RDF:Property** RDF:ID="*history-information-property*"» «**RDFS:domain RDF:resource**="*#bell*"» «**RDFS:range RDF:resource** "#bell"» «**/RDF:Property**»
history information property of ***bell*** resource, linked with ***creator*** property and ***created by*** axiom	«**RDF:Description** RDF:ID="*history-information*"» «**RDF:type RDF:resource**="*#history-information*"» «**RDFS:subClassOf RDF:resource** "#bell"» «**/RDF:Description**»
created by axiom between ***history information*** property and ***creator*** property	«**RDF:Property** RDF:ID="*created-by*"» «**RDFS:domain RDF:resource**="*#history-information*"» «**RDFS:range RDF:resource** "#bell"» «**/RDF:Property**»
creator property, subproperty of ***history information*** property	«**RDF:Description** RDF:ID="*creator*"» «**RDF:type RDF:resource**="*#history-information*"» «**RDFS:subClassOf RDF:resource** "#bell"» «**/RDF:Description**»

Signing individual fragments of an RDF graph of unique Bulgarian bells

Part of RDF/XML document from the developed ontology of one settlement of bells

```
«RDF:RDF»
  «RDF:Description RDF:HREF = "http
    «bell:belfry RDF:HREF = "#belfry"/
    «bell:media-files RDF:HREF = "#m
    «bell:history-information RDF:HRE
    «bell:audio-characteristic RDF:HRE
    «bell:technical-data RDF:HREF = "
  «/RDF:Description»
…
  «RDF:Description ID="b
    «bell:name»bell №01 от 01«/
    «bell:condition»добро«/bell:condition»
    «bell:coordinates»42˚41’45.28’’ N 23˚
    «loc:name» Катедрала Патриаршеск
    «loc:type»църковна катедрала«/loc:t
    «loc:location»София«/loc:location»
    «loc:state»София«/loc:state»
    «loc:country»България«/loc:country»
    «mf:name»bell_01-1.jpg«/mf:name»
    «mf:name»bell_01-2.jpg«/mf:name»
    «mf:name»bell_01-3.jpg«/mf:name»
    «mf:name»bell_01.flv«/mf:name»
    «mf:name»bell_01.mp3«/mf:name»
    «hi:creator»П. Н. Финляндски«/hi:c
    «hi:year-of-create
    «hi:place-of-create»M
    «hi:owner»Катедрала Па
    «hi:reservior»дарение«/hi:res
    «ach:tone»Сол ♯ от голяма октав
    «td:out-height»172.5«/td:out-heigh
    «td:in-height»163.1«/td:in-height»
    «td:weight»6002«/td:weight»
    «td:top-diameter»123«/td:top-diam
    «td:down-diameter»226«/td:down-
    «td:material»сплав олово, сребро
    «CARD:Affiliation»Home, Inc.«/CA
  «/RDF:Description»
«/RDF:RDF»
```

Part of “RDF description section”:

«RDF:RDF»
«RDF:Description RDF:HREF = "*http://www.math.bas.bg/bells/bell/*"»
«bell:location RDF:HREF = "*#location*"/»
«bell:media-files RDF:HREF = "*#media-files*"/»
«bell:history-information RDF:HREF = "*#history-information*"/»
«bell:audio-characteristic RDF:HREF = "*#audio-characteristic*"/»
«bell:technical-data RDF:HREF = "*#technical-data*"/»

Part of “bell description section”:

…
«RDF:Description ID="*bell_01_01*"»
«bell:name» *bell №01 от 01* **«/bell:name»**
«bell:condition» *добро* **«/bell:condition»**
«bell:coordinates» *42˚41’45.28’’N 23˚19’57.36’’E* **«/bell:coordinates»**
…
«loc:name» *Катедрала “Св. Александър Невски”* **«/loc:name»**
«loc:type» *църковна катедрала* **«/loc:type»**
«loc:settlement» *София* **«/loc:settlement»**

Part of “bell historical information section”:

…
«hi:creator» *П. Н. Финляндски* **«/hi:creator»**
«hi:year-of-create» *1911 г.* **«/hi:year-of-create»**
«hi:place-of-create» *Москва* **«/hi:place-of-create»**
«hi:owner» *Катедрала “Св. Александър Невски”* **«/hi:owner»**
«hi:reservior» *дарение* **«/hi:reservior»**
…

Signing individual fragments of an RDF graph of unique Bulgarian bells

Signing RDF graph

- First we will define what is the minimum "standalone" fragment of an RDF model. We will here give a formal definition of Minimum Selfcontained Graph (MSG) and use some simple properties laying the base for MSG signing.
- Then we give propositions and theorems, presented in [1, 2] related to the decomposition of the RDF graph into MSGs.

[1] J. Carroll, Signing RDF graphs, 2003;

[2] G. Tummarello, Ch. Morbidoni, P. Puliti and F. Piazza, Signing individual fragments of an RDF graph, 2005.

Signing individual fragments of an RDF graph of unique Bulgarian bells

- Definition 1. An RDF statement involves a name if it has that name as subject or object.

- Definition 2. An RDF graph involves a name, if any of its statements involves that name.

- Definition 3. Given an RDF statement ***s***, the Minimum Selfcontained Graph (MSG) containing that statement, denoted MSG(***s***), is the set of RDF statements comprised of the following:
  - The statement in question;
  - Recursively, for all the blank nodes involved by statements included in the description so far, the MSG of all the statements involving such blank nodes.

This definition recursively build the MSG from a particular starting statement.

Signing individual fragments of an RDF graph of unique Bulgarian bells

Next theorems show that the choice of the starting statement is arbitrary and this leads to an unique decomposition of the RDF graph into MSGs.

- Proposition 1. The MSG of a ground statement is the statement itself.

- Theorem 1. If ***s*** and ***t*** are distinct statements and ***t*** belongs to MSG(***s***), then MSG(***t***) = MSG(***s***).

- Theorem 2. Each statement belongs to one and only one MSG.

- Theorem 3. An RDF model has an unique decomposition in MSGs.

Signing individual fragments of an RDF graph of unique Bulgarian bells

- The MSG definition and properties say that it is possible to sign a MSG attaching the signature information to a single, arbitrary triple composing it.

- Along with the signature, an indication of the public key to use for verification might be provided. This indication is itself covered by the signing procedure.

- By "attach" we mean using a verification procedure. Using the same procedure more signatures can be attached to the same MSG either independently or "layered" thus providing a mechanism for countersigning.

- Given the MSG properties, this "information patch" can be merged into any existing model and the signature properties will be retained, checking the signature on any statement can be performed computing the MSG it belongs to and to check if any of the statements carry a MSG signature on it.

Signing individual fragments of an RDF graph of unique Bulgarian bells

Thank you!

- Web address of BELL archive: http://www.math.bas.bg/bells