Eighth International Workshop on Optimal Codes and Related Topics
July 10-14, 2017, Sofia, Bulgaria *pp. 31-36*

Provision of safety of interactive systems - problems and solutions

Galina Bogdanova[1] g.bogdanova@gmail.com
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences
Galya Georgieva-Tsaneva galicaneva@abv.bg
Institute of Robotics, Bulgarian Academy of Sciences
Todor Todorov todorvt@abv.bg
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

Abstract. The report outlines the characteristics of interactive communication and discusses the issue of ensuring the security of interactive systems using modern methods and techniques. Steganographic methods and image protection schemes with visible and invisible watermark are presented. The watermark error correction scheme uses the Reed-Solomon code. A software application for protecting digital resources using the described methods has been developed.

1 Introduction

Modern information and communication technologies have evolved over recent years to levels that allow for new ways of preserving, protecting and interactively presenting stored digital resources in digital repositories and libraries in the field of cultural and historical heritage (CHH).

In order to achieve the main objectives and tasks of the digital center North+ (online platform North+ and repositories for digital resources of cultural artefacts from the Central Northern Region of Bulgaria) there were realized interdisciplinary researches and developments offering a wider, protected and interactive presentation of the CHH.

A study and analysis of the state of the existing modern methods and technologies has been carried out. The analytical research covers the issues of common concepts for the protection of interactive systems, the standards used, the principles and the peculiarities of the construction, protection and interactive representation of the digital resources resources in the field of CHH. Research technologies and methods for interactive information representation, protection and storage of digital resources are dependent on the type of media (text, photo, video, audio, 3D).

A study was conducted on existing technologies for interactive systems and their protection. Modern interactive systems use a dynamically changing environment, offer easy navigation and dynamic design based on specialized computer languages and new mobile technologies [4, 5].

[1]

The multi-disciplinary technological approach is used to develop the interactive communication of the North+ system. The system has several layers and different user modules, depending on system users. It has first-categories navigation interactivity (the ability of the user to navigate through the information sites using the appropriate hyperlinks) and partial functional interactivity (allowing users to interact with other users). It contains an interactive cultural map and other interactive functionalities.

We will look at some aspects of North+ platform research related to its security and file system protection.

2 Security assessment of interactive systems

Protecting interactive systems and digital archives against unauthorized distribution of digital content is a serious problem that digital content users have to deal with. Existing modern software technologies and means of protection have been studied.

The Trusted Computer System Evaluation Criteria (TCSEC), known as the "Orange Book", issued in August 1983 by the National Computer Security Center (NCSC), part of the National Security Agency (NSA), define the main classes, concepts and criteria for assessing the security of computer systems. The TCSEC defines four major classes of secure protection: A - proven security; C - temporary security; C - reasonable security; D - minimum security.

Each class may contain one or more numbered subclasses. Each subclass is defined by a set of criteria.

The information security criteria are grouped into four aggregated categories: Security Policy; Accountability (reporting); Guarantee; Documentation.

Organization of Security policy:

- Identifying the necessary additional resources and means to ensure security;
- Organize access control of subjects to sites;
- The rules and means for object identification and authentication of the entities;
- Organization of anti virus protection;
- Encryption methods, tools and devices;
- Regulating the creation of working security documents - "Security Guide" and instruction for individual entities (managers, administrators, software developers, users, customers, etc.);
- Regulation of the necessary training and training of individual subjects;
- Establish a security administration unit.

Assessment of system security. Security policy requirements are the first of many requirements and are grouped into the following categories:

- Prudent access control; Discretionary Access Control (DAC) is a method of limiting access to files, based on user authentication. Determines who has

access and how he can use the files.

- Reuse of objects (resources): It requires protection of the files, memory and other objects of a secured system from random access of unauthorized users. - Labels and Mandate Access Control (Puts all access solutions under the control of the system). We introduce the term variable label for the mandatory access control, and its usage is described. For all objects and entities in the system to be assigned variable labels. Accountability has to implement the idea that the system knows who you are and what you are doing. The system should be able to authenticate (identify) all users and use this information to determine the legitimacy of access and to ensure the implementation of only those actions that require a level of security corresponding to the user level.

It exist three groups of requirements for reporting:

A. Identification and authentication;

It is required at all levels of the security system. TSEC defines the user to identify himself before any work action that requires interaction with Trusted computed base (TCB). The user identifies himself with an identifier and a password. Three important ways to implement secure passwords are recommended in the Green Book (The Department of Defense Password Guideline):

- The user must be able to change his /her own password;
- Passwords must be generated by the computer;
- Significant monitoring data as log-in date and time are automatically set by the reporting system and not by the user.

B. Protected path; The protected path must provide an environment where the user can communicate directly with the TCB without being able to interact with the system through secure applications and layers of the operating system. (like the system administrator).

C. Monitoring. The monitoring includes recording, checking, and reviewing security-related activities in the secure system. Security-related activity is the activity that links the subject's access to one object. In the terms of observation, this is called an event.

3 Organising the security of the specialized software system North+

As a result of the research offers the necessary safe measures for the hardware and software protection of the digital archives and repositories in the North+ system were selected and provided. The protection of digital archives is at the level of digital repositories and at storage level with raw original files.

The possibilities of using special steganographic methods for protecting the file system have been studied in more detail.

Research methods for protection of digital resources depending on the type of media (text, photo, audio) are studied [1–3].

Selected special steganographic methods and image protection schemes - with visible and invisible watermark - are also examined.

Steganography methods, which are used to protect images with watermark:

A. Hiding information in the spatial area

Embedding:

For each pixel a pseudo random number x is generated; If $x \leq \rho$, information is embedded in pixels:

$$B_{ij} = B_{ij} + (2s - 1)\, L_{ijq}, L = 0,299R + 0,587G + 0,114B, s = \{0,\ 1\}$$

Extraction:

$$B_{ij}{}' = \frac{1}{4c} \sum_{k=-c}^{c} B_{i+k,\ j} + \sum_{k=-c}^{c} B_{i,\ j+k} - 2B_{ij}$$

The sign of $\delta = B_{ij} - B_{ij}{}'$ determines the actual value of the extracted bit. The method is resistant to filtering, JPEG compression and geometric transformations.

B. Spread Spectrum

Embedding:

$$B(k_1, k_2) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} 4.A(i,j).cos[\frac{\pi.k_1}{2.N}(2.i + 1)].cos[\frac{\pi.k_2}{2.N}(2.j + 1)]$$

Identifying significant areas and embedding; Reverse cosine transformations.

Extraction: Reverse steps and comparison with a compliance threshold; Highly resistant to most signal processing and geometric transformations.

C. Watermark error correction scheme

An additional protection scheme for the data has been implemented. It uses Reed-Solomon code (RS) with appropriate parameters like external code and other optimal line code as internal. Message from $k.m$ bits is encoded with $RS(n, k)$ code over $GF(2m)$ - byte error correction. For a fixed size m and a limited total length capacity, an optimal internal code for bit error correction is selected.

Evaluation of the behavior:

- Probability of bit error: $P_{rep} = e^{r}_{i=\frac{r}{2}+1} C^{i}_{r} p^{i}_{bsc} (1 - p_{bsc})^{r-1}$
- Repeat code: $P_{sig,\ rep} = 1 - (1 - P_{rep})^{w}$
- BCH code: $P_{sig,code} = e^{n}_{i=j+1} C^{i}_{n} p^{j}_{bsc} (1 - p_{bsc})^{n-1}$
- RS / Inn. $P_{sig,rs} = e^{n}_{i=j+1} C^{i}_{n} P^{i}_{sig,inn} (1 - P^{i}_{sig,inn})^{n-1}$

The error probabilities and the noise resistance are examined (Table 1, Table 2).

Table 1. Error probability at a capacity of 400 bits.

Sign	5%	25%
8 bits	2.10^{-27}	2.10^{-8}
16 bits	3.10^{-19}	5.10^{-5}
32 bits	4.10^{-14}	3.10^{-2}
40 bits	6.10^{-14}	4.10^{-2}
56 bits	1.10^{-12}	7.10^{-2}
64 bits	6.10^{-11}	14.10^{-2}
128 bits	4.10^{-4}	-
256 bits	32.10^{-3}	-

Table 2. Noise resistance at $P_{sig} \leq 0,1$

Sign	
8 bits	28 %
16 bits	21 %
32 bits	14 %
40 bits	14 %
56 bits	13 %
64 bits	12 %
128 btis	6 %
256 bits	4 %

The new approach has better behavior in the average length of the message. The scheme produces good results for large lengths like 128, 256 bits where other techniques are virtually unusable.

A software application for protecting watermark images using the described methods and techniques has been developed.

- Watermarking in the spatial area;
- Additional resistance through the RS code, internal code;

- Correction of the coefficient of resistance and density of the bits used;
- Additional Password - The password CRC is used to initialize a pseudo-random generator.

Additionally, experiments have been made to protect a digital watermark image and with other specialized software products.

For instance: uMark (https://www.uconomix.com/Products/uMark/Default.aspx) to protect an image with a digital watermark.

Protection is made with both visible and invisible watermarks. A visible watermark is embedded in a macros created in the specialized system "North+" developed with the FotoStation Pro software.

Conclusion

Technologies has changed the ways in which information is presented and made possible new services that are unthinkable so far. The researches studies are part of the interdisciplinary work for the documentation, preservation and presentation of key factor cultural institutions from the Central Northern Region of Bulgaria. Long-term storage, secure data protection and interactive web presence across a wide range of users have been achieved.

The studies contribute to the overall development of the North+ region, provide future generations with widespread public access to digital materials, prevent the loss of valuable content, and provide the basis for the next activities of preserving and presenting the knowledge and artefacts of the cultural heritage of the North+ region.

References

[1] T. Berger and Todorov, T., Improving the Watermarking Process With Usage of Block Error-Correcting Codes, *Serdica Journal of Computing,* **2**, 163-180, 2008.

[2] I. Cox et al., Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing,* **6(12)**, 1673-1687, 1997.

[3] M. Kutter et, Digital signature of color images using amplitude modulation, *J. Electron. Imaging,* **7(2)**, 326-332, 1998.

[4] V. Liu and L. Shrum, A dual-process model of interactivity effects, *Journal of Advertising,* **38(2)**, 53-68, 2009.

[5] S. Rafaeli, *Interactivity. From New Media to Communication, in Robert P. Hawkins, John M. Wiemann & Suzanne Pingree (eds.): Advancing Communication Science: Merging Mass and Interpersonal Processes*, Newbury Park, 1988