

Software Approaches and Methods to Ensure the Security of Interactive Systems

*Galina Bogdanova*¹, *Todor Todorov*^{1,2}, *Galya Georgieva-Tsaneva*³

¹*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria*

²*Veliko Tarnovo University "St. Cyril and St. Methodius", 5003 Veliko Tarnovo, Bulgaria*

³*Institute of Robotics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria*

E-mails: galina@math.bas.bg todor@math.bas.bg galicaneva@abv.bg

Abstract: *In the paper are studied methods for protection of interactive systems and digital archives against unauthorized distribution of digital content. We make an overview of steganographic methods and image protection schemes. An improved watermark error correction scheme is presented. The studies contribute to the overall development of the North+region, provide future generations with widespread public access to digital materials. We achieve a long-term storage, secure data protection and interactive web presence.*

Keywords: *Data protection, watermarking, error-correcting codes.*

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-art 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 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 [1, 2, 8, 9].

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), defines criteria for assessing the security of computer systems.

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 antivirus 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 variable labels to be assigned. 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.

Methods of science steganography are used to protect stored data in the North+ system. There are two main directions for addressing the issue of data protection from unauthorized access: cryptography and steganography. Steganography is a science of embedding hidden messages, usually in an unobtrusive object of the image that is not visible at first glance, so only the user for whom the embedded message is able to find and read it.

The word "steganography" is of Greek origin and has the meaning of hidden writing. Using steganographic methods, information is hidden in the original data. Unlike cryptography, steganography has the task of hiding even the very fact that there is some built-in message. Secret key-guarding requires the transmission of this secret key, and thus, the transmission of additional information violates the idea of unbelievable communication. Two keys are used: private key (private, embedded) and public (stored in a public database). The object in which the hidden message is embedded is called a cover object. A cover object with a built-in message is called a stego object.

Protecting information by embedding a watermark aims to conceal hidden information through secret communication between the transmitting and receiving parties. For this reason, steganographic methods prove to be unsustainable when original data modification occurs (e.g.: transmission, storage, compression).

The protection of information by incorporating a watermark has additional resistance against probable attempts to remove embedded information. The watermark is a visible or invisible identification code permanently embedded in the original data that retains information about its presence in them even after it is retrieved from the data [6].

The steganographic schemes with watermark have two main blocks: a watermark embedding system and a watermark retrieving data system. The following watermark embedding system is used:

- Input – the watermark to be embedded; the cover object and an optional secret or public key.
- Exit – converted, watermarked data.

The system for extracting the information from protected data is as follows:

- Input – the data that have been protected by a watermark, the secret or public key used for the purpose, the original data, and the original watermark used.
- Exit – the watermark extracted from the data or some measure of the possibility that the watermark submitted at the entrance is present in the data considered.

3. Organizing the security of the specialized software system North+

As a result of the research we offer the necessary safety measures for the hardware and software protection of the digital archives and repositories in the North+ system. 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 [4, 6, 7].

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 are Hiding information in the spatial area, Spread spectrum, and Watermark error correction scheme.

A. Hiding information in the spatial area

A number of researchers have worked in this field, such as Brassil, Low, Maxemchuk, O'Gorman [5], Kutter et al. [7], and others.

Embedding. Let ρ be a predefined density parameter. It gives the probability of any single pixel being used for embedding. For each pixel a pseudo random number x is generated; if $x \leq \rho$, information is embedded in pixels:

$$L = 0.299R + 0.587G + 0.114B, \quad s = \{0, 1\}, \quad B_{ij} = B_{ij} + (2s - 1)L_{ij}q,$$

where R , G and B are values of Red (R), Green (G) and Blue (B) channel for pixel at position (i, j) . The value of s is either 0 or 1 and depends on the value of the bit that we want to embed and q is a constant that determines signature strength and is selected such as to offer best trade-off between robustness and invisibility.

Extraction. In order to recover the embedded bit we use values of the cross-shaped neighbour pixels as shown on Fig. 1:

$$B'_{ij} = \frac{1}{4c} \left(\sum_{k=-c}^c B_{i+k,j} + \sum_{k=-c}^c B_{i,j+k} - 2B_{ij} \right),$$

where c is the size of the cross-shaped neighbourhood.

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.

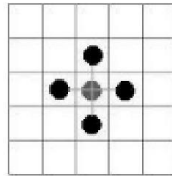


Fig. 1. Extraction according to neighbour pixels

B. Spread spectrum

In this area of information protection, the following authors have contributed Cox, Kilian, Leighton, Shamoon [6].

This steganographic method for protecting watermark images is based on various container transformations, such as Discrete Cosine Transformation (DCT). This is a standard way to represent an image in frequency domain. All actions are performed in the frequency area of the image, and it is seen as a communication channel. We compute $N \times N$ DCT coefficient matrix of an $N \times N$ image using next equation where $A(i, j)$ is the intensity of the pixel in row i and column j .

Embedding. First we compute all DCT coefficients of the DCT matrix. The DCT coefficient in row k_1 and column k_2 is calculated according to the following formula:

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

Then we determine perceptually significant regions – with highest magnitude coefficients of the transform matrix and insert there the watermark. At the end inverse DCT are made.

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 as outer code and other optimal linear codes as inner. RS codes are often used as outer codes in systems that use simpler inner codes. Using an inner code reduces the error level, and then the RS code corrects the remaining errors [3, 4].

Message from $k.m$ bits is encoded with $RS(n, k)$ code over $GF(2^m)$ – byte error correction. For a fixed size m and a limited total length capacity, an optimal inner code for bit error correction is selected.

Evaluation of the behavior. The probability of errors in the different coding used is calculated using formulas.

For data with a length w that are repeated r times we have:

- Probability of bit error

$$P_{\text{rep}} = e^{r_{i=r/2+1}} C_r^i p_{\text{bsc}}^i (1 - p_{\text{bsc}})^{r-1},$$

where p_{bsc} is probability of assuming a bit error in a binary symmetric channel; C_r^i is binomial coefficient.

- The error message level error at Repetition code is:

$$P_{\text{sig,rep}} = 1 - (1 - P_{\text{rep}})^w.$$

- For BCH (n, k, t) code (t is the number of errors that can be corrected): The upper limit of the probability of error is calculated based on the probability of t or more of the errors admitted in the data, using the formula:

$$P_{\text{sig,code}} = e^{n_{i=j+1}} C_n^i p_{\text{bsc}}^i (1 - p_{\text{bsc}})^{n-1}.$$

- RS / Inn.

In case when using RS Code coding, the formula has the form:

$$P_{\text{sig,rs}} = e^{n_{i=j+1}} C_n^i P_{\text{sig,inn}}^i (1 - P_{\text{sig,inn}})^{n-1},$$

where $P_{\text{sig,inn}}$ is probability of assuming an inner code error; it can be calculated as described above for the BCH code.

In the next tables are the results of experimental calculations of error probabilities and the noise resistance. More information could be found in [4]. The error probabilities and the noise resistance are examined (Table 1, Table 2). In Table 1 are presented error probabilities for two specific channel error rates (5% and 15%) and for different lengths of the signature.

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 presents maximum channel error rates with respect to $P_{\text{sig}} \leq 0.1$ condition for different signature lengths.

Table 2. Noise resistance at $P_{\text{sig}} \leq 0.1$

Sign	%
8 bits	28 %
16 bits	21 %
32 bits	14 %
40 bits	14 %
56 bits	13 %
64 bits	12 %
128 bits	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, inner 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.

On Fig. 2 is shown the general watermarking scheme used in North+ project.

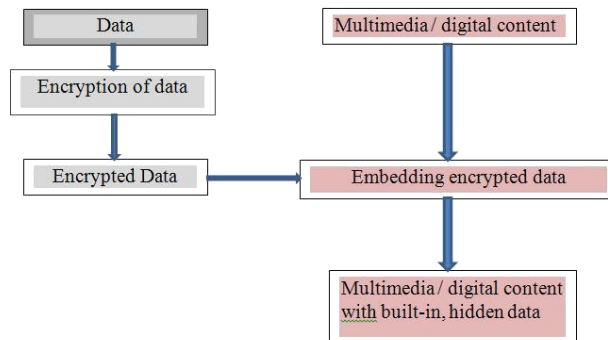


Fig. 2. General protection scheme with digital watermark

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.

On Fig. 3 is shown usage of uMark.

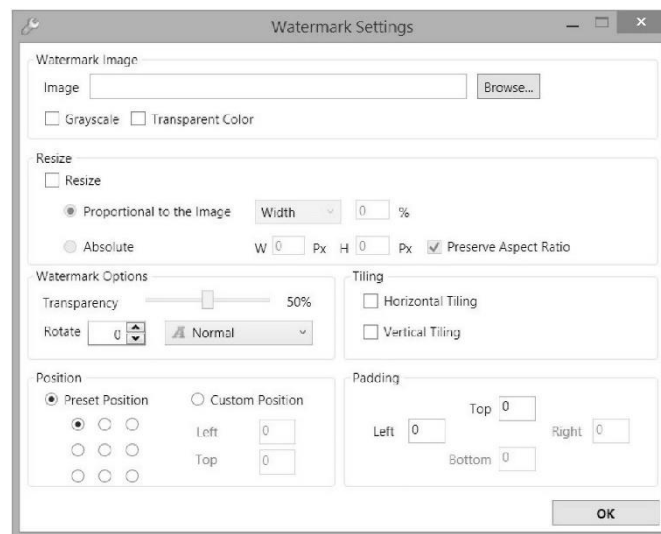


Fig. 3. Protect an image with a digital watermark using uMark

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.

Fig. 4 shows the process of protection with visible watermark using various software products.

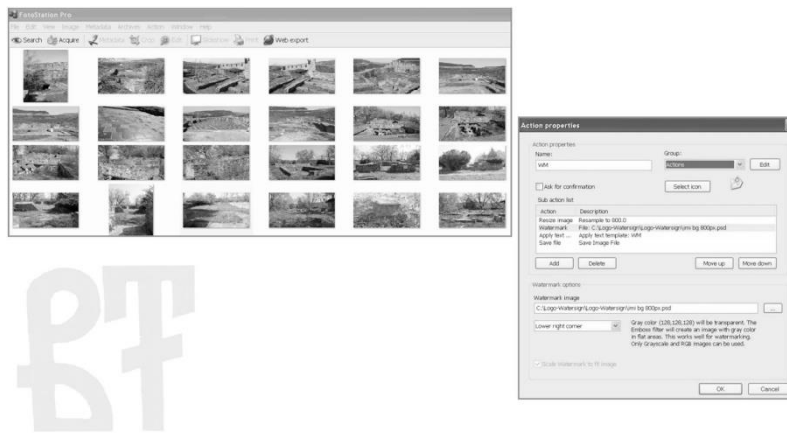


Fig. 4. Visible watermark protection with dedicated photo processing software

Audio protection. We have also made a protection mechanism for audio files included in the archive. Our approach is to use ID3 tags of the audio file [10]. This is a standard for adding metadata in audio files. We prepare a set of metadata in order to identify each file. Then calculate a hash on this data plus a set of custom file properties using SHA2 algorithm. This hash is stored in a custom text field in ID3 tags. Later if we want to check the proper usage of an audio file we just have to calculate again the hash according to the same algorithm and verify with the one saved in the ID3 tags.

4. Conclusion

Technologies have 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. Bogdanova, G., T. Todorov, N. Noev. Creating and Representing Semantic Knowledge of Bell Objects. – International Journal of Applied Engineering Research, Vol. 12, 2017, No 19, Research India Publications, pp. 8986-8994.

2. Bogdanova, G., T. Todorov, N. Noev. Digitalization and Security of "Bulgarian Folklore Heritage" Archive. – In: Proc. of 11th International Conference on Computer Systems and Technology, 2010.
3. Bogdanova, G., T. Todorov, V. Todorov. QPlus – Computer Package for Coding Theory Research and Education. – International Journal of Computer Mathematics, Vol. **88**, 2011, No 3, Taylor and Francis, pp. 443-451.
4. Berger, T., T. Todorov. Improving the Watermarking Process with Usage of Block Error-Correcting Codes. – Serdica Journal of Computing, Vol. **2**, 2008, pp. 163-180.
5. Brassil, J., S. Low, N. Maxemchuk, L. O. Gorman. Hiding Information in Document Images. – In: Proc. of 29th Annual Conference on Information Sciences and Systems, 1995, pp. 482-489.
6. Cox, I., J. Kilián, T. Leighton, G. Shamoon. Secure Spread Spectrum Water-Marking for Multimedia. – IEEE Transactions on Image Processing, Vol. **6**, 1997, No 12, pp. 1673-1687.
7. Kutter, M., et al. Digital Signature of Color Images Using Amplitude Modulation. – J. Electron. Imaging, Vol. **7**, 1998, No 2, pp. 326-332.
8. Liu, V., L. Shrum. A Dual-Process Model of Interactivity Effects. – Journal of Advertising, Vol. **38**, 2009, No 2, pp. 53-68.
9. Rafaeli, S. 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.
10. ID3 Tags.
<http://id3.org>

Received 28.09.2017; Second Version 10.12.2017; Accepted 28.12.2017