SPREAD SPECTRUM WATERMARKING TECHNIQUE FOR INFORMATION SYSTEM SECURING

Todor Todorov

Abstract: In this paper we consider a computer information system and a way to realize the security of the data in it with digital watermarking. A technique for spread spectrum watermarking is presented and its realization with MathLAB 6.5 is shown.

Introduction

Web-based information systems and their security with digital watermark are the main subjects of this paper.

On-line information automobile system Auto-World for examination and study of the different kinds of automobiles is developed. The application, which is based on the client/server module, has Application Space and Space DataBase, which are connected by PHP code. The Application Space operates with web browser, which associates with Apache Server by HTTP protocol. The application uses MySQL databases due to the necessity of convenient and rapid work with large amounts of data.

A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process. Here we present an algorithm realized with MathLab 6.5 functions and used for digital signing of images included in the presented information system.

Characteristics of Web-based Information Systems

Information systems are based on well-arranged data systems for parts of our real surroundings. It is supported by computing systems. An example of such system's data content is the information, supported by the external memory of a computing system and concerns the firms, their owners, the stocks they produce, preserve and sell/buy, the price, material and labour expenses for the particular activity. This data can show typical relations in the particular sphere – for example transport (air, railway, bus, marine), medical and other types of information insurance of the population.

The information system is a system, which processes the basic information activities - adding, preserving, processing and spreading information [2].

An information system can be considered as a model of a real process, the realization of which is an important aim for the work of an institution. Besides the organization of the basic actions (movement of objects such as stocks, services, capitals, people etc.) in it, another process must be organized - documenting the basic elementary actions, which change the process (adding, preserving and processing data for it). Instead of object, documents are moved in an information system. They show the corresponding actions and submit them in the model.

The Organization of an information system involves the organization of a particular information process, and that is why different circumstances must be clarified.

– Which data for the objects will be put in the documents.
– How will the documents be organized (at the entrance and at the exit).
– For which other processes additional information will be needed. (consistency) and which are their sources.
– How will the documents be processed, i. e. what are the problems and how will they be solved.
– What will be the purpose, the range of the information system and prospective, restrictions needed for the environment of its application.
– What results are expected - technical, economical, social etc.
– What expenses and inculcating are acceptable for the information system.

The development of local computer networks and Internet leads to fast augmentation in the appliance of software products in the organization of business objects' management.

An important part of this process is the development of web based information systems in different spheres, based on the client/server technology and data base usage.

Dynamic technologies are also very important for web-based systems.

Web-based information systems for automobiles are: http://www.peugeot.bg, http://www.bmw.com, http://www.theautochannel.com, http://www.auto.dir.bg, http://fiat.com.

Web based Information-reference system Auto-World is developed for examination and study of different automobiles. The project, which is based on the client/server module, has Application Space and Space DataBase, which are connected by PHP code [1] [10]. The Application Space operates with web browser, which associates with Apache Server by HTTP protocol [7]. The application uses MySQL databases [9] due to the necessity of convenient and rapid work with large amounts of data.

Auto-World aims to help people in examination and study of different kinds of automobiles, to present the most famous marks and models automobiles, their constructive and technical characteristics. The system offers text, video and audio information with references for them and opportunities for studying and testing in the sphere of automobiles. Due to the necessity of good results, an appropriate data base with information for the models, lessons and tests is built.

Securing Images with Digital Watermark

The proliferation of digitized media (audio, image, and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Therefore, conventional cryptography provides little protection against data piracy, in which a publisher is confronted with unauthorized reproduction of information. A digital watermark is intended to complement cryptographic processes. It is a visible, or preferably invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process.

Referring to Fig. 1 for a block diagram of a general watermarking system, the secret key is used to generate the random sequence W in this case [6].
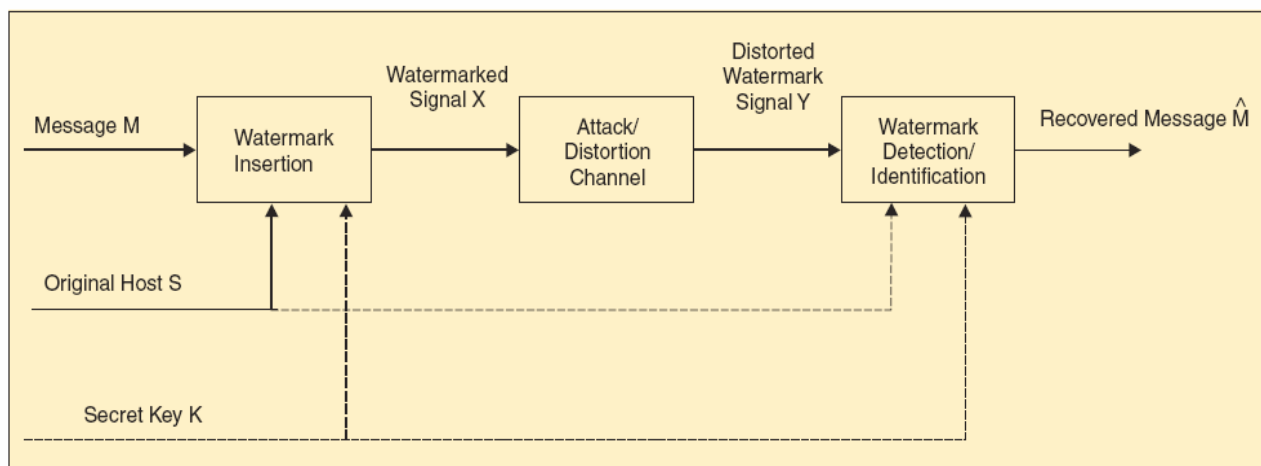

Fig. 1.

In order to be effective, a watermark should have the characteristics outlined below.

Unobtrusiveness: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Robustness: The watermark must be difficult (hopefully impossible) to remove.

In particular, the watermark should be robust in the following areas:

− Common signal processing: The watermark should still be retrievable even if common signal processing operations are applied to the data.

- Common geometric distortions: rotation, translation, cropping and scaling.
- Subterfuge attacks (collusion and forgery): In addition, the watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data.
- Universality: The same digital watermarking algorithm should apply to all three media under consideration.
- Unambiguousness: Retrieval of the watermark should unambiguously identify the owner.

Spread Spectrum Watermarking

The watermark should not be placed in perceptually insignificant regions of the image (or its spectrum), since many common signal and geometric processes affect these components [4].

The problem then becomes how to insert a watermark into the most perceptually significant regions of the spectrum in a fidelity preserving fashion. Clearly, any spectral coefficient may be altered, provided such modification is small. However, very small changes are very susceptible to noise. To solve this problem, the frequency domain of the image or sound at hand is viewed as a communication channel, and correspondingly, the watermark is viewed as a signal that is transmitted through it. Attacks and unintentional signal distortions are thus treated as noise that the immersed signal must be immune to. We originally conceived our approach by analogy to spread spectrum communications [5]. In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. To insert a watermark in the frequency domain of an image we should first apply DCT(Discrete Cosine Transformation). This is a standard way to represent an image in frequency domain.

We compute NXN DCT coefficient matrix of an NXN image using next equation where A(i,j) is the intensity of the pixel in row i and column j.

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

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.

Structure of Watermark

A watermark consists of a sequence of real numbers $X=x_1\ldots\ldots x_n$.

In practice, we create a watermark where each value xi is chosen independently according to N(0,1) (normal distribution) using such distributions leaves one particularly vulnerable to attacks using multiple watermarked documents.

We extract from each document D a sequence of values $V=v_1\ldots v_n$, into which we insert a watermark $X=x_1\ldots x_n$ to obtain an adjusted sequence of values $V'=v'_1\ldots v'_n$. V' is then inserted back into the document in place of V to obtain a watermarked document D'. One or more attackers may then alter D', producing a new document D*. Given D and D*, a possibly corrupted watermark X* is extracted and is compared to X for statistical significance.

When we insert X into V to obtain V' we specify a scaling parameter α, which determines the extent to which X alters V ($v'_i = v_i(1+a_i x_i)$).

We measure the similarity of X and X* by sim(X,X*)= X*X/SQRT(X*,X*).

To decide whether X and X* match, one determines whether sim(X,X*)>T, where T is some threshold. Setting the detection threshold is a classical decision estimation problem in which we wish to minimize both the rate of false negatives (missed detections) and false positives (false alarms).

Such a watermark is very robust to the most of common signal processing and geometric distortions.

Presented algorithm have been realized with MathLab 6.5 functions [8] and used for digital signing of images included in the Auto-World information system.

Original Image

Watermarked image

Conclusions and Future Work

The proliferation of digitized media (audio, image, and video) is creating a pressing need for copyright enforcement schemes that protect copyright ownership. Presented information system is only one of the multimedia applications that could be secured with watermarks. We also explored application of other watermarking algorithms[3] and in the future we will continue to research this area.

Bibliography

[1]   Кастането, Х., Х. Роат, С. Шуман, К.Сколо, Д. Вилайът. Професионално програмиране с PHP. СофтПрес, 2001.
[2]   Лазаров, Л., М. Лазарова, Информационни системи. Славянска култура и образование, 2001.
[3]   Bogdanova, G., T. Todorov, Application of digital watermarking, Journal of International Research Publications [serial online]. Bulgaria, Science Invest Ltd - branch Bourgas 2004.
[4]   Cox, I., J. Kilian, T. Leighton, G. Shamoon. Secure spread spectrum watermarking for multimedia. Proceedings of the IEEE International Conference on Image Processing. Vol. 6. , 1997.
[5]   Pickholtz, R., D. Schilling, L. Millstein. Theory of spread spectrum communications. IEEE Trans. Commun., vol. COMM-30, 1982.
[6]   Podilchuk, C., E. Delp. Digital Watermarking Algorithms and Applications. IEEE Signal Processing Magazine, 2001.
[7]   http://www.apache.org
[8]   http://www.mathworks.com/
[9]   http://www.mysql.com
[10]   http://www.php.net

Author Information

Todor Todorov – PhD Student, Institute of Mathematics and Informatics, BAS, V.Tarnovo: +359 62 630132, e-mail: todor@moi.math.bas.bg