Second International Conference
Modelling and Development of Intelligent Systems
Sibiu - Romania, September 29 - October 02, 2011

About Hash Function and Watermark Algorithms

Crina Rațiu, Dominic Bucerzan, Mihaela Crăciun

Abstract

In today's corporate world, images and documents travel widely and rapidly through email, across the Internet and mobile devices. Controlling and protecting sensitive or confidential documents and images has become very important. [12]

To protect the ownership rights on digital audio, image, video and all forms of media content, digital watermarking techniques can be used combined with cryptography and hash functions.

In this paper we focus on different algorithms of digital watermarking for image applications and on several types of watermarking attacks which aim at its robustness, its form and even at its removal. Also we propose a solution of digital watermarking completed with a hash function in order to increase the degree of security of the transferred data through today's uncertain environment. To sum up we present our view upon specific solutions in this field.

Key words: digital watermarking, hash function, cryptography

1 Introduction

Digital information can be copied and it is difficult to make the distinction between the original and the copied version. In order to protect the digital data against copying and forgery two complementary techniques have been developed: cryptography and digital marking. Cryptosystems may be used in order to protect digital data on its way from the sender to the receiver. The received and decrypted data is identical to the original one and it is no longer protected. Here digital watermarking can be a solution for ensuring the authenticity of digital data.

The techniques of digital watermarking as well as cryptography straighten each other in the process of sending and receiving digital information through today's unsecure networks.

Taking into consideration nowadays technology it is not difficult to apply a watermark to a digital data set, but in the same time there are many ways to remove it. In order to be able to detect when o digital watermark has been altered a "hash" function may be used considering that it has an important role in the identification of the content of a message sent through computer networks. [11]

Hash function may also be called "dispersion" function or "digest" function. These type of function changes a series of symbols of arbitrary lengths such as a password of 8 characters or a 1000 pages document, in a series of symbols with relatively short of fixed dimension. The gist of the idea is that when a difference occurs in the case of the inserted series the result changes automatically. [11]

Hash functions have an important role in cryptographic systems which protect communication channels. In the article "Find me a hash", Susan Landau, names this kind of function "tape function"-

the duct tape of cryptography, because it has so many usages: to prove a message is genuine, to ensure the integrity of the software, to create passwords which you can only use once, to create digital signatures and it has also the function of enabling many internet communication protocols.

The paper is organized as follows: in section 1 we made an introduction about the importance of assuring digital information security, section 2 contains the most used terms in cryptography especially hash functions, section 3 is reserved to watermarking algorithms, in section 4 we tackled upon different types of attacks which aim watermarking algorithms, we present our contribution to watermarking techniques in section 5 and some conclusions in section 6.

2 Cryptography and Hash Functions

The latest development of our society has lead to the increasing of the information volume sent through computer networks, which has accelerated the progress and the usage of cryptographic methods. The purpose of cryptography is to ensure through mathematical specific techniques, the fundamental characteristics of electronic data: confidentiality, integrity, authenticity and non-repudiation.

The hash functions, also known as one-way functions, are a fundamental class of primitive functions in modern cryptography, used mainly in digital signatures and in ensuring the integrity of digital data. The hash cryptographic functions compress electronic data set of arbitrary length into electronic data set of fixed length.

The characteristics of a hash cryptographic function [14]:

- it is a one way function which means it is difficult to reverse it.
- it can easily face collisions (it is difficult to find messages which generate the same type of hash)

The hash function may be regarded as a surjective function (because there is a possibility, however remote, to find "n" messages for the same hash).

Not all the hash functions are proper to cryptography. An example of a hash function which cannot be regarded as a cryptographic function is a function which gives you the sum of a series of numbers. This function is not cryptographic, first of all because we can easily find two numbers for which the function may give us the same result (for ex. 23 and 50) and secondly because it has no fixed length.

An example of daily used hash function is the algorithm used to determine the Control number of the Personal Numeric Code. The hash function which has been mostly used till recently is MD5. [14] MD5 algorithm has been made public because of possible adjustments and for a possible acceptance as a standard procedure. This algorithm is mainly designed for the application of digital signature, where a file must be safely compressed before being encrypted using a secret key through a cryptographic system with a public key.

3 Algorithms used for watermarking the images

3.1 Robust, space algorithm proposed by A. Tefas and I. Pitas

This algorithm works in space. This means that costly processing (time for calculations) is not needed for the inclusion of the watermark. Brightness values (L (x, y) ∈ {1, .., L}) or the red, green and blue (r (x, y), g (x, y), b (x, y) - Red Green Blue) are directly manipulated [9].

Watermark W is a ternary image with pixel value {0, 1 or 2}. These values are generated using digital key K. Watermark insertion is made by modifying the pixel value of the original image: [13]

$$P'(x,y) = \begin{cases} P(x,y), & \text{if } W(x,y)=0 \\ E1\,(P(x,y), IN\,(x,y)), & \text{if } W(x,y)=1 \\ E2\,(P(x,y), IN\,(x,y)), & \text{if } W(x,y)=2 \end{cases} \quad \text{where:}$$

P - original image (greyscale), (x, y)-location of a pixel, P '- image with watermark, IN - image neighborhood, E1 and E2 - functions for the inclusion of a watermark defined as follows:

E1 (P, IN) = (1-a1) •IN(x, y) + a1 •P(x, y)

E2 (P, IN) = (1-a1) •IN(x, y) + a2 •P(x, y), where a1 > 0, a2 < 0, scaling constant.

The multiplying by (1 - a1) in scaling IN's value is used to ensure that the value P' of the image with watermark will not overcome the maximum value for a representation of the image, 8 bits, corresponding to a white pixel.

The value of a neighborhood pixel is calculated as the arithmetic mean of its neighboring pixel values in the original image, for a given value of neighborhood radius r. For example, if r = 1, then the value is calculated as follows: [13]

$$I_N(x,y) = \frac{P(x+1,y) + P(x+1,y+1) + P(x,y+1)}{3}$$

3.2 Algorithm proposed by G. C. Langelaar

The watermark consists of a bit string. The algorithm manipulates the pixel brightness, in blocks of 8 x 8 pixels. Thus we get XY/64 possible locations (XY is the number of pixels in the image). No qualitative selection is made among the possible locations which are randomly selected. It creates a binary model, pseudo-random size 8 x 8 pixels, which will be used for each insertion: [6]

pat(x,y) ∈ {0, 1}, where 0 ≤ x, y < 8

To insert a watermark's bit in a block B = {l (x + xo, y + yo) where 0 ≤ x, y <8}, the first time the block is divided into two parts B0 and B1, using the model:

B0 = {l(x+xo, y+yo) where pat(x, y) =0}

B1 = {l(x+xo, y+yo) where pat(x, y) =1}

The mean brightness is calculated for both categories l0 and l1. The difference between the two values is the signature bit, where α> 0 is the threshold:

l0 – l1 > +α if s =1

l0 – l1 < -α if s =0

If this relationship does not occur naturally, we will decrease or increase pixel brightness value B1, until the required relationship appears.

3.3 Algorithm proposed by Ingemar J. Cox

This algorithm is considered a classic between the watermarking algorithms and was first introduced in 1997 [3]. The image is divided into two parts: the background and the object of interest of the owner. A watermark is then generated by a key. It consists of a series of random real numbers, which are distributed according to a Gaussian curve. Based on the reference image, the selected object is transformed into frequency domain using discrete cosine transformation.[13]

Marking can be described mathematically as follows: X = (x1, x2, ..., xn) where n is the watermark's length. The choice of length is based on the targeted extent of the watermark's spectrum. The bigger the length, the smaller the restrictions is to include the mark in the image. To incorporate the marking in the picture, a number of factors must be extracted using discrete cosine transformation applied to the result image. Consider the image denoted by P and coefficients C = (c1, c2, ..., cn), n being the length of the bookmark. C coefficients are chosen as the most important coefficients of discrete cosine transformation. Coefficients are modified by using three different formulas:[13]

ci' = ci + a • xi (1)

ci' = ci • (1 + a • xi) (2)

ci' = ci • (e a • xi) (3)

Equation (1) is not exactly suitable if the "ci" values have a wide variety. If the deviation is 106 when summing with 100, it may be insufficient to create a watermark, but if the deviation is 10, the summing with 100 will distort the value unacceptably. Equations (2) and (3) are more robust to such differences in scale. Figure 2 presents schematically the main steps in the insertion technique of a watermark using the algorithm proposed by Ingemar J. Cox.

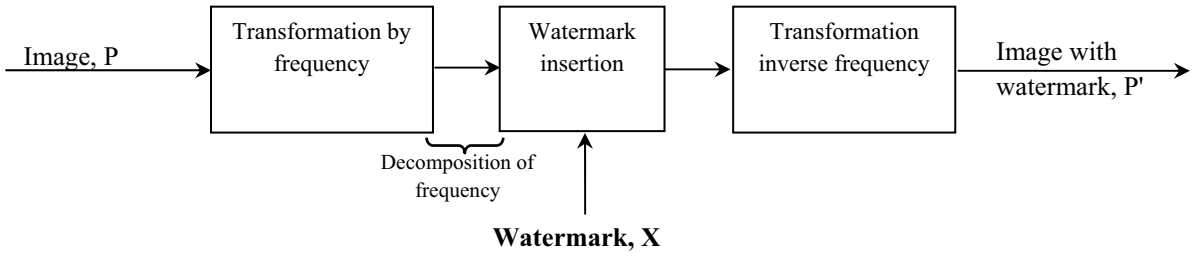

Fig. 1 Description of Cox's additive algorithm [13]

Although watermarking techniques are developing constantly and become more complex, the attacks methods are also increasing. Below we present the main types of attacks that target the watermarking algorithms.

4 Attacks on watermark

Attacker's goal is to reduce the security of marking system, in other words to reduce the probability of extraction / detection of the original watermark, i.e. to increase the likelihood of extraction / detection of a watermark inserted in a signal that was not marked (false extraction).

4.1 Attacks on the watermark's robustness

These attacks change the image pixel values and can be classified into two categories: attacks based on signal processing algorithms and attacks with algorithmic characteristics. [2]

The first category includes attacks that use conventional methods of image processing: compression, filtering or scanning. Attacks using methods of video processing to modify images by adding noise are meant to weaken the strength of the watermark. There are currently several software programs that demonstrate the strength of attacks. One of them is UnZig. Image degradation in this case is reasonable, concluding that this attack is particularly effective.

Compression - the most common category of unintentional attack. This method removes insignificant items from a multimedia signal from the perceptual point of view. Thus, by compression, perceptually similar signals come to be identical.

Filtering - marks the signal like an additive noise, which is a reasonable assumption for transparent marking spread spectrum type. Removing the marking is equivalent to a problem of disposal of a noise from an image, resulting in an estimation of the original image. Random Noise - introduces imperceptible distortions even at high signal per noise of 20 dB, but the impact on the detection of the watermark is insignificant.

Attacks on cryptographic security - cryptographic security refers to the integrity of the semantics marking and to the autentification to ensure confidentiality to robust marking. Attacks on cryptographic security are illegal. These kind of attacks have as target the cryptographic components from the transparent marking system. They use standard methods of cryptanalysis to attack the system: brute force search for the inserted message or key search.

Estimation attacks - in these cases, watermark or the host signal is estimated without knowing the secret key, but with information about the statistical of the watermark, and of the host signal. These attacks are applicable when the marking has been inserted into a redundant way, or when there are more marked copies available [10]. The re-modulation attack - with an estimated watermark an attacker can re-modulate the image: the estimated watermark (negative modulation) is extracted from the marked image. In the case of a correlation detector, this action cancels the positive correlation, provided the watermark is similar to the original. On the other hand, by extracting an amplified version of the estimated watermark, the detector using the correlation will fail to find the watermark in the marked image.

Attacks using *multiple marked copies* (multiple-copy) occur when the host signal is the same, and the marking is different. Essentially, these attacks are collision attacks [8]. There are two main approaches: signal processing and information encoding. In a collision attack, a coalition of pirates who have different versions of multimedia products, examine different copies in the hope of creating a new signal that is not tied to any one of them. There are several types of collision. One method consists in synchronizing the marked copies differently and mediating them, which is a simple example of linear collision. Another collision attack is called "copy-and-paste", in which attackers assemble parts cut from their copies, resulting in a new signal.

4.2 Attacks on Watermark's shape

The attacks on the presentation differ from the previous. The purpose is not to eliminate the watermark, but to change it so that a detector cannot find it. Examples of such attacks are: rotation, minimize and maximize, affine transformations in general.

The mosaic attack - divides the signal as if it is displayed as an entity, but marker detection is not possible. This is called a Stirmark attack. An example of such an attack was given by Petitcolas (Cambridge University Computer Laboratory). The attack is to divide an image into smaller parts. These parts will be assembled on a Web page using HTML. An intelligent agent responsible for searching the network for watermarked images will find only blocks of images which are too small to constitute a watermark. The attack does not cause a degradation of image quality because the pixel values are preserved [10].

Geometric attacks – try to desynchronize the detector in such a way that the detector cannot find the watermark. Examples of geometric attacks: translation, rotation, resizing (scaling) and their combinations; nonlinear image curving.

4.3 Attacks on the interpretation of the watermark's presence

This attack consists in the creation of another watermark by the cyber attacker and the insertion of that watermark into the image. The newly created Watermark will have the same intensity and shape with that of the owner. In this situation, a correct decision cannot be taken regarding the property of that image [11].

Attack of ambiguity - The attacker extracts its own watermark from the watermark signal, resulting in a pseudo-host signal, which when used in informational detection, will allow detection of the attackers watermark. Thus we are faced with the uncertainty regarding the identity of the copyright owner. To protect copyright, the markings must not be reversible. In other words, an attacker should not be able to extract a watermark from the original multimedia signal. A solution to this problem is to make the watermark addicted to the original signal by means of one-way function (no inverting). Copy Attack - estimates the marking from a marked signal and inserts it into another signal, called the target signal. This type of attack can be applied if the target signal can be produced without knowing a valid marking system for marking or key. Again, the marking signal depending on the original signal may be resistant to copy attack.

Attack of the multiple marking - the marked image will be marked again with another watermark algorithm. The question that rises is: which was the first watermark? A possible solution would be to generate time-stamped watermarks. Possible solutions against these types of

attacks are the establishment of some rules for the construction of the marking system, to combat the known ones, such as using non-invertible marks in the case of ambiguity attack.

4.4 Attacks by law

These types of attacks are of a completely different nature than those described above. Attacks by law may involve existing or future laws of copyright and ownership of digital images, data interpretations of laws, the owner and the credibility of the attacker, attacker's ability to spread doubts about a scheme of watermark in a courtroom and so on. One should also consider other factors such as financial strength of the owner or the attacker that the experts brought in as witnesses, the competence of judges involved in such trials.

Nowadays it is more popular to use compression with loses in the preparation of digital images via electronic data transmission. JPEG is most commonly used, but the wavelet methods are to replace TCD methods in the near future.

5 Contribution to watermarking techniques

As mentioned before, there are several methods to erase or replace a watermark from a digital image. In order to increase the security of electronic data against deleting or replacing, we drew some conclusions comparing the invisible watermarking algorithm proposed by A.Tefas and I. Pitas implemented in Delphi environment by A.Benczik and D. Bucerzan in "Protecția dreptului de autor asupra produselor multimedia. Tehnici de Watermarking" [10] and the solution presented by C.Ratiu and D.Bucerzan at SICOMAP2010 which proposes a digital watermark completed by a hash function implemented in JAVA [11].

In order to reduce this type of threats and to increase the security of transactions of electronic data, C. Ratiu and D. Bucerzan have designed an application which marks an image through a watermark technique which is secured by a hash function which uses the MD5 algorithm. In order to reach the above mentioned goals, JAVA has been chosen as the environment programming language, because it has been designed for a complex environment like the internet. [1]

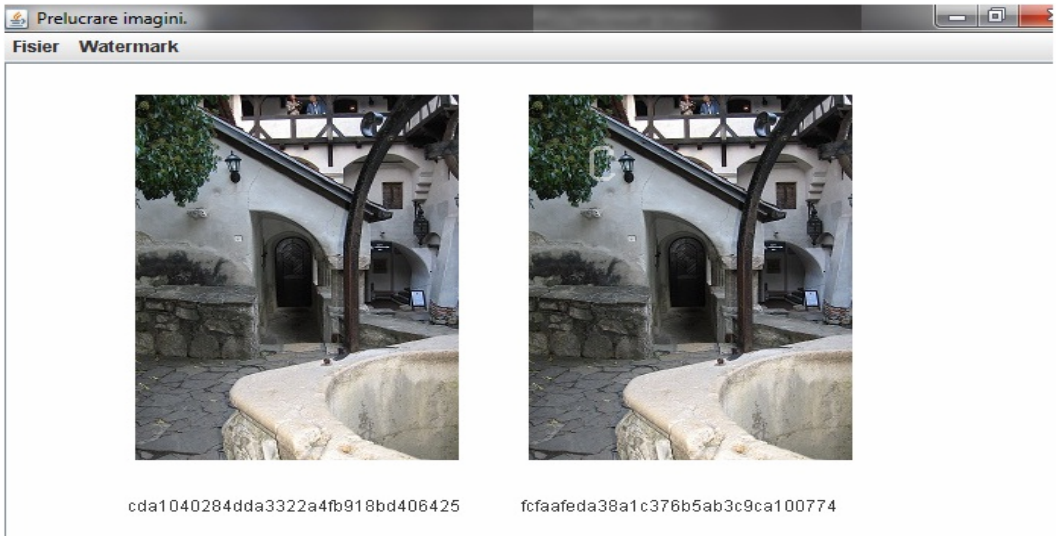

Fig. 2 The loaded image – marked with double intensity watermark and the digest code obtained after having applied the hash algorithm [11]

As seen in figure 2, after loading an image, the hash cod is processed. The user can select which watermark to use from the main menu of the program. In the next step the image is marked

with the selected watermark. Finally the hash code for the watermarked image is processed. It can be observed that a different digest code is obtained.

To implement the Pitas algorithm, the Borland Delphi programming environment was chosen. Delphi is a software development environment based on components, facilitating rapid development of highly efficient applications based on Microsoft Windows and requires only minimal code writing. Delphi class library is a solution for the traditional Windows programming requirements, sparing us of complicated and often repetitive programming [4].

As seen in figure 3, taking advantage of the opportunities offered by the Delphi environment, we will use the application to see an image selected by the user. In the next step the user chooses a key needed to mark the image. To show that the two images are not identical, we create the difference image.

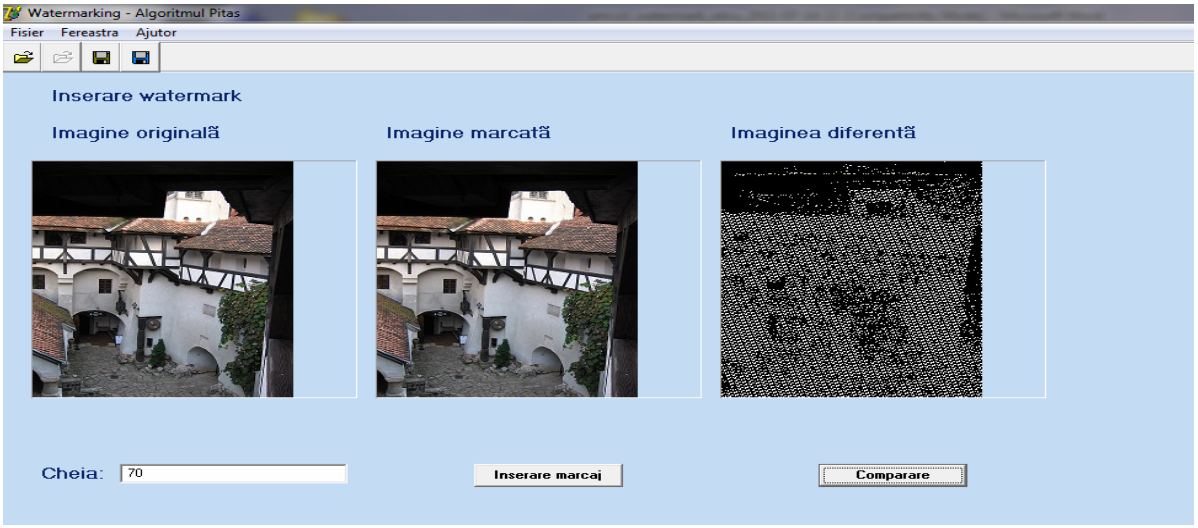

Fig.3. Pitas algorithm implemented in Delphi [10]

After comparing the results obtained from the two applications we can say that the Pitas algorithm implemented in Delphi is faster than the visible marking algorithm proposed in Java. This is due to the facilities of mending the images in Delphi environment such as the drawing canvas and its pixels property [10]. The main disadvantage of the application made in Delphi is that it can process only files of BMP type; the application implemented in Java can process different types of images.

An advantage of Java solution is the cancelation of the keys issue by applying a HASH function to the marked image. A disadvantage of Java solution is the fact that it has a longer execution time than the Pitas algorithm.

By using these techniques of perceptible or imperceptible marking, many cases in which the copyright is either violated or doubtful, can be clarified or even avoided. This technique proves to be useful if the multimedia document is used in medical applications, commercial transactions, evidence in court, etc. The electronic data must be first of all authenticated, and then a test will be made upon its integrity. Watermark can authenticate the electronic data.

6 Conclusions

In this paper we present a personal aproach to data security issues; presenting both a clasical solution of digital watermarking (A.Pitas, I.Tefas) as well as an original solution that combines digital marking with the safety given by the involvement of a HASH function.

Also we make a parallel between the presented algorithms analizing both strenght as well as vulnerable points; we also analyze the typology of possible attacks that aim digital watermarking so that a future study may approach the reduction of this kind of threats.

As written in the above rows, both algorithms that we have approached in our study have advantages and disadvantages. The Pitas algorithm is faster but the JAVA solution proposed by the authors is more secure. The JAVA solution uses a visible algorithm which does not have an artistical shape, the Pitas algorithm is an invisible one. We cannot say that either of them is a bad one or a good one. But we can see the good part of each and we can focus on improving or even eliminate the vulnerable points.

The algorithm proposed by the authors is far from being finalized but the performances reveled in this work recommend it for future development.

References

[1] ***, http://cs.unitbv.ro/~costel/secupdfs/3_3_0_Valori%20Hash%20si%20IntegritateaDatel
[2] C. Chiru, *Contribuţii la asigurarea securităţii software-ului*, PHD Theses, Bucureşti, 2003
[3] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon, *Secure Spread Spectrum Watermarking for Multimedia*, IEEE Transactions on Image Processing, vol. 6, no. 12, December 1997, pp. 1673
[4] ***, Delphi User's Guide, *Delphi for Windows*, Borland International, 1995, available at: http://www.borland.com/resources/en/pdf/white_papers/delphi_2005_reviewers_guide.pdf
[5] B. Jellinek, *Invisible Watermarking of Digital Images for Copyright Protection*, Ph.Desis, Salzburg'00.
[6] G. C. Langelaar, R. L. Lagendijk and J. Biemond, *Robust Labeling Methods for Copy Protection of Images*, Proceedings of the SPIE Storage and Retrieval for Image and Video Databases V, volume 3022, San Jose, California, 1997
[7] P. Meerwald, *Digital Image Watermarking in the Wavelet Transform Domain*, Department of Scientific Computing, University of Salzburg, Austria, 2001
[8] C. Naforniță, *Creşterea securităţii reţelelor de comunicaţii de date prin autentificare bazată pe watermarking*, Research report, Universitatea Politehnica, Timişoara, 2006
[9] A. Tefas and I. Pitas, *Robust Spatial Image Watermarking Using Progressive Detection*, Proceedings of the IEEE Conference on Acoustics, Speech, and Signal Processing (Vol. 3), 2001
[10] D. Bucerzan, A. Benczik, *Protecția dreptului de autor asupra produselor multimedia. Tehnici de Watermarking*, Dissertation report, Universitatea Aurel Vlaicu, Arad, 2008
[11] D.Bucerzan, C.Ratiu, *Aspects of a Watermark Solution*, Informatica Economica Journal, Vol.14, No. 4/2010
[12] ***, http://www.digitalwatermarkingalliance.org/app_docimage.asp, *Document and Image Security*, consultat la 14.07.2011
[13] D.Bucerzan, C.Ratiu, *Attacks on the Watermark Techniques*, 2-nd Symposium on Business Informatics in Central and Eastern Europe

CRINA RAȚIU
SC Daramec SRL

Loc. Şofronea, F.N., Jud. Arad
ROMANIA
E-mail: ratiu_anina@yahoo.com

DOMINIC BUCERZAN
Aurel Vlaicu University of Arad
Department of Mathematics-Informatics
310330 Arad, 2 Elena Drăgoi
ROMANIA
E-mail: dominic@bbcomputer.ro

MIHAELA CRĂCIUN
Aurel Vlaicu University of Arad
Department of Mathematics-Informatics
310330 Arad, 2 Elena Drăgoi
ROMANIA
E-mail: mihaeladacianacraciun@yahoo.com