Babeş Bolyai University Cluj Napoca

Mathematics and Computer Science Faculty

http://www.ubbcluj.ro

Security issues in distributed systems

- Summary -

Phd. student : Incze Árpád

Coordinator : Prof. univ. dr. Grigor Moldovan

2015

Phd. Commision

President

Prof. univ. dr. Bazil PÂRV

Babeş Bolyai University of Cluj Napoca

Referents:

Prof. univ. dr. Adrian ATANASIU

University of Bucureşti

Prof. univ. dr. ing. Mihail ABRUDEAN

Technical University of Cluj Napoca

Prof. univ. dr. Florin BOIAN

Babeş Bolyai University of Cluj Napoca

Table of contents of this summary

Key-words: network and distributed system security, social engineering, visual cryptography and secret sharing, cryptographic key management.

Content of thesis

RELATED PUBLICATIONS

The author's publications:

[Incze04] dep. Informatică, contributor **Incze Arpad**, *Document intern: Raport de audit de securitate 2004*

[Incze05] **Incze Arpad**, Ioan Ileana, Manuela Kadar, *Increasing the security of an ACCESS database,* proceedings of „Several aspects on biology, chemistry, computer science, mathematics and physics", Oradea 2005 ISBN 973-759-142-9

[Incze10a] **Incze Arpad**, *Secret sharing & visual cryptography through bit sieve for fast image encryption,* proceedings AQTR 2010 THETA 17th International IEEE confernce on Automation,Quality and Testing, Robotics, ISSN 978-973-662-562-6

[Incze10b] **Incze Arpad**, *Pixel Sieve method for secret sharing & visual cryptography,* Proceedings of the 9th RoEduNet IEEE International conference, Sibiu, 24-25 june, 2010 in ***ISI Conference Proceedings Citation Index***

[Incze10c] **Incze Arpad**, Moldovan Grigor, Maria Muntean, *From pixel sieve to bit sieve. Bit level based secret sharing cryptographic method,* in proceedings 11th International symposium CINTI, Budapest 18-20 nov. 2010 978-1-4244-9278-7 indexat **IEEE**

[Incze11] **Incze Arpad**, *Social Enineering and education in fight against cybercrime*, Acta Universitas Apulensis- Special Issue, Proceeding of ICTAMI 2011, ISSN 1582-5329 p541-553 **B+ CNCSIS**

[Incze12] **Incze Arpad,** *A greater involvement of education in fight against cybercrime* 2nd WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES NEAR EAST UNIVERSITY 27-30 June 2012 NICOSIA – NORTH CYPRUS Procedia-Social and Behavioral vol 83 Journal ISSN: 1877-0428 by ELSEVIER ***ISI Conference Proceedings Citation Index***

[Incze14a] **Incze Arpad**, "*Cryptographic key issues and solutions for the bit sieve/pixel-sieve method*", *AQTR*, 2014, 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR) 2014, pp. 1-5, doi:10.1109/AQTR.2014.6857853 ***ISI Web of Science***

[Incze14b] **Incze Arpad**, *Solutions regarding some cryptographic key issues for the pixel-sieve cryptographic method* , 4th WORLD CONFERENCE on INNOVATION and COMPUTER SCIENCES (INSODE-2014) Sapienza University, Faculty of Economics April 11-13, 2014 Rome, Italy www.insode.org in AWERProcedia Information Technology and Computer Science // Global Journal on Technology ISSN: 2147-5369 **indexat AWER Index şi trimis spre indexare ISI**

[MunInc10] Maria Muntean, Honoriu Valean, Liviu Miclea, **Incze Arpad** *A novel intrusion detection method based on support vector machines*, proceedings of 11th International symposium CINTI, Budapest 18-20 nov, 2010. 978-1-4244-9278-7 indexat **SCOPUS**

Papers citing the author:

- Feldiansyah Bin Bakri Nasution, Dr. Nor Erne Nazira Bazin , Johor Bahru, Malaysia

Adjusting ICT Capacity Planning by Minimizing Cyber Crime Effects in Urban Area: A System

Dynamics Approach, Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2014), Yogyakarta, Indonesia, 20-21 August 2014

- Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *An improved Pixel Sieve method for Visual Cryptography* , International Journal of Computer Applications, Volume 12 No. 9 January 2011 ISSN 0975-8887

- Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *Modified Pixel Sieve Method for Visual Cryptography* Vaibhav Choudhary et. al. / Indian Journal of Computer Science and Engineering Vol. 1 No. 4 321-326

- Venkatesh M.R. , Roopanjali. Daddi, *SDS Technique For Secret Image Encryption,* International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013 ISSN: 2278-0181

- Siddharth Malik, Anjali Sardana *A Keyless Approach to Image Encryption,* 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 $26.00 © 2012 IEEE DOI 10.1109/CSNT.2012.189

- Koteswari, S.; Paul, P. John; Indrani, S., *VC of IRIS Images for ATM Banking,* International Journal of Computer Applications, Volume 48 No. 18 June 2012 ISSN 0975-8887

- Deepak Aeloor,Amrita A. Manjrekar *Securing Biometric Data with Visual Cryptography and Steganography,* Security in Computing and Communications, Communications in Computer and Information Science Volume 377, 2013, pp 330-340 SprimgerLink ISBN 978-3-642-40575-4

- Anisha K Jose, Panchami V, *AN EFICIENT APPROACH FOR SECRECY BY SDS ALGORITHM* International Journal of Emerging Trends in Engineering and Development Issue 4, Vol.2 (March 2014) ISSN 2249 – 6149

- Kandar, S.; Dhara, B.C., "*Random sequence based secret sharing of an encrypted color image*," Recent Advances in Information Technology (RAIT), 2012 1st International Conference on , vol., no., pp.33,37, 15-17 March 2012 doi: 10.1109/RAIT.2012.6194475 IEEE

Also the author was invited to CINTI[1] 2010 conference to present a workshop about cyber-crime and education .

[1] 11th IEEE International Symposium on Computational Intelligence and Informatics, November 18-20, 2010 Budapest, Hungary.

EXTENDED SUMMARY

Introduction

Communication represents one of the most important necessities of the modern society. The communities are inspired by this power which lies at the basis of the society's nowadays progress .

The way in which people communicated along time developed at the same time with the society's development. The society's progress in the communications field has allowed us to pass from slow ways of communication with great latency, uncertainty, inefficiency with serious distance limitations, to quasi-instant , global ways of communication and with a high degree of security. As a matter of fact, there isn't any branch of economy which doesn't depend on communications , as well as other components of society are in a large measure dependent on communications: governance, education, health, justice, and so on. The lack of co-ordination on a building site , discontinuities in the sub-assemblies supply of a serial manufacture, the impossibility of alarming about an event that occurred or is impending and jeopardizes lives , represents as many situations as those in which the lack of communication leads to the disturbance of the natural order of things or worse, it leads to damages which could have been prevented or avoided.

The system of communications must be trustful from the confidentiality's point of view and even more from the availability and stability's point of view. A communication system which presents frequent function discontinuities , fluctuations concerning the service's quality or represents drawbacks concerning the confidentiality and the integrity of facts will eventually lead to its desertion in the prejudice of usefulness or social convenience.

If the technological progress in the communications field has solved and continues to solve most of the problems related to the speed and safety in which an information is spread, the same technological progress allows a certain class of society in which we live, to use for itself and in the prejudice of the society the instruments and the ways of communication. The wide spread of computer's network, the global computer's network ,the under structure which lays at the basis of the shared systems, are exploited by these individuals in less useful purposes for the society and , as a matter of fact, illegally.

Information transmission and the security problems from the information transmission have occurred about at the same time. The information that have been transmitted or stoked can have a certain value. The person who holds the information possesses value. So, the information became a target and the art of interception and distinguishing the information a " trade ".

Scope of thesis

This thesis follows two purposes. On one hand, it presents a synthesis of the ies of distributed systems, on the other hand it suggests some solutions to improve the security of this systems . This solutions are from the field of visual cryptography .

The security issues that are going to be discussed, answer the questions „What happens if the security services and devices are avoided? How can these services be avoided? What can be done in order to prevent these situations?

In the paper, there are synthetically presented the techniques used by the hackers to enter the wanted systems. When this part was elaborated, it had been taken into account the yearly and multi annual reports of some specialized companies from the field of IT security, emphasizing on the most frequent attack methods. At the same time with the short presentation of these techniques there are described the solutions to reduce the vulnerabilities.

As a research project, the author has worked on the security audit of an institution. This audit had as a purpose the establishing of the informatics system and institution vulnerabilities . In this purpose the institution's network of computers was subject to a set of informatics attacks in order to detect the existent vulnerabilities.

From the analyze of the data regarding the methods of illegal penetration in the informatics systems clearly results that the weakest link is the human user. So, it requires a study on the reasons why people are the target. So, the author has done a short research regarding the social aspects of the informatics delinquency. In this chapter we underlined the members of the society ,s lack of knowledge . Solutions have been proposed for improving the situation. One o these solutions aims the compulsory education of the users about the IT security.

Besides the theoretical side, regarding the security aspects of the shared systems, also as his own contribution , the author suggests a new cryptographic method . This method has roots in the field of visual cryptography . As so many times in cryptography , this visual cryptographic method it's also like a primitive for complex methods. Although in the paper the stress is on the visual method, the author also suggests a cryptographic method for the binary information based on the same principle as the visual method. In this paper there are described the steps of the method's development from the fundamental idea to a version acceptable from the safety's point of view . The suggested method can be used to encrypt images and files.

After testing and improving the method , the author suggests, besides the obvious use the encryption of information, a few possible applications from the field of distributed system security. Those proposals are: authentication , digital signature and cryptographic key-management. The suggested authentication method strengthens the classical authentication

based on the NAME – PASSWORD pair. For this an image must be interpreted like a CAPTCHA. In order to be able to answer the CAPTCHA challenge the user has to decrypt and interpret the image. The digital signature method of the image is based on a specific feature of the open cryptographic method by which we can get a partition of a wanted size of the encrypted information. The digital signature provides originality to information and authenticity of the sender. These applications are subject of some further researches and later developments of the suggested method.

History has proved that no matter how sure a cryptographic method would be at a certain time, sooner or later, a weakness of the method will be found and exploited. So the author decides to further improve the method .

Issue statement

”There is strength in numbers”—it is also the principle that lays at the basis of distributed systems development. It is accepted as a wide spread definition for distributed systems the statement that a distributed system of calculation or distributed informatics system is the large number of programmers from a computer network with the purpose of solving certain problems by sharing the resources of networked computers[2]. This approach results in a fast solution of the problems by sharing the tasks on the system’s nodes.

When it’s all about sharing tasks, the distributed systems inherits the computer networks security issues. So the security issues of the computer network are also the security issues of the distributed system.

Let’s discuss a way of communication between individuals for example, a simple act of talking. The situations in which talking it is hindered by a certain thing (cause) or it’s disturbed by the many voices nearby, these are exceptional situations and the individuals find ways of avoiding or improving them. In the situations in which communication is affected , the individual identifies the causes and corrects them, for example he goes to a direction which allows him to communicate better with the collocutor. It is noticeable that those involved in communication participate efficiently to the communication improvement by their actions .

As the virtual society is a quasi- alike resemblance of the real society[3], the situation is similar in the case of electronic society : the impossibility of communication between two

[2] Ioan Dziţac, Gligor Moldovan, *Sisteme distribuite. Modele informatice,* Editura Universităţii Agora, 2006 isbn 10 973-87960-9-1

[3] ing. Valer Bocan, *CONTRIBUŢII LA CREŞTEREA DISPONIBILITĂŢII, SCALABILITĂŢII SI SECURITĂŢII SISTEMELOR DE COMUNICAŢIE*, Teza de doctorat, Universitatea “Politehnica” din Timisoara 2006

entities can be determined by an attack of access denial (Denial of service – Dos) and a weak communication can be determined by the lack of scalability in the communication system. For the improvement of these situations, the systems involved in communication need to have methods and action protocols for detecting, avoiding or removing the facts that disturb communication. We can distinguish three parameters of the communication systems which define and measure the quality of communication :

*The **availability** of a communication system represents its ability to be ready to organize a transmission in a reasonable time. The lack of availability can be due to physical interruption of the communication way (telephone wires , network cable , radio transmitter) or it can be due to a DoS attack which hinders the dates transfer on all its extent .*

*The **scalability** of a communications system represents its capacity to adapt to different loading scenarios. It is better to avoid fast failure of the service as they could later be exploited by an attacker. Generally, the sharing protocols help the clients one by one and represent a stagnation of the performance that could have been obtained by a concomitant approach of distribution.*

*The **security** of communications represent the capacity of the system to function in normal conditions under the action of some external disturbing factors. Traditionally, when we speak about security we think about protection and confidentiality of the data transmitted by the system, and there are many protocols and security procedures that travel from different areas. The availability and the scalability directly affect the level of security of a communications system so, we consider that a fair approach of the security improvement requires a growth of the two factors.*

Information security

The fundamental notions together with the word security are the following: attack, compromising, intrusion , defend, detection , security mechanism. All these aspects are discussed in details in the specific literature[4].

By attack we understand any kind of voluntary action we use to interfere in the information communication, with the purpose to **interrupt, intercept, modify and falsify the information.**

Classifying the types of attacks we can notice **passive attacks** (message interception, traffic analysis) or **active attacks** (the retransmission of some modified messages, the transmission of some false messages , blocking some services by DoS attacks.

The security mechanisms are meant to detect certain attacks and together with the security services it has to prevent or remove these attacks. The security services provide the user or the system some instruments by which the following are prevented:

- The **access control** that guaranties that only the aimed persons , with certain privileges have access to the resources. This thing is possible most of the time by using the so called login credentials which is a combination of user names-password which has to be introduced in order to have access in the system or to a system resource. If the name of the user can be seen by other individuals , the password has to be secret and known only by the authorized person or persons.
- **Confidentiality and integrity of data** . Data can be accessed , checked , manipulated only by the legitimate users and can not be altered by unauthorized individuals.

---

[4] Schneier, Bruce - *Secrets & Lies*, Wiley Publishing, Inc., 2004

D. E. Comer. *Internetworking with TCP/IP: Principles,Protocols, and Architecture,* volume I. Prentice-Hall, Englewood Cliffs, NJ, second edition, 199

Steve Bellovin, *Security Problems in the TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, no. 2 (April 1989) pg 32-48

Steven M. Bellovin, *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 20th Annual Computer Security Applications Conference (ACSAC), December 2004, in as part of the "classic papers" track.

L. Joncheray. *A simple active attack against TCP,* Proceedingsof the Fifth Usenix Unix Security Symposium, Salt Lake City, UT, 1995.

Burtescu Emil, *"Securitatea Datelor în Sistemele Informatice Economice*", 2004

Peter Norton , Dave Kearns, *Rețele de calculatoare,* Editura Teora, 2002

Andrew S. Tanenbaum, *Rețele de calculatoare,* Computer Press Agora 1998 (traducere)

- The **availability** of the resources guaranties that at every moment a legitimate user will have access to the system's resources. The distributed system excels at this chapter. It provides functionality to the entire assembly even if some nodes from the system are taken out of use.
- **Authenticity and non repudiation** guaranties on one hand the identity of the participants at a communication session and on the other hand it excludes the user's refusal to admit the access to a certain resource or to deny transmission of a certain information.

Vulnerabilities

The vulnerabilities of the distributed systems are divided in a few major categories which will be shown here:

1. **The physical vulnerability of communication channels** which means that physics access to the under structure used to transport and manipulate the information. Due to the fact that the distributed systems are based on public communication channels (by example the global network World Wide Web) it's impossible to keep it safe. If the working stations are kept in a locked room not the same thing can be said about the communication channels for the information ,especially if these information exceed the institution's area.

2. **The terminal's physics vulnerability** although apparently it shouldn't be a problem by placing the sensitive junction in locations with limited access, in reality there are many cases when the information are compromised from distance by the remote procedure.

3. **Vulnerabilities concerning the access to information** regarding the substructure that the information travels on , comes from the physics vulnerability shown in point 2. The logical access is translated by the access to the informatics resources after there is physical access to the working station. There can be noticed the following words: authentication, access , digital signature, non repudiation.

4. **Vulnerabilities concerning the information itself.** Here we can talk about the interpretation of the information. If it can or ca not be interpreted. Also some should consider the possibility of modifying the information or to block the information transfer.

To secure an informatic system means to approach every type of vulnerability previously discussed. The result is a layered structure on levels of security"

- The external level , at the physic level, to limit the access to the communication channels.
- If unauthorized individuals still find access to the communication channels ,the

access to critical nodes should be limited to avoid information being extracted, modified, etc.

- If inadequate individuals find access at the junctions \terminals of the system, to limit as much as possible the logical access to information (authentication, limited rights)
- If the security to the access to information is compromised and the information is extracted , then, at least this information needs to be in a shape that can not be interpreted by unauthorized individuals. The sensitive information must be encrypted.

Cryptography. Visual cryptography. Secret sharing

The last line of defense against the vulnerabilities mentioned above is the hidden of the information that travels through the network. For this situation, the data have to be encrypted. So, cryptography plays a very important role in the security of the data communications.

Both in the case of distributed systems and also databases, securing them, means securing the messages and the transactions in the system.

The cryptography is a "tool" useful to provide the security of the system. It is not the only one , other measures have to be taken like implementing security politics to ensure the system's security. There are two types of cryptographic systems: symmetrical and asymmetrical. The symmetrical systems (with one secret key) use the same key to encrypt and decrypt the messages. The asymmetrical systems use two keys. One key to encrypt, another key to decrypt the message. The cryptographic algorithm used in cryptographic systems are divided in stream ciphers and block ciphers. The stream ciphers can clearly encrypt a single bit from the text in a certain moment ,while the block ciphers encrypt more bits (usually blocks of 64 or 128 bits) at the same time.

Visual cryptography is that part of cryptography which aims to encrypt visual information. It happens many times that the transmitted information by the network to be visual information. For example, a bank scans the client's contracts and sends them electronically to the centre. These contracts need to be encrypted so even if the data would be intercepted , the information couldn't be extracted or interpreted.

THESIS CONTENT

Chapter 1 . **Introduction**. It responds to the question: why I have chosen this theme? There have been described on short the constitutive elements of the distributed system of calculus, problems regarding the security of the distributed systems.

In **chapter 2**, after a short presentation of the general ideas from this paper, there is a presentation of the main players from the field, of those who deal with finding and exploiting the vulnerabilities, the so called hackers.

In this chapter there is also a review of the most important methods to penetrate the informatics security systems. To be able to do this, I have used the data from a few specialized companies in IT security. The most useful instrument was the yearly report of the VERIZONE[5] company. These reports are presented in some tables.

Threat	**Attack type**	**% of attacks**	**% compromised records**
Malware	Key logger and Spyware	19%	82%
Malware	Backdoor and/or RAT	18%	79%
Hacking	SQL Injection	18%	79%
Abuse	Abuse of privileges	17%	1%
Hacking	Unauthorized access using default credentials	16%	53%
Abuse of privileges	Violation of security policies (access to PC, mail, internet, within the organization)	12%	less 1%
Hacking	Unauthorized access thru misconfigured access points	10%	66%
Malware	Packet sniffer	9%	89%
Hacking	Unauthorized access with stolen credentials	8%	less 1%
Scam	Social engineering	8%	2%
Hacking	Bypassing authentication	6%	less 1%
Physic	Physical theft of data storage components	6%	2%
Hacking	Brute force attack	4%	7%
Malware	RAM Scraper	4%	less 1%
Scam	Phishing	4%	4%

Table 1 main attack trends and their incidents

[5] http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

The following statistical values reflect a wide spread situation among the logins of the shared systems and computers networks which is the fact that not the lack of security instruments represents the main reason for the security gaps but the lack of information in the area and also the lack of using these security systems. Here are the facts:

69 % from the gaps have been discovered by others after the employees have noticed certain unusual situations and they asked for an expert examination.

83 % from the attacks were not difficult and the hackers didn't need any special information .

Only 17% from the attacks were complicated.

87% from the attacks could have been avoided by using some elementary security instruments ! This last number it is shown also by the results of the author's experiment along the security vulnerability evaluation of an institution.

Let's make an X-ray of the social aspects and of its social- economical implications. There are aspects that have been discussed about the informatic delinquency and after an inspection to see how the society relates to this event there are certain solutions to solve the situation. The solutions imply , in the first place education. The conclusions of this chapter would be that the population it is not ready to face the attacks and this lack of education it is due in the first place to the lack of elementary knowledge and decency of those who use the computer.

As much as from the conclusions presented in this chapter as from my own experience , due to the security audit that had taken place at the appointed institution, it results that the weakest link on the security component's list is the human user. The methods, the tools and the ways to secure a system do exist! If they are properly applied, they would considerably make a hacker's work more difficult.

Once the protection methods developed and they have been automatically introduced in the communication systems , the attackers don't try to open gaps in these systems. Their target is the user. Because the user is not experienced or educated in this field, so it offers all the ways to access the system .

In **chapter 2.3.1,** to prove this point of view , I have applied a test in which a group of students was asked to install an application. But, while it was installing, on the computer's screen warnings have appeared which indicated the fact that the application is harmful.

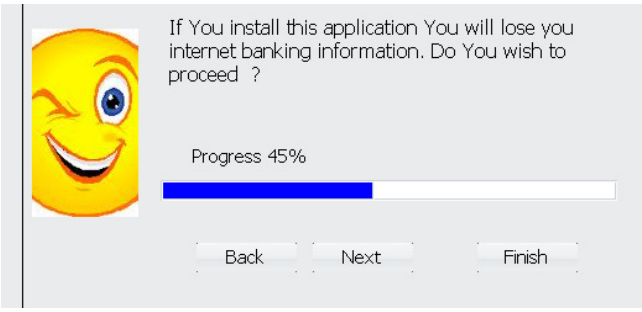

Figure 1 Warning message during installation

The test has been applied on three groups each of 20 students from different specialities. Unfortunately, the results of the test were surprising but also as expected. The following table shows the test results.

Main subject	IT knowledge	Promoted	Failed
Public Administration	medium	5	15
Accounting	Medium to good	8	12
Informatics	Excellent	2	18

Table 2 Results of the awareness test

The results speak about themselves. More then 80% from the subjects agreed to install an application which is going to warn them about a malicious application. What can we say about other applications which respect the form of the messages or gets installed without giving any information? As it can be seen from the test's result, people can be „convinced'' (fooled) easy enough. The success of placing some backdoor applications and the superficial way of installing a program underlines the necessity of education for the users. This education needs to start from school and to continue even after finishing school, at work where the computer systems are involved.

Chapter 3 Is a synthesis of the computer's networks as a stand for the distributed systems, the accent being on their vulnerability. The TCP\IP layers are discussed on short by their vulnerability's point of view. There are also described the tools used to prevent the attacks. Firewall technology is presented among others as a defense line against attacks.

Chapter 4 contains the audit of security's stages of an institution. The purpose of this experiment was to determine the vulnerabilities of the informatic system at that time. By this security audit , the identification of the security vulnerabilities, the identification of the

unauthorized level of access (by where a hacker can get into system), but also the identification of the minimum level of knowledge a hacker needs in order to get into the system. There are two possible ways: an attack organized by an internal employee with limited access to the network's nodes or to simulate an external attack.

The internal weaknesses of the institution's IT architecture have been tested from the following point of view:

- Physical access to the equipments and junctions of the network **ch. 4.2.1**
- Logical access to the information from the computers **ch. 4.2.2**
- Remote access to the computers and to the resources from the internal network **ch. 4.2.3**
- Penetration possibilities to outside in order to transmit information outside the institution **ch. 4.2.5.1**

During the tests we have succeeded to access from an insignificant junction of the information network, stations placed in departments with a high degree of confidentiality. This thing is possible due to a wrong made design and deployment of the network. The computers from the network also presented default settings that allowed a successful hacking.

If in case of a internal attack the purpose is to determine the network configuration defects, in the case of an external attack the purpose is to find the weaknesses which allowed to access from outside the institution's resources.

A Backdoor application needs to be installed to allow access to the organisation's internal network.

In **Chapter 4.3** the deployment of a social engineering attack is illustrated. This attack was meant to test the possibilities of installing a backdoor virus on to computers within the organization. Once the backdoor virus installed it would allow us to hack the system. The strategy to achieve this was to fool some employees of the institution to install an apparently harmless application.

The attack was put in scene in three steps (**chapter 4.3.1**)

Step 1: Planning and information gathering

Step 2: Pretexting, finding a reasonable motive

Step 3: deploying the attack and measuring it's effects

A forged email was sent to a target group of employees. In that mail a security alert was issued and the recipient was asked to install a security patch regarding the antivirus software used within the organization. But the patch was just a small software which allowed us to count the number of "infected" computers. For this at the end of the fake installation the user had to

reply with a code generated by the application.

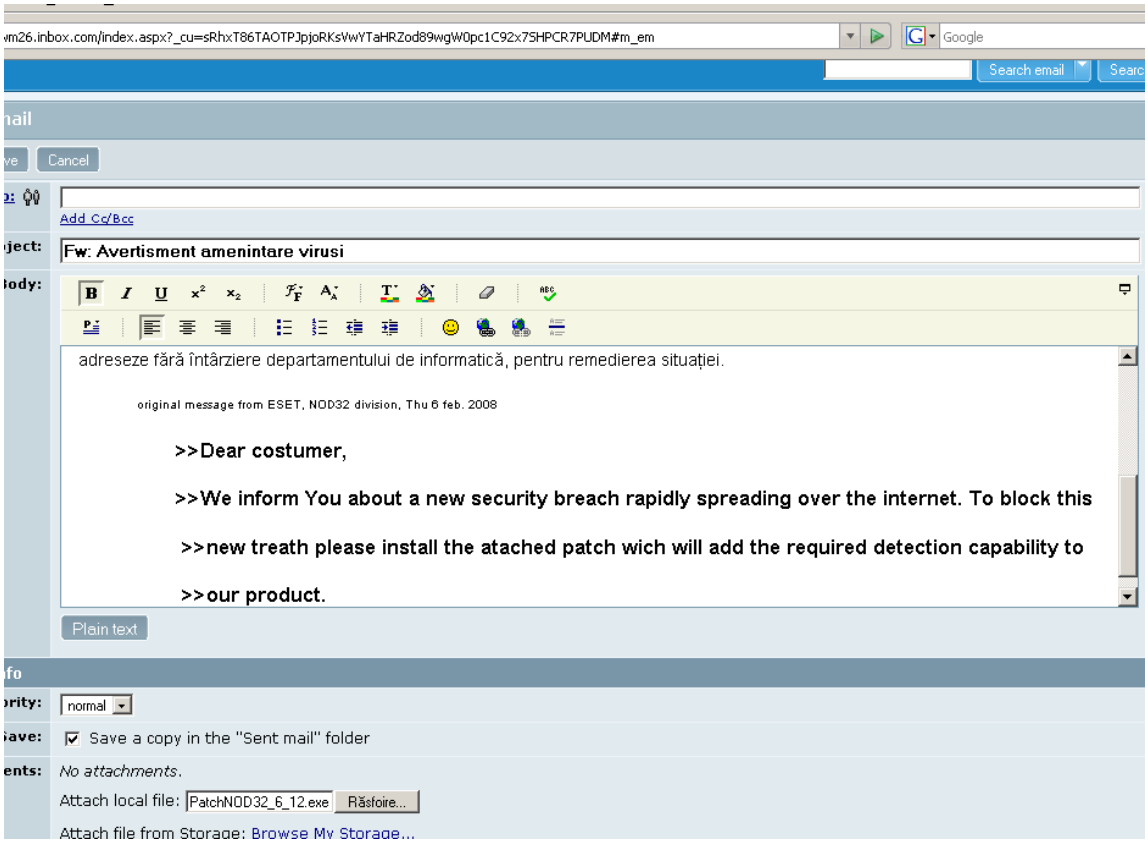

Figure 2 The forged message

The message has been sent to 36 persons. In the following table it can be seen the situation of the confirmed e –mails, which translates as a successful BACKDOOR installation.

Day	0(expedition)	1	2	3	4	5(alarm)	6,7	total
Confirmation	19	12	4	5	4	3	4	51

Table 3 Success rate of a social engineering attack

CHAPTER 5 is dedicated to cryptography as the last line of defense. After a short introduction, the author describes the stages of his own cryptographic method's development , from the original idea to the finished product.

The concept of **pixel's sieve** has the following fundaments.

Visual cryptography which has as its purpose to hide the information represented as an image. The original image has to be reproduced from the image that has been encrypted. In some cases we can talk about a partial reproduction, situation in which the image that has resulted needs to be interpreted by a human user. From this point of view, our method can be placed in both categories. We can have a decrypted image, identical with the original one or we can have a decrypted image with noise but which can be interpreted by humans.

Secret sharing[6,7,] is a method to protect the information by which the information is divided in partitions. There are certain requirements regarding these partitions:

- A partition by itself can not supply enough information to be able to understand the whole message.
- Regarding the method, to remake the original message all or at least a certain number of partitions are needed.
- As certain requirements regarding the partitions, the dividing method also has a secret key. Reconstructing the image is possible only in the presence of the key.

Secret Sharing Visual Cryptography (SSVC) is obtained when the two principles stated before are brought together. In early SSVC schemes sharing the initial secret were done by printing the partitions on transparent sheets8. To distinguish the image it is enough to put the sheets on top of each other.

Chapter 5.3 Pixel Sieve

Starting from this situation I have suggested the method of sieving the pixels. The concept is a simple one and it consist in generating images which are the two partitions by sieving the pixels of the original image through the pixels of a key image. If the key image has got irregular holes we can imagine that certain pixels of the original image fall through the holes (black pixels) and pixels situated over the white pixels would stay on the sieve. The pixels that go through the sieve form one partition, the pixels that stay on the sieve form the other partition.

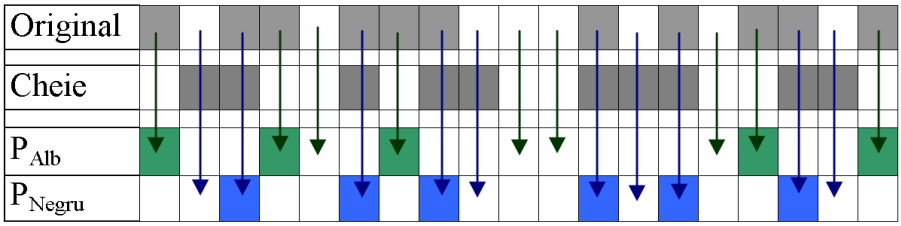

Figure 3 The concept of sieving

Like in the case of de Shamir's [Sham79] method we have the basic components:

- The secret key
- P_{Alb} The share corresponding to a white pixel of the key
- P_{Negru} The share corresponding to a black pixel of the key

Replacing the black and white pixels of the key with 0's and 1's the following formula describes the method:

---

[6] Ronald L. Rivest, Adi Shamir, Yael Tauman *How to share a secret* - Communications of the ACM , 1979

[7] Gustavus J. Simmons *How To (Really) Share A Secret* , 1998

[8] Moni Naor and Adi Shamir, *Visual Cryptography,* EUROCRYPT 1994, pp1–12 [1].

$$P_{ij}^{0} = \begin{cases} O_{ij}, \text{ if } K_n = 0 \\ \text{x random, if } K_n = 1 \end{cases}$$

$$P_{ij}^{1} = \begin{cases} O_{ij}, \text{ if } K_n = 1 \\ \text{x random, if } K_n = 0 \end{cases}$$

$\mathbf{P_{ij}}$ the value of the pixel in position *i,j* in share 0 or 1 with consideration to the bit of the key.

$\mathbf{O_{ij}}$ is the value of the pixel in the current *i,j* position from the original image

$\mathbf{K_n}$ current position in the key; $K_n \in \{0,1\}$

The process is presented in the following figure

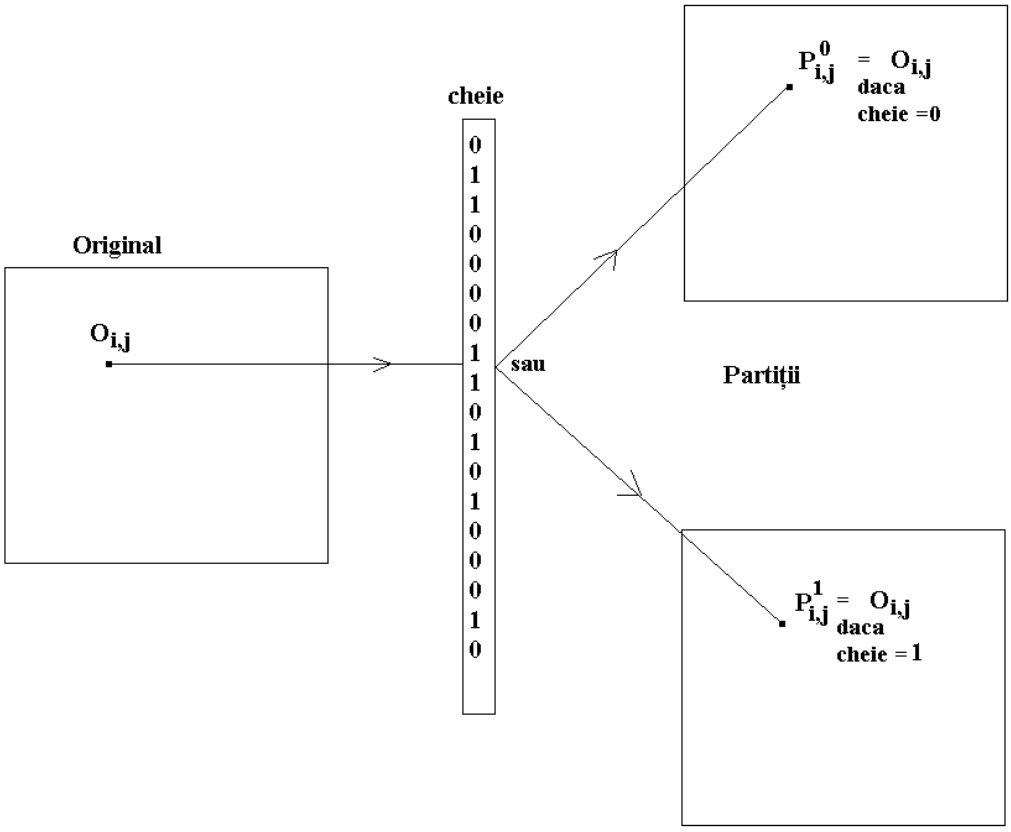

Figure 4 Generating the share through the bits of the key

The concept in its primary form is not safe, improvements are necessary to reach the cryptographic requirements. The steps by which the concept progresses are described in the pages that deal with that chapter. More possibilities of improvement are described in the paper. They refer either to improvements which take into consideration the human physiology, the way in which the human eye distinguishes the image, or the improvements brought by cryptographic methods and techniques. These methods are the transposition, logical operations (XOR), different techniques to read the original information, to add supplementary keys for a more

secure method.

Chapter 5.4 From pixel to bit. By replacing the black and white pixels with 0's and 1's we get the ***bit sieve***[Incze10c]. If ***T*** is the clear text with length **n**, ***C*** encryption key with length ***k***, ***P₀*** and , ***P₁*** the shares, all in a form of binary string:

Clear text	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1
Key	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0
Share 1	x	x	x	x	0	1	X	1	x	1	0	X	1	x	1	x
Share 0	1	0	0	1	x	x	0	x	0	x	x	0	x	1	x	1

Table 3 example for bit sieve with *overall advance*

Clear text	1	0	0	1	0	1	0	1	0	1	0	0	1	1	1	1
key	0	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0
Share 1	0	1	1	1	0	1	1									
Share 0	1	0	0	1	0	0	0	1	1							

Table 4 example of bit sieve with *partial advance*

For the *bit sieve* we can state :

$$T = \{w = t_1 t_2 ... t_n \mid t_i \in \{0,1\},\ i = \overline{1,n}\ \}$$

$$C = \{u = c_1 c_2 ... c_k \mid\ c_j \in \{0,1\},\ j = \overline{1,k}\}$$

$$P_0 = \left\{ \begin{matrix} t_i \ \ if \ \ c_x = 0 \\ random \ \ if \ \ c_x = 1 \end{matrix} \right\}$$

$$P_1 = \left\{ \begin{matrix} t_i \ \ if \ \ c_x = 1 \\ random \ \ if \ \ c_x = 0 \end{matrix} \right\}$$

$$where \ \ x = \left\{ \begin{matrix} i \bmod k, if \ \ i \bmod k \neq 0 \\ k, if \ \ i \bmod k = 0 \end{matrix} \right\}$$

Chapter 5.5 Key expansion

An omnipresent issue regarding the encryption key is related to its length especially when a user is asked to enter it from the keyboard. Humans usually tend to use short passwords.

There are several well known methods (usually hashing) to expand the password to a usable encryption key. Another solution is ***Liner Feedback Shift Registers*** or LFSR. LFSR is used to extend a binary key by XOR and cyclical shift. A similar method is proposed in the thesis.

Chapter 5.5.2. Key Shifting and XOR for key expansion

We will use the XOR operation on the bits of the original key as follows:

Let there be a binary key A={a_i (0,1)} We intend to build the key B ={b_i} as follows. First we XOR the first two bits of the key A.

$$b_1 = a_1 \; XOR \; a_2$$

The result is XOR-ed with the second bit of the key. The new result is XOR-ed with the third bit and so one.

$$b_i = b_{i-1} \; XOR \; a_i \qquad i=2,n$$

An example of generating a new key with XOR is shown in Table 5.

a_i	1	1	0	0	0	0	1
b_i	0	1	1	1	1	1	0

Table 5 example of XOR to generate a new key

We noticed that we can continue generating the new key by starting over the bits of the original key and XOR-ing them with the current bit of the generated key one more time before repetition of block occurs. We can write the following formula:

$b_{n+i}=a_i \; XOR \; b_{n+i-1}$ or $b_k=a_{k \bmod n} \; XOR \; b_{k-1}$

where **n** is the length of the original key and **k**=(1..2n).

The result for one round of key expansion is presented in Table 6.

a_i	1	1	0	0	0	0	1	*1*	*1*	*0*	*0*	*0*	*0*	*1*	*i=(1..n)*
b_j	0	1	1	1	1	1	0	1	0	0	0	0	0	1	j=(1..2n)

Table 6 example of XOR to generate a new key with block repetition

Unfortunately if the result of the XOR operation at the end of the first iteration equals the first value of the generated key the second half of the generated key will be identical with the first half. The main issue here is the repetitive blocks. In cryptography repetitive blocks of the key are to be avoided. To correct this issue we introduce a new rule.

$$if \; b_1 = b_n \; then \; b_{n+1} = NOT(b_n) \; XOR \; a_1$$

Another advantage of this method, actually a requirement for cryptographic methods, a slight change in the original key will result in an avalanche of changes in the expanded key. This is true because each value of the expanded key depends from each previous value of the original key.

The cyclical shift

So far we can generate a **2n** length expanded key from an **n** length original key. To further increase the length of the generated key we will continue with the same XOR-ing

operation but after cyclically shifting the bits of the original key.

$(a_1, a_2, \ldots a_{n-1}, a_n) \rightarrow (a_2, a_3, \ldots, a_n, a_1)$ $\quad a_n=a_1 \quad and \quad a_i=a_{i+1}$, i=(1..n-1)

For a given key with the length of **n**, Because **n** such circular permutations can be done, and for each permutation a **2n** length expanded key can be generated we get a total length for the generated key of $\mathbf{2n^2}$. For instance for an 8 bit (1 byte) long key the expanded keys length is 124 bit.

A short program to test the method was written. For simplicity we use the ASCII code of the characters converted in binary as key. The results is shown in Fig 5.

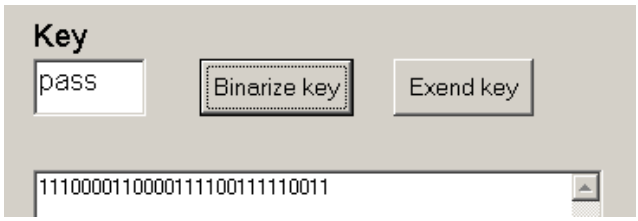

Figure 5 A key after bynarisation

Now we will apply the XOR expansion algorithm on the binary key. The result is presented in Figure. 6

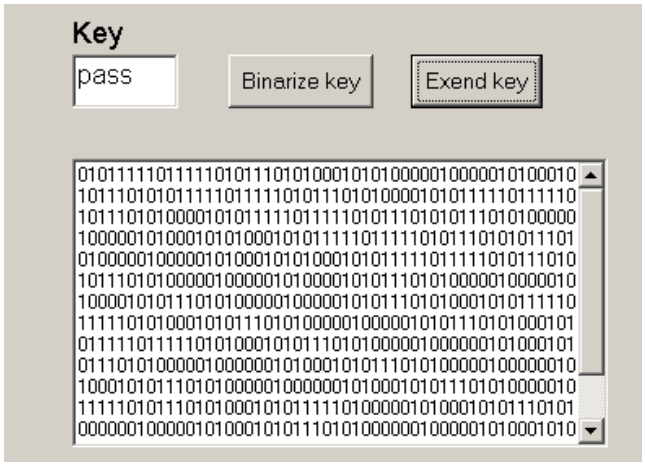

Fig. 6 The key **pass** after expansion

This model is a theoretical one. The application was written only to test the proposed method.

Although considerably increases the time needed to break the code with a brute force attack still the circular permutation of the key is predictable. Therefore in a real life situation we propose the introduction of a second, numeric, key. The role of this second key is to replace the circular shift with a pseudo random shift of the bits of the key. This numeric key can be chosen by the user.

For instance let there be the following secret number: 5368. After the first iteration of the

original key instead of cycling the key with step 1 we will cycle the key but with the step of 5 then in the next iteration with the step of 3 then 6 then 8. Thus for a given original key with the length of **n** we will get an expanded key with the length of 2*n*5 because we make only 5 iterations, one initial key and four shifted keys. For demonstration purposes we used a short number but a longer number can be used in a real case scenario. In this case an attacker will have to find not only the original key but the second numeric key too $\mathbf{N_k}$.

Obviously the information will be encrypted with the expanded key instead of the short original key.

Chapter 5.6 The L3 issue

Affecting mainly the pixel-sieve version this problem occurs when the number of a color in the key image, is much in favor of one share. For instance if the number of black pixels of the key image are considerably higher than the number of white pixels obviously the share corresponding to the black pixels will get more useful original pixel during the sieving process. Regardless of the quantity of the noise added to the share, because a lot of original data is already in a certain share, the image can be visually interpreted from that share only without the need of decryption. In Fig 3 such a situation is presented where in the left share the message is visible.

Figure. 7 The left share is readable due to more usable data.

After several empirical tests we have concluded that a maximum ratio between black and white pixels of the key should not be higher than 3. By empirical we understand that by dealing with visually encrypted images, those images were interpreted by humans. It is impossible to create an application that would analyze such an encrypted image due to the noise embedded to the encrypted image.

$$R_k = \frac{m}{n} \cong 1 \quad \Leftrightarrow \quad m \cong n$$

- R_k the ratio between black (n) an white (m) pixels of the key

An ideal ratio between black and white pixels would be 1, meaning that the number of black and white pixels are identical or at least very close. Thus the shares could get an equal number of pixels from the original image. We can replace black and white pixels with 0's and 1's of a binary key.

In figure 8 a situation is shown where the number of 0's is higher then the number of 1's ,

the corresponding share, n_0 will receive more data .

position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
key	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0
n0		1		2	3		4	5	6		7	8		9		10	11	12	13	14	15		16		17	18	19	20		21	22		23
n1	1		2			3				4			5		6							7		8					9			10	
δ	1	0	1	0	1	0	1	2	3	2	3	4	3	4	3	4	5	6	7	8	9	8	9	8	9	10	11	12	11	12	13	12	13

Figure 8 Distribution of data in shares

But with this requirement the number of usable keys are drastically reduced. For a given number of pixels (a given key length) only 1/3 of possible keys are feasible and an even smaller number of keys are safe for encryption due to some other restrictions like repetitive blocks or huge blocks of only black or only white pixels. For a total length L of a key if the number of 0's is b there are C_L^b possible different keys.

Chapter 5.6.1 Solution proposal. Threshold-swap

To overcome the L3 issue we propose the introduction of two counters $\mathbf{n_0}$ and $\mathbf{n_1}$. Each counter is associated to a share. and each time a share gets a bit/pixel the associated counter is incremented. Thus, the counters will store the total number of bits/pixels received by the associated share at a certain moment.

Also a third variable is introduced as **δ**, the difference in absolute value, between the above mentioned counters.

$\delta = | n_0 - n_1 |$

During the encryption/decryption process δ is constantly compared to a fixed value, a ***threshold***. If the threshold is reached there will be a swap in the shares. In this case, although the bit of the key would send the current pixel of the original image to share A, the pixel will be transferred to share B. Thus the difference in numbers of pixels received by each share will be no more than the threshold.

After a swap the shares should be swapped back soon after the next step (*local swap*) or they should remain swapped until the δ reaches the threshold again (*permanent swap*). A permanent swap example is presented in Fig. 9 where between positions 12 an 26 the role of the shares are swapped due to threshold overcome.

position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
key	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0
n0		1		2	3		4	5	6		7		8		9							10		11		12	13	14		15	16		17
n1	1		2			3				4		5		6		7	8	9	10	11	12		13		14				15			16	
δ	1	0	1	0	1	0	1	2	3	2	3	2	3	2	3	2	1	0	1	2	3	2	3	2	3	2	1	0	1	0	1	0	1

Figure 9 Example of distribution in shares with swap

There is a good chance that, in certain situations, modifying some bits of the key (during a brute force attack), by obtaining different values for the counter, swaps should occur in different positions therefore increasing the security of the method.

Both methods bring some enhancement to the original pixel-sieve and bit-sieve cryptographic primitives. The first method with swap between the shares solves pretty well the stated L3 issue.

The key expansion method helps us to generate long encryption keys with reduced computational power in reasonable time. Also the expanded key is totally dependent from the original key considerably reducing the success rate of a brute force attack.

With *threshold-swap* technique the extended key is practically replaced by a new key. We will call this key ***equivalent key*** in **Chapter 5.6.2** in which at certain positions the bits are switched.

$$C_e = f(\ C_i,\ threshold\ )$$

We represent this situation in the following Figure in which we noted *Ci* the initial key *Ce* equivalent key. The pink coloured cells shows the positions where the bits are switched

poziția	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
C_i	1	0	1	0	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	1	0
C_e	1	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1	0
n_0		1		2	3		4	5	6		7		8		9							10		11		12	13	14		15	16		17
n_1	1		2			3				4		5		6		7	8	9	10	11	12		13		14				15			16	
δ		0	1	0		0	1			2	3	2	3	2	3	2	1	0	1	2	3	2	3	2	3	2	1	0	1	0	1	0	1

Figure 10 equivalent key with regard to threshold

To further strengthen the method during encryption these keys will be used as follows:

- From the extended key, the equivalent key will be generated using *threshold-swap*
- The equivalent key C_{eq} will be used only to determine which share will get a certain bit. By this we assure that each share will get a reasonable amount of data
- The unmodified **extended key** is used to alter the **bit/pixel** transferred **with XOR** as follows.

Chapter 5.7 XOR cryptography to further strengthen the method

By simply moving a pixel to a certain share not much is solved. Because about half of the pixels are moved between shares there is plenty of information to visually interpret the image.

Figure 11 Unaltered pixels in a share

We use XOR cryptography to hide the information. Each colour component is XOR-ed with an 8 bit block of the extended key

In table 7 such a situation is presented

Initial colour	Colour code	key	Result XOR	Final colour
R	128=10000000	01101000	11101000=232	R
G	159=10011111	00011100	10000011=131	G
B	87=01010111	01110100	00100011=35	B

Table 7 changing the color by XOR on RGB components

5.8 Encryption and decryption by „sieving”

Summarizing the above mentioned reflections we arrive to the final form of the sieving based secret sharing cryptographic method.

Mc – clear message converted in binary **BMc**

Ci – initial key converted in binary **CiB**

$\mathbf{N_k}$ – numeric key – for the steps in key shift

T - threshold

$\mathbf{C_{ex}}$ - extended key in binary

$\mathbf{C_{eq}}$ **–** equivalent key in binary CEB=f(CB, threshold)

P – The share for values **BMc** $\oplus$ **CiB** where the $\mathbf{C_{eq}}$= 0

Q - The share for values **BMc** $\oplus$ **CiB** where the $\mathbf{C_{eq}}$= 1

$$M = \{w = m_1 m_2 ... m_n \mid m_i \in \{0,1\},\ i = \overline{1,n}\ \}$$

$$C_i = \{a = a_1 a_2 ..... a_k \mid a_j \in \{0,1\},\ j = \overline{1,k}\ \}$$

$$C_{ex} = \{u = c_1 c_2 ... c_k \mid c_j \in \{0,1\},\ j = \overline{1,k}\ \} \quad şi \quad C_{ex} = f_{Rk}(C_i)$$

$$C_{eq} = \{v = d_1 d_2 ... d_k \mid d_j \in \{0,1\},\ j = \overline{1,k}\ \} \quad şi \quad C_{eq} = f_T(C_{ex})$$

$$P = \left\{p = p_1 p_2 .... p_n \mid p_i \in \{0,1\},\ i = \overline{1,n}\ \right\} \quad (total\ advance\ )$$

$$or\ P = \left\{p = p_1 p_2 .... p_l \mid p_i \in \{0,1\},\ i = \overline{1,l}\ \right\} \quad (partial\ advance)$$

$$Q = \left\{q = q_1 q_2 .... q_n \mid q_i \in \{0,1\},\ i = \overline{1,n}\ \right\} \quad (total\ advance)$$

$$or\ Q = \left\{q = q_1 q_2 .... q_m \mid q_i \in \{0,1\},\ i = \overline{1,m}\ \right\} \quad (partial\ advance)$$

Where :

- ***M*** – clear binary text
- ***C_i*** **–** initial key (text ASCII)
- ***C_{ex}*** **–** extended key used for ***XOR***
- ***C_{eq}*** – equivalent key used to determine the share
- ***P, Q*** – the two shares

5.8.1 Encryption

Using the above mentioned notations we can state:

$$P = \left\{\begin{matrix} p_i = m_i \otimes c_x & if & d_x = 0 \\ p_i = random & if & d_x = 1 \end{matrix}\right\}$$

$$Q = \left\{\begin{matrix} q_i = m_i \otimes c_x & if & d_x = 1 \\ q_i = random & if & d_x = 0 \end{matrix}\right\}$$

$$where\ \ x = \left\{\begin{matrix} i \bmod k, if\ i \bmod k \neq 0 \\ k, if\ i \bmod k = 0 \end{matrix}\right\}$$

$$d_x \in \{0,1\},\ i = \overline{1,k}$$

Or for the partial advance version :

$$P = \{p_i = m_i \otimes c_x \quad if \quad d_x = 0\} \qquad p_i \in \{0,1\},\ i = \overline{1,l}$$

$$Q = \{q_i = m_i \otimes c_x \quad if \quad d_x = 1\} \qquad q_i \in \{0,1\},\ i = \overline{1,m}$$

5.8.2 Decryption

For the total advance we have:

$$M = \begin{Bmatrix} m_i = p_i \otimes c_x & if & d_x = 0 \\ m_i = q_i \otimes c_x & if & d_x = 1 \end{Bmatrix}$$

$$where \;\; x = \begin{Bmatrix} i \bmod k, if \; i \bmod k \neq 0 \\ k, if \; i \bmod k = 0 \end{Bmatrix}$$

The original message is rebuild bit by bit by from the corresponding share.

Chapter 5.9 Pixel sieve Application

A software application for image encryption using pixel sieve method was written mostly for experimental purposes. The interface shows the image, ask for the password as ASCII key , also the numeric key for key-shifting. After bynarization the extended key is shown in a text box.

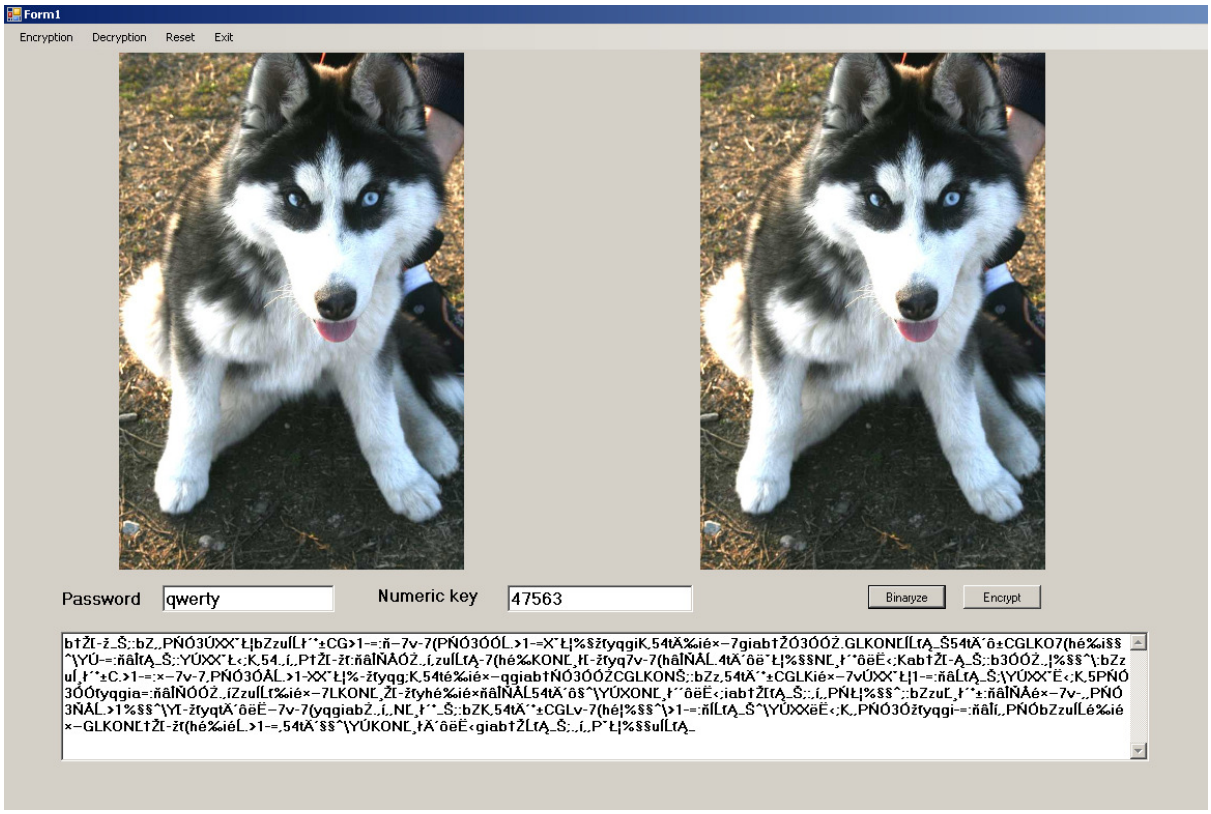

Figure 11 The pixel-sieve application in action

After encryption the resulting shares are presented for evaluation. This step is necessary because for certain keys, usually short ones with repetitive characters, can result in interpretable encrypted shares.

A well encrypted image is presented in figure 12.

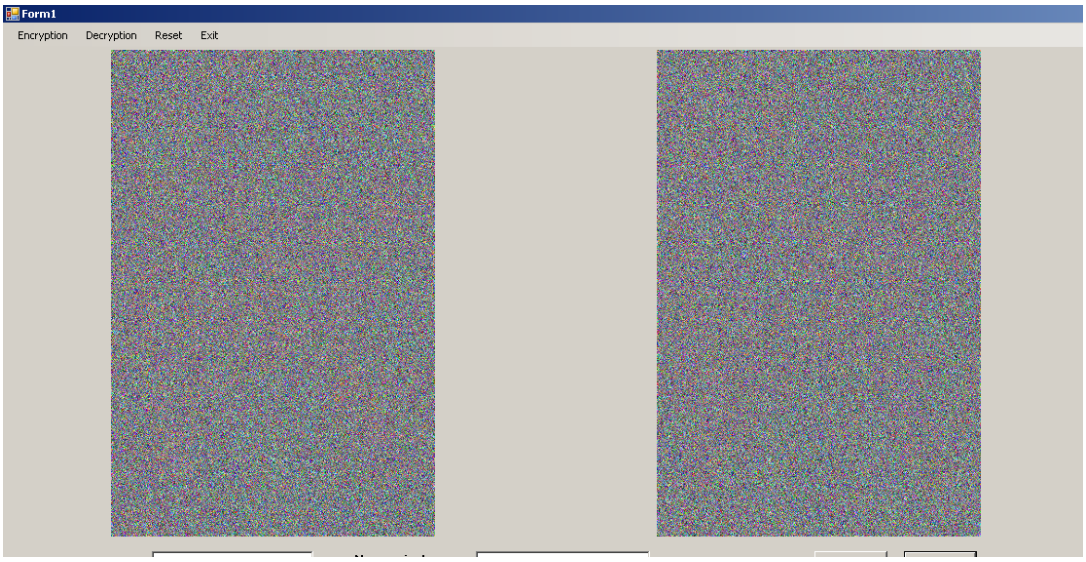

Figure 12 Encrypted images

Chapter 5.10 Testing the application

Several comparative and statistical tests were conducted to test the strength of the method. First the shares are compared with the original image.

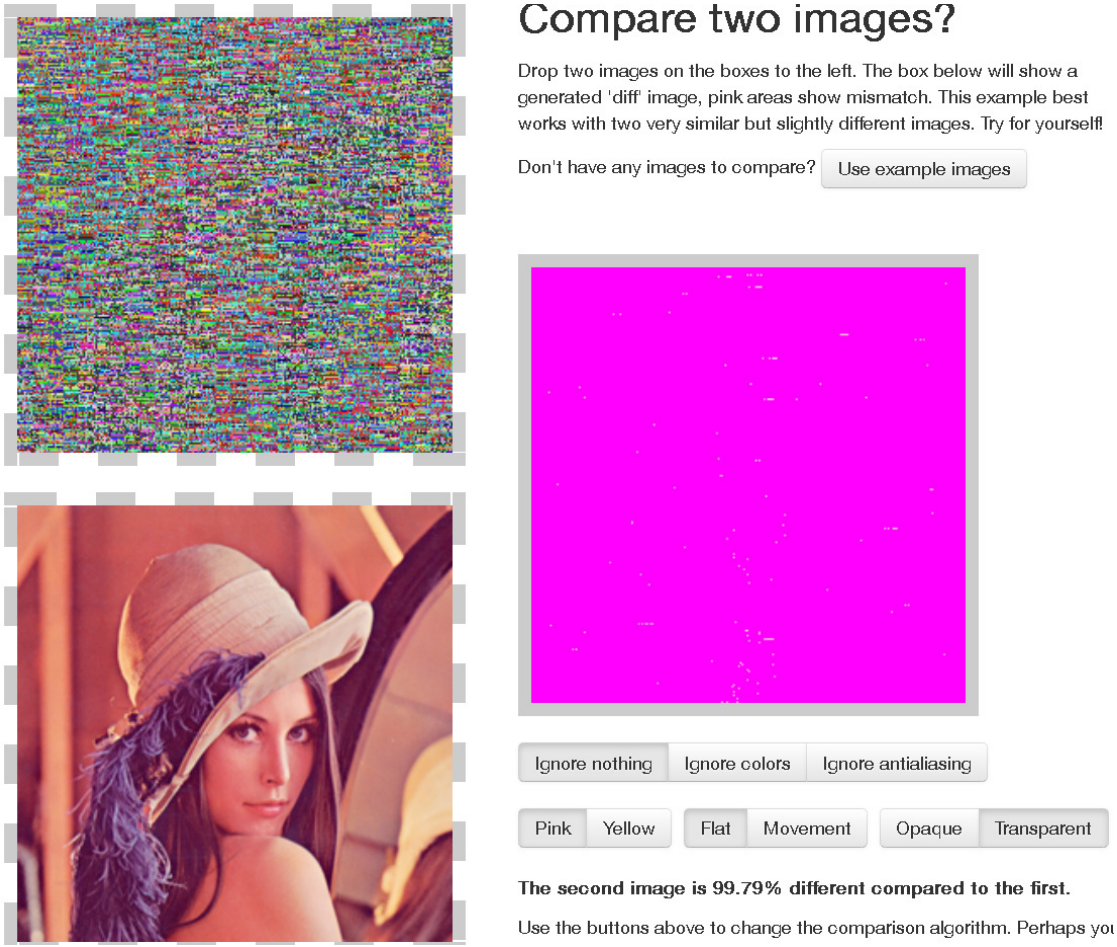

Figure 13 Comparing between original image and encrypted share

Second, the shares are compared against each other with very good result

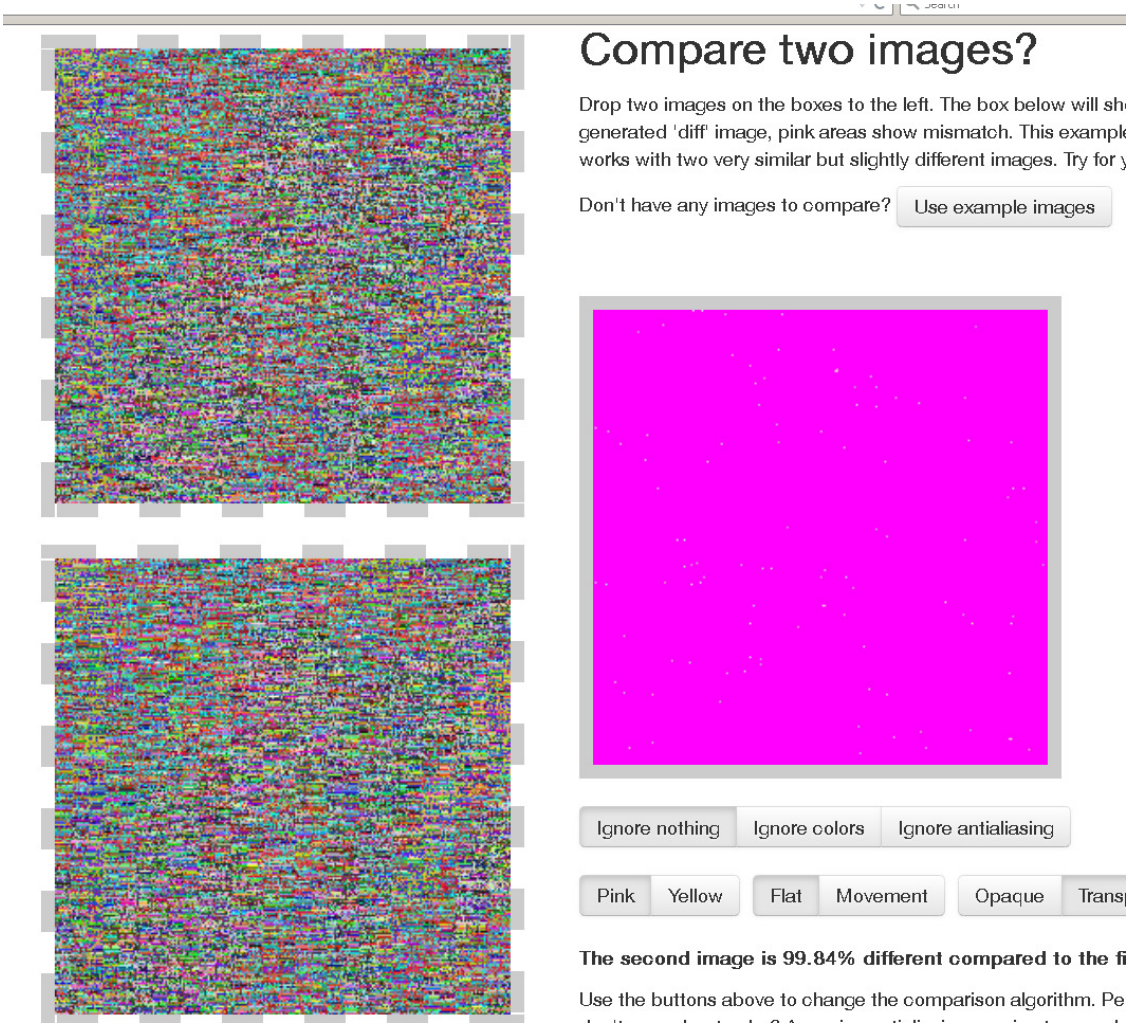

Figure 14 Comparison of shares

Also image processing filters were applied to see if there is any usable information left in the shares. For this we used several Photoshop filters

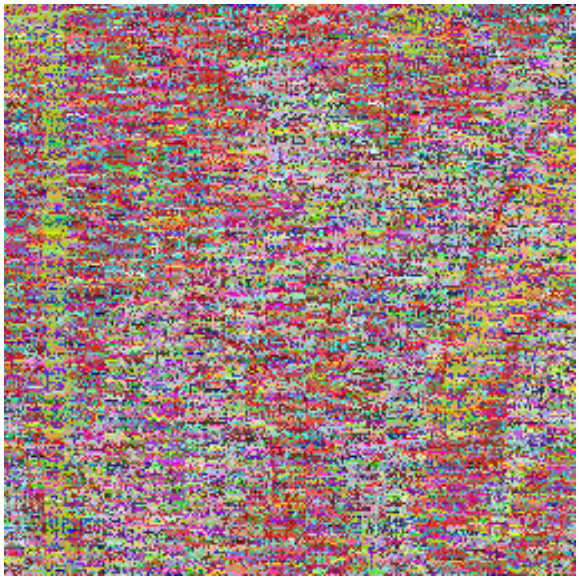

Figure 15 The „best" result of filtering in Photoshop

Statistic comparison of the histograms of images also have been conducted with very good results

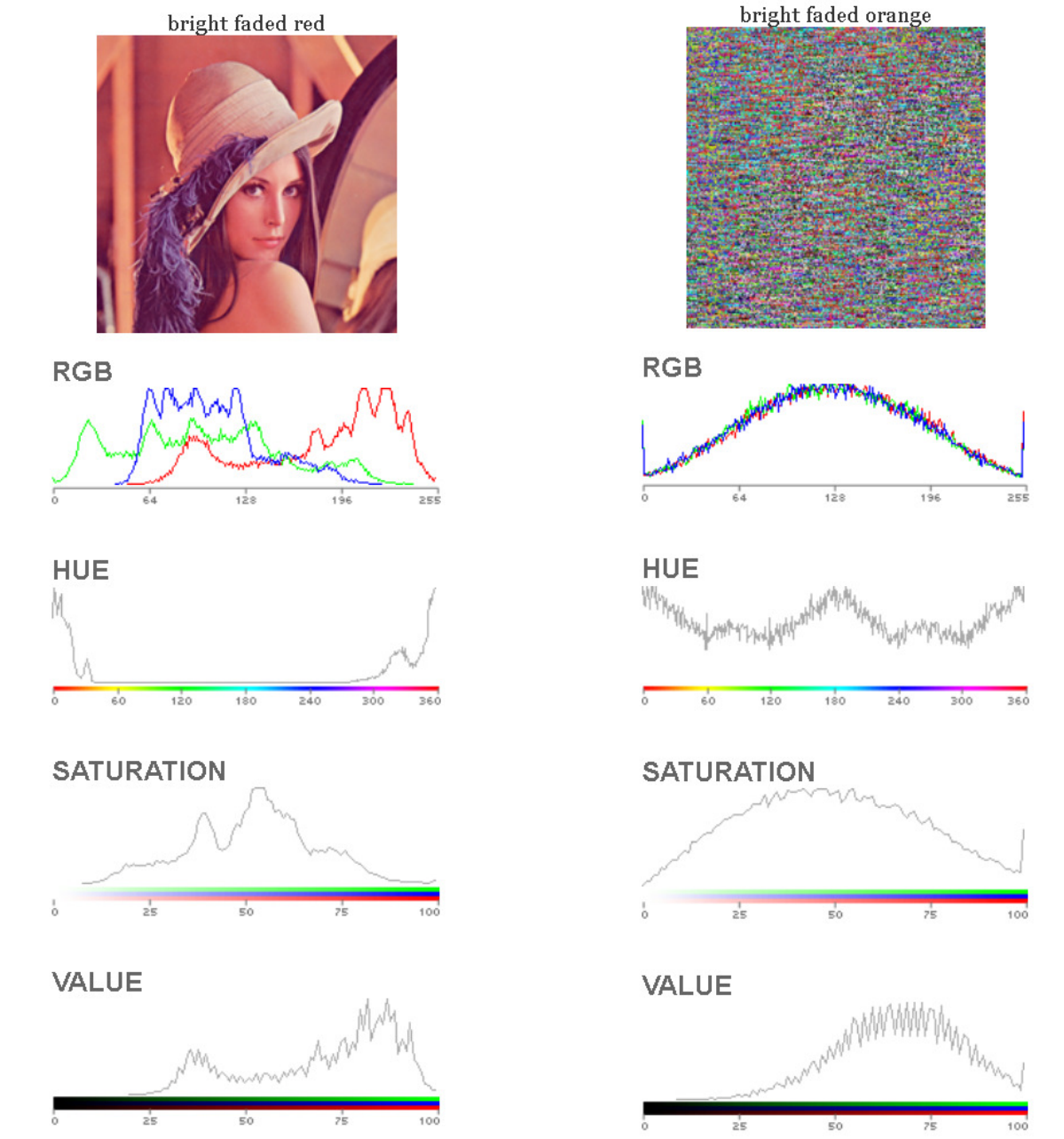

Figure 16 The histograms of original image and encrypted share

The conclusion of these test is that the method is strong enough, the information is severely dissimulated in the shares.

In **Chapter 5.10.2** some computational performances were tested. These test shows that the encryption time is dependent from the length of the original key, length of numeric key, number of iteration used during key-shift.

Finally in **Chapter 5.11** some uses are proposed for the method :

- System and user authentication
- Message authentication

FURTHER RESEARCH

As further research the author propose himself to further study the pixel-sieve and bit-sieve methods. The method may be further improved for instance embedding it with steganography. The proposed key expansion method offers some possibilities for a certain key management protocols.

BIBLIOGRAPHY of THESIS

[AAtan] Adrian Atanasiu, *Curs de Criptografie* http://www.galaxyng.com/adrian_atanasiu/cript.htm

[Baden915] Sir Robert Baden-Powell *My Adventures as a Spy* 1915

[Bor96] Boran Sean, IT Security Cookbook, Draft V0.84 1996

[BreNa89] David F. C. Brewer, Michael J. Nash *The Chinese wall security policye* IEEE Symposium on reasarch in security and privacy , 1-3 may 1989, OAKLAND, CALIFORNIA. (pp 206-14)

[Burt04] Emil Burtescu, *"Securitatea Datelor în Sistemele Informatice Economice"*, 2004

[CheBel94] Bill Cheswick , Steve M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994

[Chen01] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, *A new encription algorithm for image cryptosystems,* The Journal of Systems and Software 58 (2001), 83-91

[Chen06] Chao-Shen Chen, Rong-Jian Chen, *Image Encryption and Decryption Using SCAN Methodology*, Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), 2006

[Chou10] Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh *Modified Pixel Sieve Method for Visual Cryptography* Indian Journal of Computer Science and Engineering Vol. 1 No. 4 321-326 2010

[Chou11] Vaibhav Choudhary, Pravin Kumar, Kishore Kumar and D S Singh. *An Improved Pixel Sieve Method for Visual Cryptography*. International Journal of Computer Applications 12(9):7–10, January 2011. ISSN 0975-888

[CHUKS] Chuck Semeria, *Internet Firewalls and Security A Technology Overview,* http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html

[ClWil87] Clark, David D.; Wilson, David R.; *A Comparison of Commercial and Military Computer Security Policies*; in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), May 1987, Oakland, CA; IEEE Press, pp. 184–193

[DECo00] D. E. Comer. *Internetworking with TCP/IP: Principles,Protocols, and Architecture*,

volume I. Prentice-Hall, Englewood Cliffs, NJ, fourth edition, 2000

[DzMo06] Ioan Dziţac, Grigor Moldovan, *Sisteme distribuite. Modele informatice,* Editura Universităţii Agora, 2006 isbn 10 973-87960-9-1

[FYS07] Frank Y. Shih *Digital Watermarking and Steganography: Fundamentals and Techniques* , CRC Press, 2007, ISBN: 9781420047578

[Gra72] Graham, G.S. , P. J. Denning, *Protection : Principles and Practice*, Proc. Of AFIPS Spring joint compute conference, vol. 40, 1972

[GRB79] G. R. Blakley, *Safeguarding cryptographic keys*, proceedings of the National Computer Conference, 48, pp 313–317, 1979.

[GRN] Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, on http://www.securityfocus.com/infocus/1527/ (accesat in marte 2007)

[Guha96] Biswaroop Guha, Biswanath Mukherjee, *Network Security via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposed Solutions*. Proc. of the IEEE Infocom'96 , San Francisco, CA, March 1996, pp. 603-610

[Incze04] dep. Informatică, contributor **Incze Arpad**, *Document intern: Raport de audit de securitate 2004*

[Incze05] **Incze Arpad**, Ioan Ileana, Manuela Kadar, *Increasing the security of an ACCESS database,* proceedings of „Several aspects on biology, chemistry, computer science, mathematics and physics", Oradea 2005 ISBN 973-759-142-9

[Incze10a] **Incze Arpad**, *Secret sharing & visual cryptography through bit sieve for fast image encryption,* proceedings AQTR 2010 THETA 17th International IEEE confernce on Automation,Quality and Testing, Robotics, ISSN 978-973-662-562-6

[Incze10b] **Incze Arpad**, *Pixel Sieve method for secret sharing & visual cryptography,* Proceedings of the 9th RoEduNet IEEE International conference, Sibiu, 24-25 june, 2010 in ***ISI Conference Proceedings Citation Index***

[Incze10c] **Incze Arpad**, Moldovan Grigor, Maria Muntean, *From pixel sieve to bit sieve. Bit level based secret sharing cryptographic method,* in proceedings 11th International symposium CINTI, Budapest 18-20 nov. 2010 978-1-4244-9278-7 indexat **IEEE**

[Incze11] **Incze Arpad**, *Social Enineering and education in fight against cybercrime*, Acta Universitas Apulensis- Special Issue, Proceeding of ICTAMI 2011, ISSN 1582-5329 p541-553 **B+ CNCSIS**

[Incze12] **Incze Arpad,** *A greater involvement of education in fight against cybercrime* 2nd WORLD CONFERENCE ON EDUCATIONAL TECHNOLOGY RESEARCHES NEAR EAST UNIVERSITY 27-30 June 2012 NICOSIA – NORTH CYPRUS Procedia-Social and Behavioral vol 83 Journal ISSN: 1877-0428 by ELSEVIER ***ISI Conference Proceedings Citation Index***

[Incze14a] **Incze Arpad**, "*Cryptographic key issues and solutions for the bit sieve/pixel-sieve method*", *AQTR*, 2014, 2014 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR) 2014, pp. 1-5, doi:10.1109/AQTR.2014.6857853 ***ISI Web of Science***

[Incze14b] **Incze Arpad**, *Solutions regarding some cryptographic key issues for the pixel-sieve cryptographic method* , 4th WORLD CONFERENCE on INNOVATION and COMPUTER SCIENCES (INSODE-2014) Sapienza University, Faculty of Economics April 11-13, 2014 Rome, Italy www.insode.org in curs de publicare in

AWERProcedia Information Technology and Computer Science // Global Journal on Technology ISSN: 2147-5369

[IPSEC95] IPSEC Working Group, Ashar Aziz, Tom Markson, Hemma Prafullchandra *Simple Key-Management For Internet Protocols* Sun Microsystems, Inc. December 21, 1995, http://tools.ietf.org/html/draft-ietf-ipsec-skip-06

[Jiun99] Jiun-In Guo, Jui-Cheng Yen, *A new mirror-like image encryption algorithm and its VLSI architecture*, Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China 1999

[Kot12] Koteswari, S.; Paul, P. John; Indrani, S., *VC of IRIS Images for ATM Banking,* International Journal of Computer Applications, Volume 48 No. 18 June 2012 ISSN 0975-8887

[LJo95] L. Joncheray. *A simple active attack against TCP*. Proceedingsof the Fifth Usenix Unix Security Symposium, Salt Lake City, UT, 1995.

[MaBo01] S.S.Maniccam, N.G. Bourbakis, *Lossless image compression and encryption using SCAN*, Pattern Recognition 34 (2001), 1229-1245

[Men96] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone *Handbook of Applied Cryptography* CRC Press ISBN: 0-8493-8523-7 October 1996 on http://www.cacr.math.uwaterloo.ca/hac/

[Mill88] S. P. Miller , B. C. Neuman , J. I. Schiller , J. H. Saltzer, *Kerberos Authentication and Authorization System,* In Project Athena Technical Plan ,1988

[Mit02] Kevin Mitnick, William L. Simon, *The Art of Deception*, Wiley Publishing inc 2002, Hardback ISBN 0-471-23712-4

[MOL06] Grigor Moldovan, Ioan Dziţac, *Sisteme distribuite. Modele matematice,* Editura Universităţii Agora, 2006 isbn 10 973-88205-0-2

[Morr85] Robert T. Morris, *A Weakness in the 4.2BSD Unix TCP/IP Software*, Computing Science Technical Report 117, AT&T Bell Laboratories, Murray Hill, NJ, February 1985.

[MOV--] A. Menezes, P. Oorschot, S. Vanstome, *Handbook of Applied Cryptography* (https://notendur.hi.is/pgg/Handbook%20of%20Applied%20Cryptography.pdf)

[MRan04] Marcus J. Ranum , *Tales From The Early Days of the Firewall* , CyberGuard User Conference, 2004, West Palm Beach http://www.ranum.com/security/computer _security/archives/

[MunInc10] Maria Muntean, Honoriu Valean, Liviu Miclea, **Incze Arpad** *A novel intrusion detection method based on support vector machines*, proceedings of 11th International symposium CINTI, Budapest 18-20 nov, 2010. 978-1-4244-9278-7 indexat **SCOPUS**

[NamSnet02] SamsNet*, Securitatea în internet*, Editura Teora, Bucureşti, 2002

[Naor94] Moni Naor and Adi Shamir, Visual Cryptography, EUROCRYPT 1994, pp1–12

[Nort02] Peter Norton , Dave Kearns, *Reţele de calculatoare,* Editura Teora, 2002

[Perl88] R. Perlman. *Network Layer Protocols with Byzantine Robustness*. PhD thesis, M.I.T., 1988

[PRM14] Praveen Gujjar J., Raghvendra M. Dev *Concealment of Images using S^3 approach* ISRASE First International Conference on Recent Advances in Science &

Engineering 2014 (ISRA SE-2014) ISRASE eXplore digital library

[SBel04] Steven M. Bellovin, *A Look Back at "Security Problems in the TCP/IP Protocol Suite"* 20th Annual Computer Security Applications Conference (ACSAC), December 2004, in as part of the "classic papers" track.

[SBel89] Steve Bellovin, *Security Problems in the TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, no. 2 (April 1989) pg 32-48

[SBel95] Steven M. Bellovin, *Using the Domain Name System for System Break-Ins,* Proceedings of the Fifth Usenix Unix Security Symposium 1995

[SCH04] Schneier, Bruce - *Secrets & Lies,* Wiley Publishing, Inc., 2004

[Schu94] Christoph L. Schuba. and Eugene H. Spafford *Countering Abuse of Name-Based Authentication,* Computer Sciences Department Purdue University West Lafayette, IN 47907 CSD-TR-94-029 April, 1994

[Sham79] Shamir, Adi , *How to share a secret*, Communications of the *ACM* 22 1979 : 612–613

[Shob13] Shobha Patil, V.R.Udupi *A Secure Approach to Image Encryption of color image without using key* International Journal of Current Engineering and Technology ISSN 2277 – 4106 ©2013 INPRESSCO. Available at http://inpressco.com/category/ijcet

[Sidd12] Siddharth Malik, Anjali Sardana *A Keyless Approach to Image Encryption,* 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 $26.00 © 2012 IEEE DOI 10.1109/CSNT.2012.189

[Sin03] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[Stein88] Jennifer G. Steiner , Clifford Neuman , Jeffrey I. Schiller, Kerberos: *An Authentication Service for Open Network Systems,* Usenix Conference Proceedings 1988

[Tan98] Andrew S. Tanenbaum, *Rețele de calculatoare*, Computer Press Agora 1998

[TWO01] Terry William Ogletree – FIREWALLS. Protecția rețelelor conectate la internet, Ed TEORA 2001

[VBOC06] ing. Valer Bocan, *CONTRIBUȚII LA CREŞTEREA DISPONIBILITĂȚII, SCALABILITĂȚII SI SECURITĂȚII SISTEMELOR DE COMUNICAȚIE*, Teza de doctorat, Universitatea "Politehnica" din Timisoara 2006

[Venk13] Venkatesh M.R. , Roopanjali. Daddi, *SDS Technique For Secret Image Encryption,* International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013 ISSN: 2278-0181

[VERIZONE] http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

[VVP00] Victor-Valeriu Patriciu, Neculai-Daniel Stoleru *APLICAȚII LA CRIPTOGRAFIA VIZUALĂ*, Volumul Conferintei de Informatica Teoretica si Tehnologii Informatice, Univ. Ovidius, Constanta, mai. 2000

[VVP95] Victor-Valeriu Patriciu – *Criptografia si securitatea retelelor de calculatoare cu aplicatii in C si Pascal* Editura: Tehnica , 1996

[WhNew05] Whitaker A., Newman D, *Penetration testing and Network Defence* , Publisher: Cisco Press November 04, 2005 , ISBN: 1-58705-208-3

[YuvJn08] Yuval Ben-Itzhak, "*The Cybercrime 2.0 Evolution*", The ISSA Journal, June 2008

[YuvOc08] Yuval Ben-Itzhak, "*Organized Cybercrime*", The ISSA Journal, October 2008

Other bibliography and online resources used for synthesis.

Jim Doherty, "*A Brief History of Data Theft*", The ISSA Journal, June 2008

Bruce Schneier, *Schneier on security,* Wiley Publishing inc., 2008, ISBN 978-0470-39535-6

Bruce Schneier, *Secrets & Lies Digital Security in a Networked World*, John Wiley & Sons, 2000 ISBN 0-471-25311-1

Schell, B.H. and Martin, C. *Contemporary World Issues Series: Cybercrime: A Reference Handbook*. Santa Barbara, CA: ABC-CLIO, 2004

T. ElGamal (1985). "*A public key cryptosystem and a signature scheme based on discrete logarithms*". IEEE Trans inf Theo 31 (4): 469–472.

Ralph Merkle and Martin Hellman, Hiding Information and Signatures in Trapdoor Knapsacks, IEEE Trans. Information Theory, 24(5), September 1978

Farmer, Dan and Venema, Wietsa *Improving the Security of your site by breaking into it* Sun Microsystems (11/29/2000) URL:http://www.geocities.com/hackernet_99/breakintoyoursite.htm

Gibbs, Mark *Any Port is a Hacker Storm* (11/29/2000) URL: http://www.antionline.com/

Fordham, Doug *Intelligence Preparation of the Battlefield* (6/19/2000)

URL: http://www.securityfocus.com/focus/ih/articles/battlefield.html (12/3/2000)

Kubin, Larry *Protect Your Business From Hacker Attack*s

Reto E. Haeni, *Firewall Penetration Testing*, , 1997 r.haeni@cpi.seas.gwu.edu

Diffie W, , Hellman M., *Multiuser criptography* , National Computer Conference, New York 1976

R. Rivest, A. Shamir, L. Adleman. "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*". Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977. Initial publication of the RSA scheme. (http://theory.lcs.mit.edu/~rivest/rsapaper.pdf)

URL: http://www.suite101.com/article.cfm/1345/11549 (11/29/2000)

http://www.winpcap.org/

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.1117&rep=rep1&type=pdf

http://www.brainbell.com/tutorials/Networking/Proxy_Servers.html

http://hermes.etc.utt.ro/teaching/tart/FINAL.pdf

http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html

www.buzzsurf.com/surfatwork/

http://www.webopedia.com/TERM/S/SOCKS.html

www.buzzsurf.com/surfatwork/

http://www.bitvise.com/winsshd

http://www.chiark.greenend.org.uk/~sgtatham/putty/

http://www.no-ip.com/services/managed_dns/free_dynamic_dns.html

http://www.ssh.com/.

http://www.teamviewer.com/en/index.aspx

http://sourceforge.net/projects/packetyzer/

http://www.securityfocus.com/infocus/1527

http://www.dcd.uaic.ro/default.php?t=site&pgid=82
http://www.hackerwhacker.com/