[5] J. Moran, R. Desimone. Selective attention gates visual processing in the Extrastriate Cortex. Science, vol. 229, pp. 784-787, 1985.

[6] G. Sperling, E. Weichselgartner. Episodic theory of the dynamics of spatial attention. Psychological review, vol. 102, no. 3, pp. 503-532, 1995.

[7] A. Treisman. Features and targets: The fourteenth Barlett memorial lecture. Quarterly Journal of Experimental Psychology, 40A, pp. 201-237, 1988.

[8] A. Treisman. Feature binding, attention and target perception. Philosophical Transactions of the Royal Society of London, vol. 353, pp. 1295-1306, 1998.

[9] A. Treisman, G. Gelade. A feature-integration theory of attention. Cognitive Psychology, vol. 12, pp. 97-136, 1980.

[10] A. Treisman, D. Kahneman, J. Burkell. Perceptual targets and the cost of filtering. Perception & Psychophysics, vol. 33, pp. 527-532, 1983.

[11] S. Yantis. Targets, attention, and perceptual experience in “Visual Attention". R. D. Wright (Eds.), pp. 187-214. Oxford, NY: Oxford University Press, 1998.

[12] M. I. Posner. Orienting of attention. Quarterly Journal of Experimental Psychology, vol. 32,pp. 3-25, 1980.

[13] C. Koch, B. Mathur. Neuromorphic vision chips. IEEE Spectrum, vol. 33, pp. 38–46, May 1996

[14] C. Koch, S. Ullman. Shifts in Selective Visual Attention: Towards the Underlying Neural Circuitry. Human Neurobiology, vol. 4, pp. 219–227, 1985.

[15] E. Artyomov, O. Yadid-Pecht. Adaptive Multiple Resolution CMOS Active Pixel Sensor. ISCAS 2004, Vancouver, Canada, May 2004, Vol. IV, pp. 836-839.

Authors' Information

Alexander Fish – The VLSI Systems Center, Ben-Gurion University, Beer Sheva, Israel; e-mail: afish@ee.bgu.ac.il

Orly Yadid-Pecht – Dept of Electrical and Computer Engineering, University of Calgary, Alberta, Canada; e-mail: oyp@ee.bgu.ac.il

EXAMINATION OF PASSWORDS’ INFLUATION ON THE COMPRESSING PROCESS OF NON-ENCRYPTED OBJECTS

Dimitrina Polimirova-Nickolova, Eugene Nickolov

Abstract: The principal methods of compression and different types of non-encrypted objects are described. An analysis is made of the results obtained from examinations of the speed of compression for objects when using passwords with different length. The size of the new file obtained after compression is also analyzed. Some evaluations are made with regard to the methods and the objects used in the examinations. In conclusion some deductions are drawn as well as recommendations for future work.

Keywords: Password, Methods of Compression, Non-Encrypted Applications, Archive Programs, Level of Compression, File Extensions, Information Security.

ACM Classification Keywords: D.4.6 Security and Protection: information flow controls

The Situation

The information technologies’ progress leads to increasing need of creation and use of compressed objects. With regards to this, examination and analysis are made of different methods of compression and their varieties, which purpose is the creation of high-speed, effective compression of information flows working in real time.

The compression represents a method for reducing the size of some object. In the case of digital data, the compression is connected to the reduction of the bytes'number by removing the unneeded and/or non-critical information which results in decrease of object's size. The methods of compression are used when the user wishes to economize space when storing the object, to gain time, when it is emailed or to reduce the risk for loss or modification of the information.

When using the different methods of compression a password could be put which allows the achievement of highest information security of the object. The password represents confidential authentication information, formed by symbol strings.

In this article are examined and analyzed non-encrypted applications, on which different methods of compression and passwords with different size are applied. We shall use the term "non-encrypted application" for all applications which are executed under the control of the operation system, process some input data and produce relevant output results while the information flows are in normal (non-encrypted) form all the time. In this examination the non-encrypted applications are represented by 18 types of extensions belonging to 6 basic types archiving programs. They are chosen among the 300 archiving programs known at the moment. They are:

1) E-mail archiving programs – this type of archiving programs use the relative homogeneity of information flow (e-mail traffic) to select the most appropriate methods for compression.

2) Converting archiving programs – these archiving programs are able to convert objects compressed by some method in objects compressed by another method.

3) Multiple archiving programs – these programs execute some successive archiving processing on the different parts of some object using methods of compression with different properties.

4) Image archiving programs – these programs help solving a very important problem of the present day connected to the real-time processing of video and image web-objects – the obligatory immediate compression of the object after its creation. The transmission and the processing of the object are executed entirely in compressed state, till the end moment of its reproduction by the appropriate media.

5) Data archiving programs – these programs are specialized in the processing and the use of compressed objects, got from information flows owning the characteristics of "data" (in this case we are concerned by the circumstance that the data in the different phases of their existence pass in compressed mode, are kept for some time in this "minimized" form, after which thy are decompressed.).

6) Executable archiving programs – the goal in these programs is to achieve some specificity of the compression, connected to the possibilities for running the compressed objects.

The Problem

The object of examination are the methods of compression (different types of compressing programs) and their varieties (different levels of compression, size of the used password etc.); the stress will be laid on the password length and its effect on the compression process [2, 3]. The methods will be analysed after their application on non-encrypted objects from the 6 types of archiving programs specified above. By contrast with the compressin, the archiving is a process of storing a data structure for a later use. In most cases this data structure (which is usually a single object) is stored in a file, but besides this it could be written in memory or transmitted to another application.

Some kinds of examinations are made, concerning the effect of the password size on certain characteristics of the compression of non-encrypted applications.

The first examination analyses the SPEED of the compression process. The following tasks are put in connection to this examination:

1) Determination of the *objects* which will be analyzed and the *methods of compression*, applied on them. The objects are the selected 18 types, mentioned above and described in Table (1a – 1f), by which a formal presentation of non-encrypted applications is obtained. The initial size of each type is 1 024 000 bytes.

Table 1a
E-mail archiving programs

Extension	Program / Information
DBX	Outlook Express Email Folder
IDX	Outlook Express Mailbox Index
PCE	Eudora Mailbox Name Map

Table 1b
Converting archiving programs

Extension	Program / Information
ACE	WinAce Compressed File
RAR	WinRAR Compressed Archive
ZIP	Compressed Archive File

Table 1c
Multiple

Extension	Program / Information
ARJ	ARJ Compressed Archive
JAR	JAR Archive
TAR	Tape Archive File

Table 1d
Image archiving programs

Extension	Program / Information
AIS	ACDSee Image Sequence File
B&W	Image Lab
BIL	AreView Image File (ESRI)

Table 1e
Data archiving programs

Extension	Program / Information
DOC	Word Document (Microsoft)
PDF	Acrobat Portable Document Format
TXT	Text File

Table 1f
Executable archiving programs

Extension	Program / Information
EXE	Executable File (Microsoft)
PE	Portable Executable File
PL	Linux Shell Executable Binary

2) Evaluation of the *time*, needed for compression without password by the means of 5 compressing programs, selected among the dozens, known up to now– ACE, GZip, JAR, RAR, ZIP. With the purpose of simplifiing the exposition we shall desribe only the examinations for level of compression Normal (Figure 1).

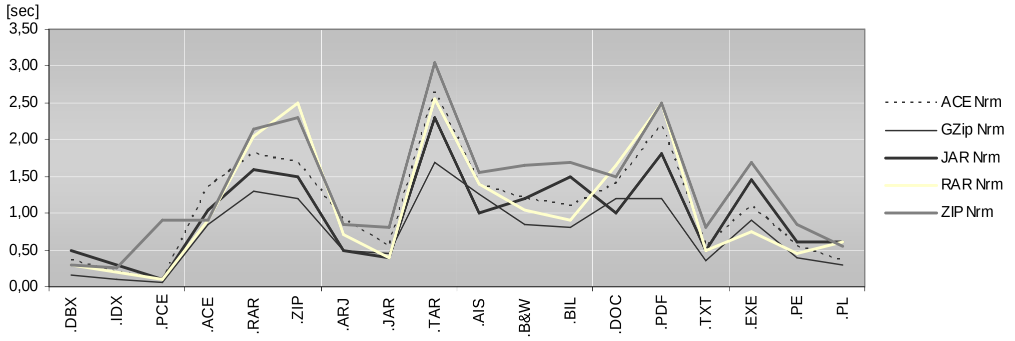

Figure 1

3) Compression of the initial objects with *8, 16 and 32-digit password* and measurement (by software means) of the time, needed for their processing. Fixed passwords are used with length of 8, 16 and 32 symbols, which for simplicity are formed only by the numbers from 0 to 7, ranged consecutively in ascending order, and repeated periodically (Figure 2a – 2c).

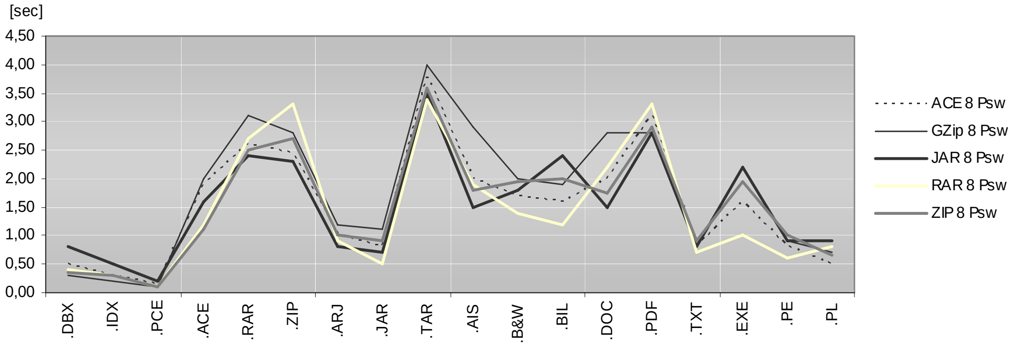

Figure 2a

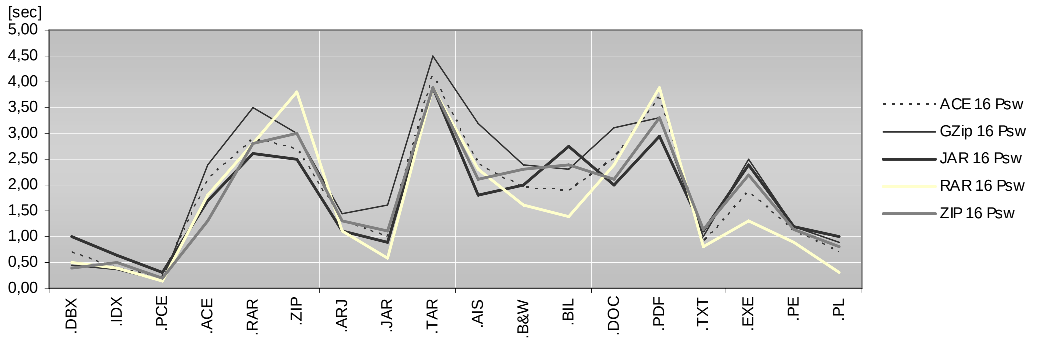

Figure 2b

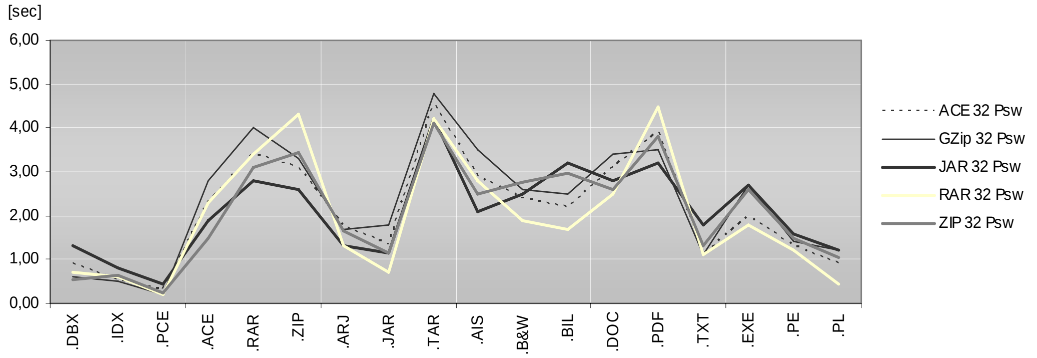

Figure 2c

4) Juxtaposing of the time, needed for the compression of objects when *8, 16 and 32-digit password* is used (Figure 3).

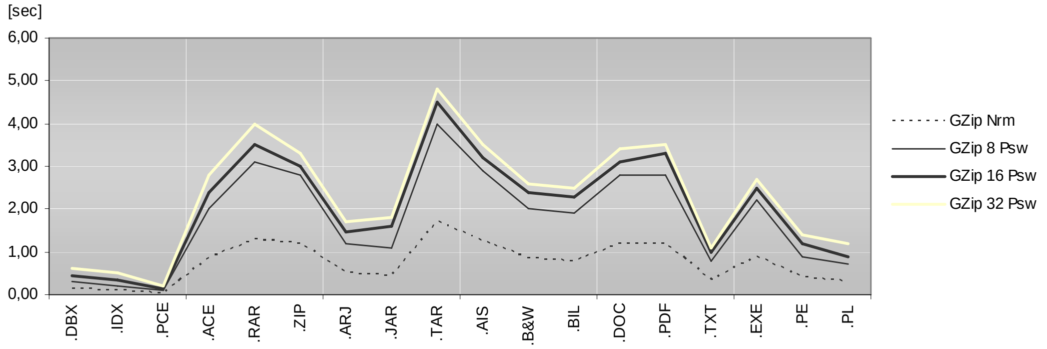

Figure 3

The second examination analyses the SIZE of the resulting file after compression by using passwords with different length. The following tasks are put in connection to this examination:

1) To compress different file formats with different compressing programs with level of compression Normal *without using passwords* (Figure 4a, b, c, d, e, f).

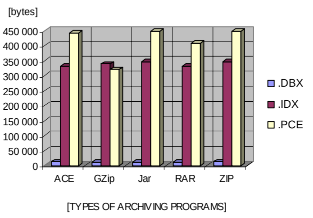

Figure 4a

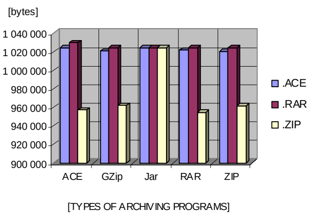

Figure 4b

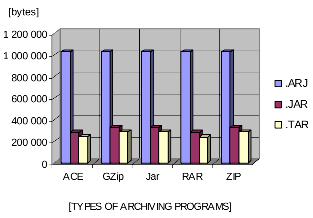

Figure 4c

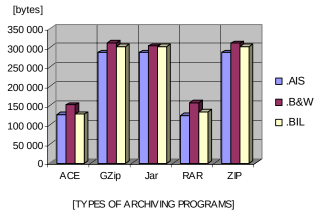

Figure 4d

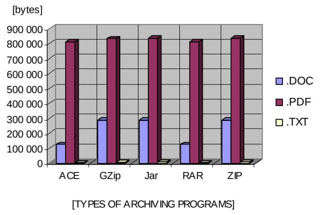

Figure 4e

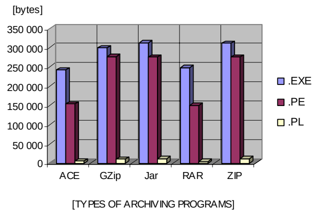

Figure 4f

2) To compress different file formats with different compressing programs using *8, 16 and 32-digit passwords* (Figure 5).

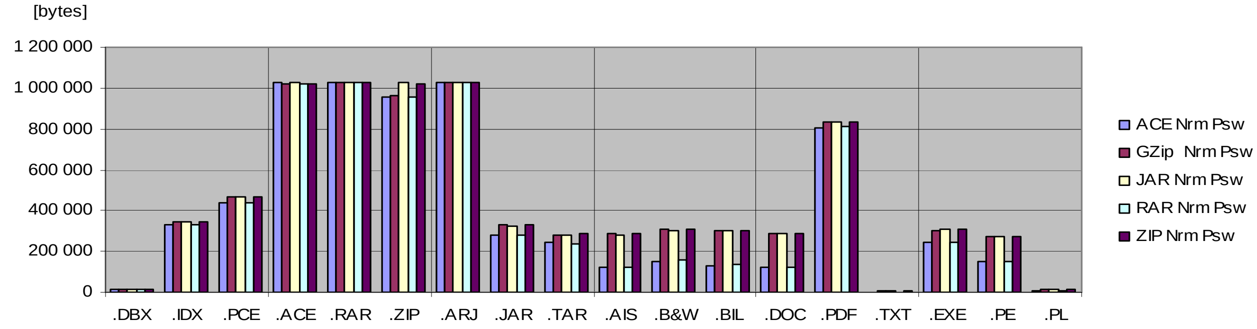

Figure 5

3) To juxtapose the size of the files, compressed *without password* with the size of the files compressed with *8, 16 and 32-digit passwords*.

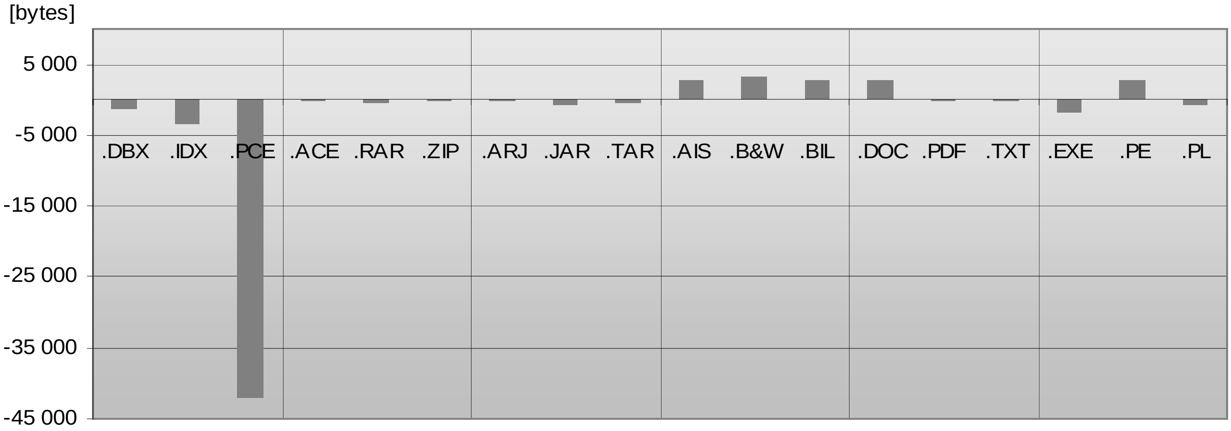

Figure 6

With the purpose of simplifiing the exposition, on Figure 6 are demonstated the results only for one method of compression (GZip) with regards to the different size of files *with* and *without* password.

The following assessments could be made from the experiments, which were carried out:

1) With regard to the SPEED:

a) The evaluation with regard to the selected objects for compression is positive and the assumptions that are made have not influence on the obtained results. The evaluation with regard to the selected methods of compression is also positive and the experiments that are carried out could be generalized for the other methods. The selected size of the objects is sufficient for conducting the necessary evaluations, conclusions and recommendations.

b) The evaluation with regard to the time, needed for compression *without password* shows a maximum for .TAR and minimum for .PCE. The examinations made for a level of compression Normal (Nrm) illustrate enough the main evaluations, conclusions and recommendations.

c) The evaluation with regard to the compression with *8, 16 and 32-digit passwords* shows that the number and the types of the symbols are correctly chosen. The maximum with regard to the speed is for .TAR, the minimum – for .PCE; this evaluation is valid for the three examined password lengths.

d) The evaluation with regard to the time, needed for compression with *8, 16 and 32-digit passwords,* shows a confirmation of the maximum for .TAR and of the minimum for .PCE for the chosen most appropriate method of compression GZip, along with some local extremums which could be seen in the graph on Figure 3. The relative increase of the time for compression with password in comparison with the compression without password is largest in the case of 8-digit password. The relative increase of the time for compression with 16 and 32-digit password is minimal and practically the same for all other extensions.

2) With regard to the SIZE:

a) The evaluation with regard to the compression of different file formats with the selected types of compressing programs for level of compression Normal *without using a password* shows the presence of minimums, maximums and other local extremums, illustrated on Figure 4a – 4f. The absolute maximum is for .TXT compressed with ACE, and the absolute minimum - for .ARJ compressed with JAR.

b) The evaluation with regard to the compression of different file formats with the selected types of compressing programs for level of compression Normal *with a password* shows the presence of minimums, maximums and other local extremums, illustrated on Figure 5. The use of 8, 16 and 32-digit passwords practically does not influence the size of the resulting objects.

c) The evaluation with regard to the juxtaposition of the sizes of files compressed *without password* and *with password* for a selected method of compression (GZip) shows the largest difference for .PCE and the smallest for .ACE.

Conclusions and Future Work

The examinations that are made and the extensive experiments that are carried out, show the significant perspectives in the scientific research on these problems. The influence of the methods of compression on the different applications together with the use of password with different length is considerable and could be used for decision-making connected to the information security and the risk evaluation in processing of information flows [1].

Bibliography

[1] Bahram Javidi, Optical and Digital Techniques for Information Security (Advanced Sciences and Technologies for Security Applications), Springer, June, 2005.

[2] David Salomon, Data Compression: The Complete Reference, Springer Verlag New York, Inc., 2004.

[3] Rob Shimonski, Introduction to Password Cracking, IBM Developer Works Hacking Techniques article, July 2002.

Authors' Information

Dimitrina Polimirova-Nickolova - PhD Student, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: polimira@nlcv.bas.bg.

Eugene Nickolov - Prof.DSc, PhD, Eng, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: eugene@nlcv.bas.bg.