ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КЕРУВАННЯ

UDC 004.4.277:004.056
DOI: 10.20535/1810-0546.2016.1.60749

I.A. Dychka[1], S.S. Shyrochyn[2], Ye.S. Sulema[1]
[1]National Technical University of Ukraine "KPI", Kyiv, Ukraine
[2]Trinetix LLC

ANALYSIS OF PARALLEL COMPUTATIONS EFFICIENCY FOR USER'S PRIVATE MULTIMEDIA DATA PROTECTION IN CLOUDS

Background. A significant part of data stored in cloud storages is multimedia data. The procedure of data protection can be organized as a trusted cloud service. Since this service is an intermediate layer between user layer and cloud storage the time of data processing in it is a critical matter. To achieve decreasing of time required for data protection procedure, parallel computations can be employed.
Objective. The objective of the research is to evaluate and analyze the time efficiency of parallel computations fulfilling in multimedia data protection procedures.
Methods. The comparative analysis results for three methods, namely: data fragmentation method, complementary image method, and LSB-based method with AES encryption, are presented in the paper. The methods are considered in terms of data processing time efficiency. The impact of both stegobits used for data embedding and data parallel processing threads is analyzed. The comparison is carried out for two types of multimedia data – audio data and graphical data.
Results. The time efficiency characteristics obtained and analyzed in the research show that the use of parallel computations in the Complementary Image method enables the decreasing of data processing time up to 70%.
Conclusions. The presented results enable comparing the considered methods in terms of their realization as software tool that is, along with data protection level, important characteristic for cloud services user. The Complementary Image method with parallel data processing can be effectively used for multimedia data protection.
Keywords: multimedia data protection; steganography.

Introduction

Cloud storages become more and more popular due to convenience and freedom in storing data they offer to users. However when a user stores own data in an external storage he or she loses full control over it and a problem of unauthorized access to user's private data appears. Thus, the task of user's private data protection is topical, especially for cloud storages.

A significant part of data stored in cloud storages is multimedia data such as audio, video and graphical files. Their protection can be fulfilled by using specific method based on features of multimedia data such as redundancy and large volume. Such methods are usually based on the principles of steganography [1–9].

The procedure of data protection itself can be organized as a trusted cloud service providing access to user's personal data for a number of cloud storages to be chosen by the user according to his or her preferences.

Since the proposed trusted service is an intermediate layer between a user and cloud storage the time of data processing in it is a critical matter. To achieve significant decreasing of time required for data protection procedure, parallel computations can be employed. Therefore the research of parallel computations efficiency for different methods of multimedia data protection takes on special significance.

Research Objective

The objective of the research presented in this paper is to evaluate and analyze the time efficiency of parallel computations fulfilling in multimedia data protection procedures for different protection methods [3–5] proposed earlier by the authors. The achievement of this objective can be important for further development of trusted protection services.

Taking into consideration all important characteristics of steganographic protection methods, including:

- robustness against attacks,
- payload capacity,
- time efficiency,

the authors present the research results on the time efficiency only in this paper. Thus, the paper continues the research of steganographic protection methods time efficiency presented in [6] and it complements related researches [7, 8].

Multimedia Data Protection Methods

Let us consider three LSB-based (*LSB* is *Least Significant Bits* [9]) steganographic protection methods:

- Data fragmentation method [3, 5];
- Complementary image method [4];
- LSB-based method with AES encryption.

Input data of every method is *secret data* (data to be protected) and a *cover-object* (it is also called a *container* or a *vessel*). Secret data and cover-object usually have the same multimedia nature – they are both either graphical data or audio data.

Output data of every method is a *stego-object* and a *key*.

The basic principle of LSB-based steganographic protection [1, 2, 9] is that the *secret data* are embedded into the *cover-object* by modifying the least significant bits (usually up to 4 bits) of every byte of the cover-object data with bits sequence of the secret data. Due to redundancy of multimedia data the change of the cover-object is insignificant and usually cannot be recognized visually if both the cover-object and the number of used LSBs have been chosen properly. The modified cover-object is called *stego-object*. The specific parameters of secret data processing related to a certain protection method form the *key*. The procedure of the secret data extraction is opposite to the procedure of the data embedding.

Data Fragmentation Method. The data fragmentation method [3, 5] uses a separable secret key that consists of 2 sub-keys: the *Key of Lengths* (KL) and the *Key of Addresses* (KA). The secret multimedia data (either graphical image or audio signal) is transformed into one data sequence. This sequence is divided into fragments of a random length defined by the KL. Every fragment is embedded into the cover-object (either graphical image or audio signal) by modifying its LSBs. The place of the embedding is specified by a random address according to the KA. As the result the stego-object (the cover-object with embedded secret data) is obtained.

The time T_w necessary for secret data embedding can be estimated as it follows:

$$T_w = T_{rc} + T_{rd} + T_g + T_m + T_{ws} + T_{wk},$$

where T_{rc} is time necessary for the cover-object reading from a file; T_{rd} is time necessary for the secret data reading; T_g is time necessary for the keys generation; T_m is time necessary for the cover-object modification; T_{ws} is time necessary for the stego-object writing to a file; T_{wk} is time necessary for the keys writing.

The secret data retrieval procedure is opposite to the secret data embedding procedure. The time T_r necessary for the secret data retrieval can be estimated as it follows:

$$T_r = T_{rs} + T_{rk} + T_e + T_{wd},$$

where T_{rs} is time necessary for the stego-object reading from a file; T_{rk} is time necessary for the keys reading; T_e is time necessary for the secret data extraction from the cover-object; T_{wd} is time necessary for the secret data writing.

Complementary Image Method. The complementary image method [4] is based on the *complementary transformation* of the secret data. The complementary transformation consists in the replacement of every byte of the secret data by a byte kept in the cell of the key table. This cell has coordinates equal to the current byte of the secret data (used as the row number) and the current byte of the cover-object (used as the column number). The obtained transformed secret data (called the *complementary image*) is embedded into the cover-object instead of the secret data.

The time T_w necessary for secret data embedding can be estimated as it follows:

$$T_w = T_{rc} + T_{rd} + T_g + T_t + T_m + T_{ws} + T_{wk},$$

where T_{rc} is time necessary for the cover-object reading from a file; T_{rd} is time necessary for the secret data reading; T_g is time necessary for the key table generation; T_t is time necessary for the complementary transformation of the secret data; T_m is time necessary for the cover-object modification; T_{ws} is time necessary for the stego-object writing to a file; T_{wk} is time necessary for the key table writing.

The secret data retrieval procedure is opposite to the secret data embedding procedure. The time T_r necessary for the secret data retrieval can be estimated as it follows:

$$T_r = T_{rs} + T_{rk} + T_e + T_o + T_{wd},$$

where T_{rs} is time necessary for the stego-object reading from a file; T_{rk} is time necessary for the key table reading; T_e is time necessary for the complementary image data extraction from the cover-object; T_o is time necessary for the opposite transformation of the complementary image to the secret

data; T_{wd} is time necessary for the secret data writing.

LSB-Based Method with AES Encryption. The LSB-based method with AES encryption is used as en etalon necessary for comparison of the methods proposed by authors [3–5]. This method consists in the encryption of the secret data according to the AES algorithm Rijndael [10] and the embedding of the encrypted data in to the cover-object.

The time T_w necessary for secret data embedding can be estimated as it follows:

$$T_w = T_{rc} + T_{rd} + T_c + T_m + T_{ws} + T_{wk},$$

where T_{rc} is time necessary for the cover-object reading from a file; T_{rd} is time necessary for the secret data reading; T_c is time necessary for the transformation of the secret data according to AES algorithm; T_m is time necessary for the cover-object modification; T_{ws} is time necessary for the stego-object writing to a file; T_{wk} is time necessary for the key writing.

The secret data retrieval procedure is opposite to the secret data embedding procedure. The time T_r necessary for the secret data retrieval can be estimated as it follows:

$$T_r = T_{rs} + T_{rk} + T_e + T_d + T_{wd},$$

where T_{rs} is time necessary for the stego-object reading from a file; T_{rk} is time necessary for the key table reading; T_{wd} is time necessary for the secret data writing; T_e is time necessary for the complementary image data extraction from the cover-object; T_d is time necessary for the opposite transformation of the secret data according to AES algorithm.

The time necessary for data transmission is the same for every of the considered methods and therefore it does not taken into account in further analysis of the methods time efficiency.

Methods Time Efficiency

To compare the time efficiency of the considered methods two series of tests were fulfilled:

- tests on audio data processing;
- tests on graphical data processing.

Every series included:

1) Test 1 – data protection with 1 stegobit (it means that 1 bit in every 3 bytes of RGB colour – a byte of red colour plain, a byte of green colour plain, a byte of blue colour plain of RGB colour model [11] – of a current pixel in the cover-object is used for the secret data embedding);

2) Test 2 – data protection with 2 stegobits (2 bits in every 3 bytes of RGB colour of a current pixel in the cover-object is used for the secret data embedding);

3) Test 3 – data protection with 4 stegobits (4 bits in every 3 bytes of RGB colour of a current pixel in the cover-object is used for the secret data embedding);

4) Test 4 – data protection with 8 stegobits (8 bits in every 3 bytes of RGB colour of a current pixel in the cover-object is used for the secret data embedding).

The time efficiency of audio data processing is presented in Fig. 1 and the time efficiency of graphical data processing is presented in Fig. 2.

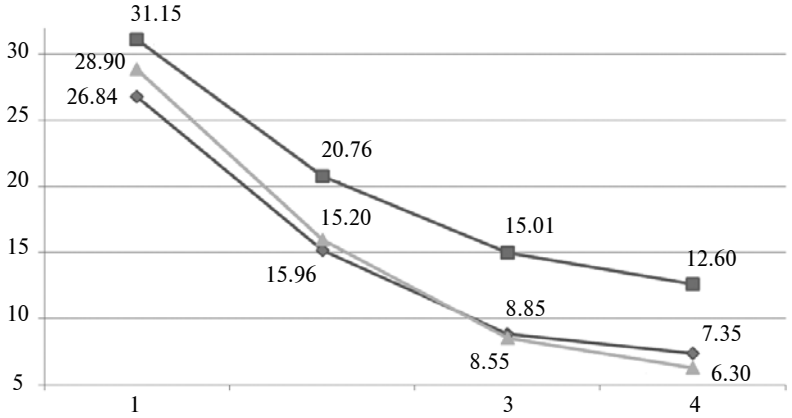

Fig. 1. Comparison of audio data processing time: ■ – AES Encryption method, ▲ – CI method, ◆ – Fragmentation method

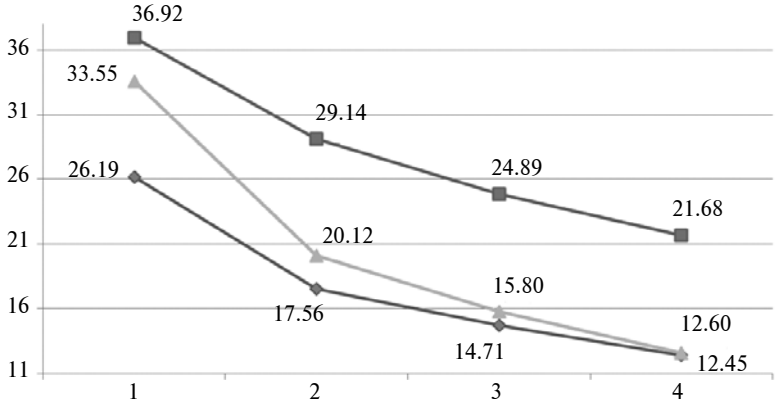

Fig. 2. Comparison of graphical data processing time: ■ – AES Encryption method, ▲ – CI method, ◆ – Fragmentation method

As shown in Fig. 1, the complementary image method (further – CI method) demands less time for data processing than the LSB-based method with AES encryption (further – AES Encryption method) in every test: the highest gain is 50 % and is obtained in test 4; the lowest gain is 7 % and is obtained in test 1.

The data fragmentation method (further – Fragmentation method) demonstrates the time efficiency similar to CI method: the highest gain is 42 % and is obtained in test 4; the lowest gain is 14 % and is obtained in test 1.

As shown in Fig. 2, the results of the second series of the tests are quite similar to the results of the first series. In particular, the CI method demands less time for data processing than the AES Encryption method in every experiment: the highest gain is 42 % and is obtained in test 4; the lowest gain is 9 % and is obtained in test 1. The Fragmentation method demonstrates the following time efficiency in comparison with the AES Encryption method: the highest gain is 42 % and is obtained in test 4; the lowest gain is 29 % and is obtained in test 1.

The comparison of the results obtained on the same tests, but in different series (i.e. on data of different multimedia nature) shows the audio data processing demands less time in every experiment.

In particular for CI method:

- up to 14 % in test 1;
- up to 50 % in test 4.

The time efficiency of graphical data processing is less dependent on stegobit quantity.

The fulfilled tests confirm that the CI method and the Fragmentation method enable faster data processing in comparison with the basic method AES Encryption.

Parallel Data Processing

The analysis of time efficiency of the CI method on different data sets allows assuming that the productivity of its algorithm can be improved by employing parallel computations on multiple cores of CPU for data processing.

To choose the part of CI algorithm to be parallelized the time requirements for different paths of algorithm were analyzed. The main loop of the algorithm [3] was chosen for parallelization. The inner loop that modifies different bits was not parallelized because of high computational cost of transfer between threads. User's PC is expected to have up to 8 CPU cores.

The tests were fulfilled in the same way: two series with 4 types of tests in each series.

As shown in Figure 3 and Figure 4, parallel processing allows decreasing the processing time for both audio data and graphical data. In particular, for audio data processing by CI method with parallel computations on 8 cores the highest gain is 69 % and is obtained in test 1; the lowest gain is 45 % and is obtained in test 4. For graphical data processing by CI method with parallel computations on 8 cores the highest gain is 46 % and is obtained in test 1; the lowest gain is 42 % and is obtained in test 4.

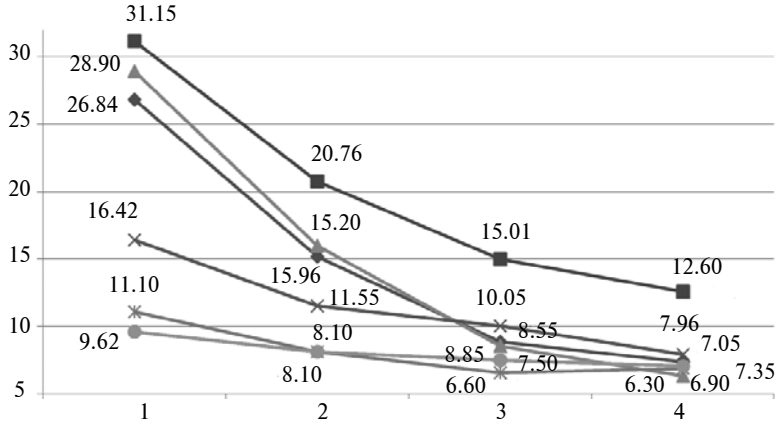

Fig. 3. Comparison of audio data processing time (with different realizations of CI method): ■ – AES Encryption method, ▲ – CI method, ◆ – Fragmentation method, × – CI method (2 cores), ✳ – CI method (4 cores), ● – CI method (8 cores)

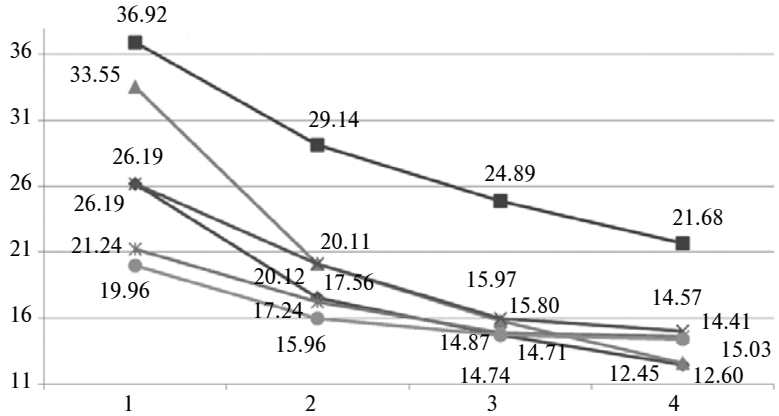

Fig. 4. Comparison of graphical data processing time (with different realizations of CI method): ■ – AES Encryption method, ▲ – CI method, ◆ – Fragmentation method, × – CI method (2 cores), ✳ – CI method (4 cores), ● – CI method (8 cores)

***Table* 1.** Data processing time efficiency

Number of stegbits	Consequent processing time, ms	Best parallel processing time, ms	Time efficiency, %
Audio data			
1	28.90	9.62	77
2	15.96	8.10	49
4	8.55	6.60	23
8	6.30	6.90	–9
Graphical data			
1	33.55	19.96	41
2	20.12	15.96	21
4	15.97	14.74	8
8	12.60	14.41	–14

Table 1 shows the time efficiency obtained by the use of parallel data processing for both audio and graphical data. This efficiency depends on the number of stegobits used for secret data embedding: the highest gain can be obtained for 1 stegobit in both cases (77 % and 41 % respectively). At the same time the using of 8 stegobits don't allow to achieve the time efficiency.

***Table* 2.** Parallel processing time efficiency

Number of cores	CI method for audio data parallel processing	CI method for graphical data parallel processing
Data protection procedure		
2	1.76	1.28
4	2.6	1.57
8	3	1.68
Data retrieval procedure		
2	1.56	1.43
4	1.77	1.89
8	1.06	1.22

Table 2 shows the time of parallel computations on 2, 4, and 8 cores for data processing in CI method when 1 stegobit is used for secret data embedding. In both data protection procedure and data retrieval procedure the increasing of cores quantity enables gain in time efficiency.

However audio data processing can be accelerated more due to increasing the number of cores used for parallel computations.

Conclusions

The use of parallel computations in the Complementary Image method enables the decreasing of data processing time. The best efficiency can be obtained at the maximum number of cores. Parallel computation is more efficient for data protection and retrieval procedures if 1 or 2 stegobits are used. At the same time the less number of stegobits is used the less probability of steganographic protection detection is. Therefore, the achieved results can be considered as positive and of practical value.

The Complementary Image method with parallel data processing can be effectively used for user's personal audio and graphical data protection in cloud services. The future improvement of the method can be focused on video data protection.

Another important issue for further research is to investigate computational complexity of the proposed methods, in particular the Complementary Image method, in order to find additional opportunities for time efficiency increase.

List of literature

1. *Digital* image steganography: survey and analysis of current methods / A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt // Signal Processing. – 2010 – **90**, is. 3. – P. 727–752.
2. *Bhattacharyya S., Banerjee I., Sanyal G.* A Survey of steganography and steganalysis technique in image, text, audio and video as cover carrier // J. Global Res. Comp. Sci. – 2011. – **2**, № 4. – P. 1–16.
3. *Сулема Є.С., Широчин С.С.* Спосіб стеганографії зображень з фрагментацією стегоданих та розділенням закритого ключа // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Вип. 1 (22). – С. 64–68.
4. *Сулема Є.С., Широчин С.С.* Спосіб стеганографії зображень на основі комплементарного образу // Захист інформації. – 2013. – Вип. 4. – С. 345–353.
5. *Сулема Є.С., Широчин С.С.* Спосіб стеганографічного захисту даних в аудіо-файлах на основі комплементарного образу // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка. – 2014. – Вип. 61. – С. 85–92.
6. *Сулема Є.С., Широчин С.С.* Аналіз ефективності паралельної реалізації алгоритмів захисту зображень // Зб. праць Міжнар. науково-практ. конф. "Актуальні проблеми комп'ютерних технологій". – Хмельницький, 2014. – С. 64–68.

7. *Kharrazi M., Sencar H.T., Memon N.* Performance study of common image steganography and steganalysis techniques // J. Electronic Imaging. – 2006. – № 15 (4). – P. 1–16.
8. *Moving* steganography and steganalysis from the laboratory into the real world / A. Ker, P. Bas, R. Böhme et al. // Proc. 1st ACM Workshop IH&MMSec'13. – 2013. – P. 45–58.
9. *Bandyopadhyay S.K., Maitra I.K.* An application of palette based steganography // Int. J. Comp. Applications. – **6**, № 4. – 2010. – P. 24–27.
10. *Daemen J., Rijmen V.* The Design of Rijndael, AES – the Advanced Encryption Standard. – Springer-Verlag, 2002. – 238 p.
11. *Understanding* color models: a review / N.A. Ibraheem, M.M. Hasan, R.Z. Khan, P.K. Mishra // ARPN J. Sci. Technol. – 2012. – **2**, № 3. – P. 265–275.

References

1. A. Cheddad *et al.*, "Digital image steganography: survey and analysis of current methods", *Signal Processing*, vol. 90, is. 3, pp. 727–752, 2010.
2. S. Bhattacharyya *et al.*, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier", *J. Global Res. Comp. Sci.*, vol. 2, no. 4, pp. 1–16, 2011.
3. Y. Sulema and S. Shyrochyn, "Method of image domain steganography with stegodata fragmentation and separation of private key", *Pravove, Normatyvne ta Metrolohichne Zabezpechennya Systemy Zakhystu Informatsiyi v Ukrayini*, no. 1 (22), pp. 64–68, 2012 (in Ukrainian).
4. Y. Sulema and S. Shyrochyn, "Image steganography method based on complementary image", *Zakhyst informatsiyi*, no. 4, pp. 345–353, 2013 (in Ukrainian).
5. S. Shyrochyn and Y. Sulema, "Method of steganographic data protection in audio-files based on complimentary image", *Visnyk NTUU "KPI". Informatyka, Upravlinnya ta Obchyslyuval'na Tekhnika*, no. 61, pp. 85–92, 2014 (in Ukrainian).
6. Y. Sulema and S. Shyrochyn, "Analysis of image protection algorithms parallel realization efficiency", in *Proc. Int. Sci. Conf. "Contemporary Problems of Computer Technologies"*, Khmelnitsky, Ukraine, 2014, pp. 335–342 (in Ukrainian).
7. M. Kharrazi *et al.*, "Performance study of common image steganography and steganalysis techniques", *J. Electronic Imaging*, no. 15 (4), pp. 1–16, 2006.
8. A. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world", in *Proc. 1st ACM Workshop IH&MMSec'13*, 2013, pp. 45–58.
9. S.K. Bandyopadhyay and I.K. Maitra, "An application of palette based steganography", *Int. J. Comp. Applications*, vol. 6, no. 4, pp. 24–27, 2010.
10. J. Daemen and V. Rijmen, *The Design of Rijndael, AES – the Advanced Encryption Standard*. Springer-Verlag, 2002, 238 p.
11. N.A. Ibraheem *et al.*, "Understanding color models: a review", *ARPN J. Sci. Technol.*, vol. 2, no. 3, 2012, pp. 265–275.

І.А. Дичка, С.С. Широчин, Є.С. Сулема

АНАЛІЗ ЕФЕКТИВНОСТІ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ ПРИ ЗАХИСТІ МУЛЬТИМЕДІЙНИХ ДАНИХ КОРИСТУВАЧА У ХМАРНИХ СХОВИЩАХ

Проблематика. Істотна частина даних, що зберігаються у хмарних сховищах, – це мультимедійні дані. Процедура захисту цих даних може бути реалізована як довірений хмарний сервіс. Оскільки цей сервіс є проміжним рівнем між рівнями користувача та хмарного сховища, час обробки даних у ньому є важливим показником. Для зменшення часу виконання процедури захисту можуть бути використані паралельні обчислення.

Мета дослідження. Мета роботи – оцінити та проаналізувати часову ефективність паралельних обчислень, що виконуються в процедурах захисту мультимедійних даних.

Методика реалізації. Подано результати порівняльного аналізу трьох методів стеганографічного захисту даних: методу стеганографічного захисту з фрагментацією даних, методу на основі комплементарного образу та методу LSB-стеганографії з шифруванням даних за алгоритмом AES. Ці методи розглянуто з точки зору часової ефективності обробки даних. Проаналізовано вплив кількості використовуваних стегобіт та кількості потоків паралельної обробки даних. Порівняно результати для мультимедійних даних двох типів – графічних та аудіоданих.

Результати дослідження. Отримані часові характеристики показують, що використання паралельних обчислень у методі на основі комплементарного образу дає змогу зменшити час обробки даних до 70 %.

Висновки. Отримані результати дають можливість порівняти розглянуті методи з огляду на часові характеристики їх програмної реалізації, що є, разом зі ступенем захисту, суттєвим для користувача хмарних сервісів. Метод на основі комплементарного образу з паралельною обробкою даних може бути рекомендований до використання у процедурі стеганографічного захисту мультимедійних даних.

Ключові слова: захист мультимедійних даних; стеганографія.

И.А. Дичка, С.С. Широчин, Е.С. Сулема

АНАЛИЗ ЭФФЕКТИВНОСТИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ ПРИ ЗАЩИТЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЯ В ОБЛАЧНЫХ ХРАНИЛИЩАХ

Проблематика. Существенная часть данных, хранящихся в облачных хранилищах, – это мультимедийные данные**.** Процедура защиты этих данных может быть реализована как доверенный облачный сервис. Поскольку этот сервис является промежуточным уровнем между уровнями пользователя и облачного хранилища, время обработки данных в нем является важным показателем. Для уменьшения времени, необходимого для процедуры защиты, могут быть использованы параллельные вычисления.

Цель исследования. Цель работы – оценить и проанализировать временную эффективность параллельных вычислений, которые выполняются в процедурах защиты мультимедийных данных.

Методика реализации. Представлены результаты сравнительного анализа трех методов стеганографической защиты данных: метода с фрагментацией данных, метода на основе комплементарного образа и метода LSB-стеганографии с шифрованием данных по алгоритму AES. Представленные методы рассмотрены с точки зрения временной эффективности обработки данных. Проанализировано влияние количества используемых стегобит и количества потоков параллельной обработки данных. Для сравнения использовались результаты для мультимедийных данных двух типов – графических и аудиоданных.

Результаты исследования. Полученные временные характеристики показывают, что использование параллельных вычислений в методе на основе комплементарного образа позволяет уменьшить время обработки до 70 %.

Выводы. Представленные результаты позволяют сравнить рассмотренные методы с точки зрения временных характеристик их программной реализации, что является, наряду со степенью защиты, существенным для пользователя облачных сервисов. Метод на основе комплементарного образа может быть рекомендован к использованию в процедуре стеганографической защиты мультимедийных данных.

Ключевые слова: защита мультимедийных данных; стеганография.

Рекомендована Радою
факультету прикладної математики
НТУУ “КПІ”

Надійшла до редакції
23 грудня 2015 року