*материаловедение:* восточно-европейский журнал передовых технологий. Харьков: Техн. центр, 2013. № 1/5(61). С. 4−6.

**References**

1. Zhiguts, Yu.Yu. 2008. Splavy, syntezovani metalotermiieiu i SVS-protsesamy [Alloys synthesized by metallothermy and SVS-processes]. Uzhgorod: Grazhda.

2. Zhiguts, Yu., and Lazar V. 2009. “Resursozberihaiucha tekhnolohiia termitnoho zvariuvannia stalevykh detalei [Resource-saving technology of thermit welding of steel parts]”. *Bulletin of TDTU* 14, 4: 94–98.

3. Zhiguts, Yu. Yu. 2012. “Tekhnolohiia otrymannia termitnykh sudnobudivnykh stalei [The technology of obtaining termite shipbuilding steels]”. *Bulletin of the Donbas State Machine-Building Academy* 3(28): 283−286.

4. Zhiguts, Yu. Yu. 2007. “Vykorystannia termitnykh lehovanykh stalei dlia zhyvlennia vylyvkiv [The use of thermite alloyed steels for feeding castings]”. *Bulletin of the Lviv Polytechnic National University* 583: 118–122.

5. Zhiguts, Yu., and Shirokov, V. 2005. “Metodyka rozrakhunku skladu ekzotermichnykh shykht na osnovi termokhimichnoho analizu [Methodology for calculating the composition of exothermic charges based on thermochemical analysis]”. *Mechanical engineering* 4: 48−50.

6. Zhiguts, Yu.Yu. 2013. Syntez termitnykh kavitatsiinostiikykh stalei [Synthesis of thermite cavitation-resistant steels]”. *Applied physics and materials science* 1/5(61): 4-6.

**УДК 51:004.056.55:004.05(045)**

## ТЕХНОЛОГІЯ РЕСУРСОЗБЕРЕЖЕННЯ ПРИ ШИФРУВАННІ ІНФОРМАЦІЇ

Ігнатишин М. І., Жигуц Ю. Ю., Лазар В. Ф.

## RESOURCE SAVING TECHNOLOGY IN ENCRYPTING INFORMATION

Ihnatyshyn Mykola, Zhihuts Yuriy, Lazar Vasyl

*Шифрування інформації та енергозбереження є двома різними концепціями, але можуть мати певний зв'язок у деяких аспектах. Ефективне управління інформацією може допомогти зменшити кількість ресурсів. Наприклад, використання компресії даних дозволяє зменшити обсяг інформації, яка потрібна для збереження, і, крім того, зменшує вимоги до обладнання та пропускної здатності. У процесі шифрування можна використовувати алгоритми, які вимагають значних обчислювальних ресурсів. Це може призвести до більшого споживання енергії в пристроях, що використовують шифрування. Особливо це стосується мобільних пристроїв, які мають обмежені ресурси, таких як смартфони або планшети. Хаотична динаміка може бути застосована для створення ефективних криптографічних систем у контексті генерації ключів, шифрування та розшифрування даних. Розглянуто застосування хаотичної динаміки подвійного маятника для генереції шифрувальної матриці та шифрування зображення.*

***Ключові слова:*** *шифрування, хаотична динаміка.*

*Information encryption and energy saving are two different concepts, but may have some connection in some aspects. Effective information management can help reduce the number of resources. For example, using data compression can reduce the amount of information that needs to be stored and, in addition, reduces hardware and bandwidth requirements. Algorithms that require*

*significant computing resources can be used in the encryption process. This may result in higher power consumption on devices using encryption. This is especially true for mobile devices that have limited resources, such as smartphones or tablets. Chaotic dynamics can be applied to create efficient cryptographic systems in the context of key generation, data encryption and decryption. The application of the chaotic dynamics of a double pendulum for the generation of an encryption matrix and image encryption is considered.*

***Keywords:*** *encryption, chaotic dynamics.*

Застосування хаотичних послідовностей чисел різного походження є актуальним при шифруванні інформації. В [1] розглянуто апаратну реалізація пристрою шифрування мовної інформації хаотичними послідовностями, що генеруються на основі одномірних дискретних хаотичних відображень. Роботу пристрою досліджено на прикладі шифрування гармонійного сигналу. Проведені дослідження пристрою підтвердили можливість застосування мікроконтролерів для шифрування мовної інформації з використанням сучасних криптостійких алгоритмів. Алгоритм шифрування текстової інформації, що базується на використанні двох динамічних систем, системи Ресслера та кубічного відображення представлено в [2]. В роботі також було проведено моделювання роботи динамічних систем в середовищі Matlab. Спосіб шифрування зображення з використанням хаотичного відображення запропоновано в [3].

Враховуючи збільшення обсягів інформації, яку необхідно зашифрувати, актуальною є потреба в ресурсозберігаючих методах шифрування, які дозволяють ефективно використовувати наявні обчислювальні ресурси.

Хаотична динаміка може бути застосована для створення ефективних криптографічних систем у контексті генерації ключів, шифрування та розшифрування даних.

Нами застосовано хаотичну динаміку подвійного маятника [4] для шифрування зображення, рис.1.

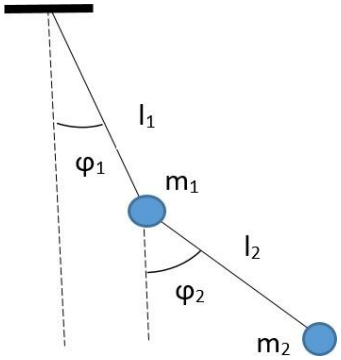



**Рис.1. Подвійний маятник.**

Програма шифрування реалізована в Mathcad 2001 і складається з файлів:

1. Генератор шифрувальної матриці A «GeneratorSend». Перетворює зображення в цифрову матрицю та визначає кількість рядків і стовпчиків матриці. Генерує шифрувальну матрицю, що має кількість рядків і стовпчиків матриці таку як у зображення.

**Рис.2. Генератор шифрувальної матриці A «GeneratorSend».**

2. Генератор шифрувальної матриці A «GeneratorAccept». Перетворює зашифроване зображення в цифрову матрицю та визначає кількість рядків і стовпчиків матриці. Генерує шифрувальну матрицю, що має кількість рядків і стовпчиків матриці таку як у зображення.

**Рис.3. Генератор шифрувальної матриці A «GeneratorAccept».**

3. «SendBMP» файл, що шифрує зображення.

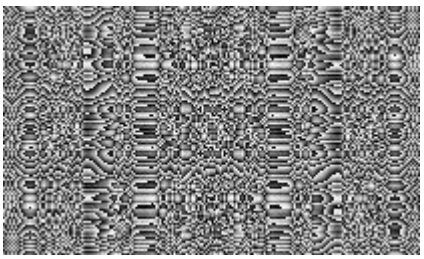
**Рис.4. «SendBMP» файл, що шифрує зображення.**

Блок шифрування.

M := READBMP ("Send" ) - оператор, що переводить зображення "Send" в числову матрицю.

A := READBMP ("A") - оператор, що переводить зображення, шифрувальну матрицю "A", в числову матрицю, рис.2.

"Send"

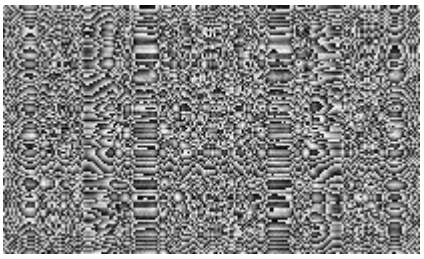


"A"

**Рис.2. Шифрування зображення.**

M := M + A - шифрування зображення.

WRITEBMP ("M.bmp" ) := M - збереження зашифрованого зображення для передачі його отримувачу, рис.3.



"M"

**Рис.3. Зашифроване зображення.**

4. «AcceptBMP» файл, що розшифровує зображення.

Блок дешифрування.

M := READBMP ("M" ) - оператор, що переводить зашифроване зображення "M" в числову матрицю.

A := READBMP ("A") - оператор, що переводить зображення, шифрувальну матрицю "A", в числову матрицю.

M := M – A - дешифрування зображення. На рис.4 розшифроване зображення, збереження кольору не передбачалось.

M

**Рис.4. Розшифроване зображення.**

В роботі використано хаотичну динаміку для шифрування зображення та текстової інформації. В середовищі Mathcad створено програму шифрування на

основі хаотичної динаміки подвійного маятника, яка включає генератори шифрувальних матриць і блоки шифрування та дешифрування для зображення. Вказано на важливість ресурсозбереження в контексті шифрування інформації та використання хаотичної динаміки для реалізації ефективних криптографічних систем.

**Список використаних джерел**

1. Апаратна реалізація пристрою шифрування мовної інформації / О. Гресь та ін. *Сучасний захист інформації*. 2014. № 3.

2. Косован Г. В., Кушнір М. Я., Політанський Л. Ф. Алгоритм шифрування інформації на основі двох хаотичних динамічних систем для захищених систем зв'язку. *Захист інформації*. 2013. Т. 15, № 4. С. 299-306. URL: https://nbuv.gov.ua/UJRN/Zi_2013_15_4_6.

3. Політанський Л. Ф., Кушнір М. Я., Косован Г. В. Спосіб шифруваннязображення з використанням хаотичного відображення: пат. UA 80695 U, МПК H04L 9/24, H03M 7/00. подання заявки 10.12.2012; опубліковано10.06.2013, Бюл. № 11.

4. Ігнатишин М. І., Туряниця І. І., Пелех Я. М. Дослідження та анімація хаотичного руху подвійного маятника в пакеті mathcad. *Міжнародний науковий журнал «Освіта і наука».* 2021. Вип. 2(31). С. 18–22.

**References**

1. Hres, O. and others. 2014. Aparatna realizatsiia prystroiu shyfruvannia movnoi informatsii [Hardware implementation of the language information encryption device]. *Modern information protection* 3.

2. Косован Г. В., Кушнір М. Я., Політанський Л. Ф. 2013. Алгоритм шифрування інформації на основі двох хаотичних динамічних систем для захищених систем зв'язку. *Захист інформації* 15, 4: 299–306. https://nbuv.gov.ua/UJRN/Zi_2013_15_4_6.

3. Politanskyi L. F., Kushnir M. Ya., Kosovan H. V. Sposib shyfruvanniazobrazhennia z vykorystanniam khaotychnoho vidobrazhennia: pat. UA 80695 U, MPK H04L 9/24, H03M 7/00. podannia zaiavky 10.12.2012; opublikovano10.06.2013, Biul. № 11 [A method of image encryption using chaotic mapping: patent. UA 80695 U, IPC H04L 9/24, H03M 7/00. submission of the application on 10.12.2012; published on 10.06.2013, Bull. No. 11.].

4. Ihnatyshyn M. I., Turianytsia I. I., Pelekh Ya. M. 2021. Doslidzhennia ta animatsiia khaotychnoho rukhu podviinoho maiatnyka v paketi mathcad [Investigation and animation of the chaotic motion of a double pendulum in the mathcad package]. *International scientific journal "Education And Science"* 2(31): 18–22.

# МУКАЧІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

**89600, м. Мукачево, вул. Ужгородська, 26**
**тел./факс +380-3131-21109**
**Веб-сайт університету: www.msu.edu.ua**
**E-mail: info@msu.edu.ua, pr@mail.msu.edu.ua**
**Веб-сайт Інституційного репозитарію Наукової бібліотеки МДУ: http://dspace.msu.edu.ua:8080**
**Веб-сайт Наукової бібліотеки МДУ: http://msu.edu.ua/library/**