© Barannik V., Havrilov D., Shulgin S., Parkhomenko M., Yroshenko V. The possibility of using the arithmetic coding method in the systems of cryptographic information protection // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 3, pp. 156-167.

Криптологія / Cryptology

DOI: 10.18372/2225-5036.26.15157

МОЖЛИВІСТЬ ЗАСТОСУВАННЯ МЕТОДІВ АРИФМЕТИЧНОГО КОДУВАННЯ В СИСТЕМАХ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Бараннік[1], Дмитро Гаврилов[1], Максим Пархоменко[2], Сергій Шульгін[1] , Валерій Ерошенко[2]

[1]Харківський національний університет радіоелектроніки, Україна
[2]Харківський національний університет Повітряних Сил, Україна

БАРАННІК Володимир Вікторович, д.т.н., професор.

Рік та місце народження: 1971 рік, м. Ізюм, Харківська область, Україна.
Освіта: Харківський військовий університет, 1994 рік.
Посада: професор кафедри штучного інтелекту та програмування Харьковского национального университета имени В.Н. Каразина.
Наукові інтереси: технології кодування, штучній інтелект, інформаційна безпека.
Публікації: понад 750 наукових публікацій, монографії, підручники, навчальні посібники, наукові статті та патенти на винахід.
E-mail: vvbar.off@gmail.com.
Orcid ID: 0000-0002-2848-4524.

ГАВРИЛОВ Дмитро Сергійович, аспірант

Рік та місце народження: 1995 рік, м. Харків, Харківська область, Україна.
Освіта: Харківський національний університет Повітряних Сил ім. Івана Кожедуба, 2017 рік.
Посада: аспірант.
Наукові інтереси: інформаційна безпека, селективні методи, кодування, шифрування.
Публікації більше 20 наукових публікацій, серед яких монографії, наукові статті та тези доповідей на конференціях.
E-mail: havrylov_d@ukr.net.
Orcid ID: 0000-0002-3344-7808.

ПАРХОМЕНКО Максим Вікторович

Рік та місто народження: 1976 год, м. Токмак, Запоріжська область, Украина.
Освіта: Харьковскій інститут Військово-Повітряних Сил, 2001 рік.
Посада: викладач Харьковского національного університету Повітряних Сил, Харків, Україна.
Наукові інтереси: інформаційна безпека, селективні методи, кодування, шифрування.
Публікації: более 13 наукових публікацій.
E-mail: maxpro@gmail.com.
Orcid ID: 0000-0001-6062-7743.

ШУЛЬГІН Сергій Сергійович, к.т.н.

Рік та місто народження: 1983 рік, м. Черкаси, Україна.
Освіта: Черкаський державний технологічний університет , 2012 рік.
Посада: докторант, Харьковского національного університету радіоелектроніки.
Наукові інтереси: інформаційна безпека.
Публікації: более 20 наукових публікацій.
E-mail: barannik_v_v@ukr.net.
Orcid ID: 0000-0001-5174-290X.

ЕРОШЕНКО Валерій Петрович, к.т.н.

Рік та місто народження: 1959 рік, село Смяліч Брянська область, СРСР
Освіта: Харківське вище авіаційне льотне училище, 1980 рік.
Посада: викладач кафедри Харківського національного університету Повітряних Сил.
Наукові інтереси: інформаційна безпека.
Публікації: более 120 наукових публікацій.
E-mail: wpEroshenko@gmail.com.
Orcid ID: 0000-0003-3175-6444.

Анотація. *В статті проведено аналіз останніх публікацій, що вказав на стрімке створення даних різними типами носіїв. Відзначено, що п'ята частина створених даних є критично важливою та потребує захисту. Для зменшення об'єму даних, що зберігається, пропонується використовувати методи кодування без побудови таблиці кодування. Саме тому, детально розглянуто арифметичне та адаптивне арифметичне кодування з позиції можливості застосування в системах криптографічного захисту інформації для систем критичної інфраструктури. В результаті дослідження для гарантованого захисту інформації пропонується використовувати технологію послідовного криптографічного захисту інформації (після кодування) з застосуванням адаптивного арифметичного кодування. Для систем з потоковою обробкою даних (технологія селективного захисту інформації) пропонується застосовувати арифметичне кодування. Під ключовою інформацією в алгоритмі арифметичного кодування розуміємо вагу кожного елементу, решта інформації додаткового захисту не потребує.*

Ключові слова: *захист інформації, арифметичне кодування, адаптивне арифметичне кодування, Великі Дані(Big Date).*

Вступ

Стратегічно важливим для функціонування Не зважаючи на активний розвиток технологій та принципів побудови носіїв інформації, направлених на збільшення об'єму даних, що можуть зберігатися (при зменшенні фізичного об'єму та ваги) потреба в алгоритмах зменшення об'єму досі є актуальною проблематикою, що потребує вирішення. Даний ефект зберігається у зв'язку з одночасним розвитком технологій вводу даних. До даних технологій можна віднести фото та відеокамери різних фірм, які дозволяють отримувати багатовимірні дані високої якості (роздільної здатності) та глибини побудови зображень, що в свою чергу значно збільшує об'єм інформації необхідної для зберігання та подальшому відтворення на засобах відображення.

При цьому, використання високотехнологічних пристроїв спостерігається не лише на рівні держав чи підприємств, а й на рівні персонального користувача, який в свою чергу має змогу надавити доступ та/чи висвітлювати фото, відео, тощо на ресурсах соціальних мереж, блогах, сховищах хмарного типу чи власних сайтах.

В результаті даної можливості користувач ініціює вимоги до адміністраторів, провайдерів, власників перерахованих вище інформаційних ресурсів з позиції потреби в ресурсах (сховищах) та швидкодії (обчислювальна потужність) замикаючи коло «Інформаційних ресурс (сховище) – Якість (об'єм) - Інформаційних ресурс (сховище))».

Адже, ринок надання інформаційних послуг зріс настільки, що незадоволений користувач (тривалий час завантаження, недостатня функціональність чи навіть незадовільний дизайн сайту) має можливість легко та швидко (на протязі не більше декількох хвилин) змінити провайдера послуг, що спричинить збиток останньому.

Множина користувачів, об'єднаних в організації, підприємства, держави призвело до появи поняття Великих даних (Big Date). Під Big Date розуміємо роботу з інформацією значного обсягу і різноманітного по структурному, семантичному складу даними, що оновлюється щосекунди і знаходиться в різних джерелах (сховищах) з метою забезпечення збереження, збільшення ефективності роботи, створення нових продуктів і підвищення конкурентоспроможності. Консалтингова компанія Forrester дає коротке формулювання: «Великі дані об'єднують техніки і технології, які витягують сенс з даних з максимальною практичністю».

Аналіз існуючих досліджень

За даними аналітиків IDC [10 - 43] та інших дослідників, в найближчі роки основний обсяг даних будуть проводити не користувачі, а компанії. На промисловість та інші сфери економіки доведеться до 60% всіх даних світу. Наприклад, у 2015 році підприємства генерували третину всіх світових даних. Автори розглянутих досліджень єдині в думці про те, що в майбутньому набагато важливіше буде якість даних, а не їх кількість. «Не всі дані однаково важливі, а без контексту вони і зовсім не приносять користі. У цей період змін лідерство буде належати організаціям, які зуміють визначити найбільш критичні підгрупи інформації з максимальним впливом на потрібну сферу діяльності і зосередяться саме на них », - йдеться в звіті аналітиків IDC. В публікаціях також відзначалося, що до 2025 року обсяг створених даних в світі перебільшить 150 Зеттабайтів (10^{21} байт) на рік (рис. 1). При цьому п'ята частина всіх даних до 2025 року буде вважатися критично важливою.

Тобто це ті відомості, від яких буде залежати життя і безпеку людей, збереження капіталу компаніями, репутація країн, міжнародна обстановка, мир на планеті та питання існування планети Земля вцілому.

При цьому в найближчі роки розрив між обсягом даних, що потребують захисту, і реально захищеною інформацією буде тільки рости, ще більше збільшуючи об'єм даних.

До 2025 року до 90% всієї інформації повинно бути так чи інакше захищене.

Проте, фактично під захистом буде перебувати менше половини всього обсягу відомостей.

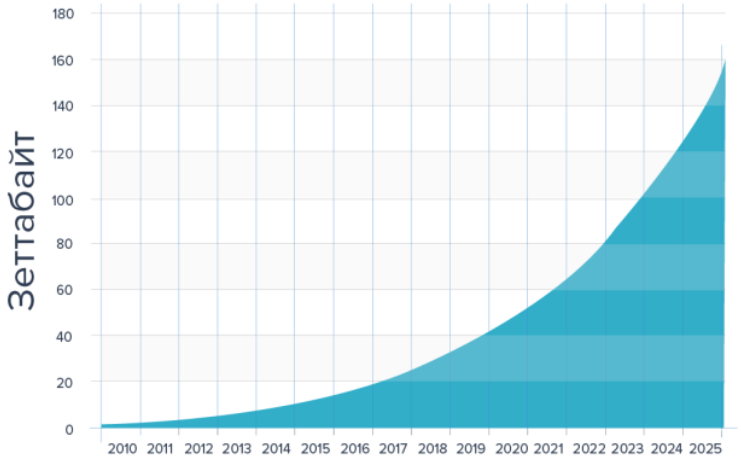


Рис. 1. Кількість створених даних в світі з прогнозом до 2025 року

Дослідники відзначають також, що значний обсяг даних буде виходити з пристроїв, які оточують нас кожен день у відповідності до концепції Інтернету Речей (Internet of Things), таким чином можна зробити висновок, що:

По-перше, до 2025 року 75% всього населення Землі буде мати постійний доступ в Інтернет.

Кількість відправлених даних в світи по типу носіїв приведено на рис. 2.

По-друге, кратно зросте кількість розумних гаджетів і домашніх роботів, які будуть виробляти так звані метадані - службову інформацію, якої машини будуть обмінюватися між собою для злагодженої роботи.

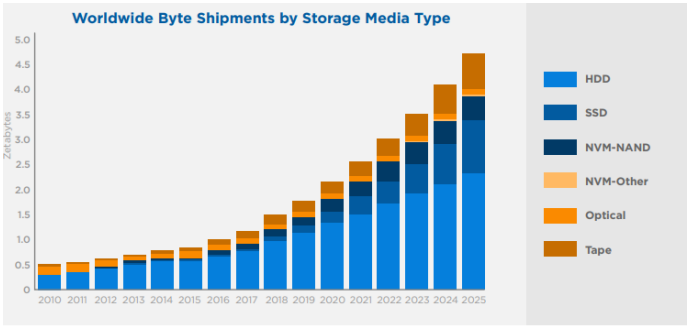


Рис. 2. Кількість відправлених даних в світи по типу носіїв

У порівнянні з сьогоднішнім днем кожна людина буде в 20 разів частіше взаємодіяти з Інтернетом або з пристроями з виходом в Інтернет.

Якщо зараз середня кількість взаємодій - трохи більше 1400, то до 2025 року ми буде стикатися з мережею більше 4900 раз в день (рис. 3).

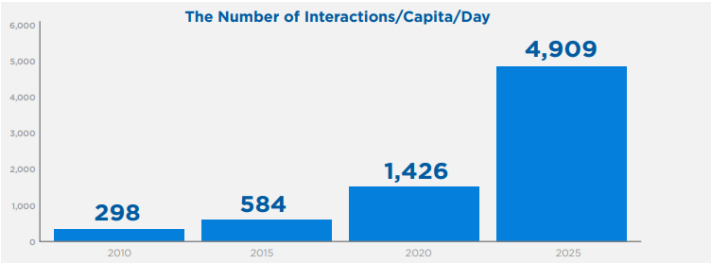


Рис. 3. Кількість взаємодії користувачі з Інтернетом (раз/день)

Тож, відшуковуючи шляхи рішення проблеми зберігання великої кількості інформації було з'ясовано наявність різних підходів до вирішення задачі зменшення кодової послідовності (об'єму даних) для обробки, зберігання та/чи передачі інформації.

Аналіз методів кодування на основі побудови таблиць Хаффмана, RLE, Лемпеля-Зіва, арифметичного кодування та адаптивного арифметичного кодування вказало як на позитивні, так і негативні властивості кожного метода.

Враховуючи те, що основними критеріями вибору алгоритму є здатність зменшувати об'єм даних (не збільшуючи у виняткових випадках) при надходженні на обробку даних з ймовірністю появи елементів близької до рівноймовірної та час роботи алгоритму.

Емпіричним шляхом, реалізованого за допомогою об'єктно-орієнтованої мови програмування Java, було набрано статистичні дані близько 10 000 об'єктів до яких входили числа в двійковому та десятинному представленні, масиви даних (матриці, блоки), слова та речення, та обрано для більш детального дослідження арифметичне кодування та адаптивне арифметичне кодування.

Метою даної роботи є визначення придатності арифметичного кодування та адаптивного арифметичного кодування для застосування в технологіях забезпечення криптографічного захисту інформації в об'єктах критичної інфраструктури.

Основна частина дослідження

Обрання в якості дослідження методів заснованих на принципах арифметичного кодування обумовлено тим, що дані методи є винятковими, адже не будують таблиці кодів, як більшість методів кодування, та у випадку адаптивного арифметичного кодування мають можливість поточного кодування. В результаті кодування отримуємо дійсне число в межах інтервалу [0,1) (low – початок робочого інтервалу; high – кінець робочого інтервалу), що дає змогу однозначно відтворити кодовану послідовність.

Алгоритм арифметичного кодування (рис. 5) та декодування (рис. 6) дозволяє знайти розбіжність з алгоритмом адаптивного кодування (рис. 7) та декодування (рис. 8), яка полягає у тому, що ваги символів, що поступають на вхід кодера, для арифметичного кодування формуються перед початком процесу кодування та мають бути передані декодеру.

В той час при адаптивному арифметичному кодуванні величина ваг кожного символу формується в процесі кодування, без необхідності передачі цих службових даних декодеру.

Вага елементу знаходиться за формулою:

$$\eta_i = \eta_i^{(0)} + \eta_i^{(1)} + \eta_i^{(w)}, \quad (1)$$

де η_i – сума ваг на і -тому кроці, $\eta_i^{(0)}$ – вага «0» на і -тому кроці, $\eta_i^{(1)}$ – вага «1» на і -тому кроці, $\eta_i^{(w)}$ – вага «w» на і -тому кроці.

Величина сегмента ρ_i на і -тому кроці знаходиться за формулою:

$$\rho_i = \frac{h_i - l_i}{\eta_i}. \quad (2)$$

Заключним етапом є знаходження кодового числа шляхом визначення середнього арифметичного числа між початком і кінцем робочого інтервалу останнього кодованого символу в повідомленні:

$$Z = \frac{l_i + h_i}{2}, \quad (3)$$

де Z – кодове число повідомлення.

Графічно процес адаптивного арифметичного кодування бітової послідовності " 0 0 1 0 1 1 1 0" прийме вигляд рис. 4.

В результаті отримаємо закодоване число 24_2 = 1 1 0 0 0 з коефіцієнтом компресії 1,6. Аналіз рис. 5 та рис. 6 дає змогу зробити наступні висновки по можливості застосування даних методів в системах криптографічного захисту:

- у зв'язку з важливістю значень ваги $\eta_i^{(w)}$ елемента «w» на і -тому кроці можна зробити висновок, що дана інформація є ключовою. Вилучення чи заміна значень ваги $\eta_i^{(w)}$ елемента «w» на і-тому кроці унеможливить коректне відтворення закодованої послідовності. При цьому варто відзначити, що величина ваги $\eta_i^{(w)}$ елемента «w» на кожному кроці рівна:

$$\eta_1^{(w)} = \eta_2^{(w)} = \eta_3^{(w)} = \ldots = \eta_i^{(w)}, \quad (4)$$

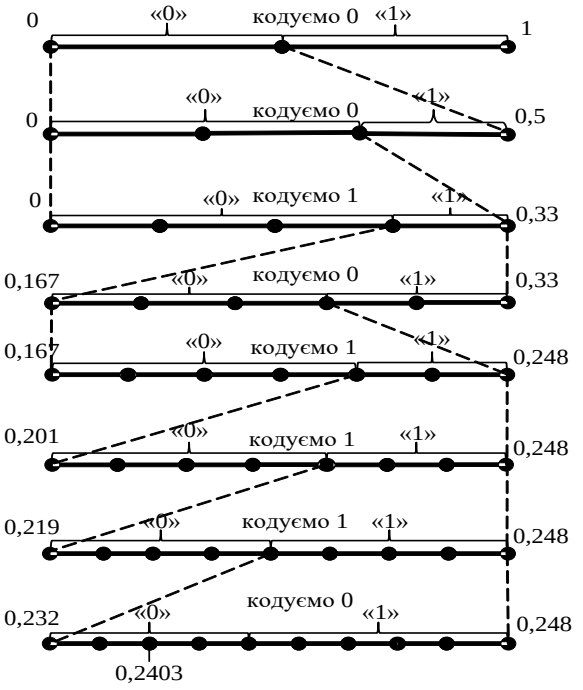


Рис. 4 Побудова адаптивного арифметичного коду

Дана особливість дає можливість рахувати що застосування криптографічних даних для значень ваги $\eta_i^{(w)}$ елемента «w» може збільшити ступінь захищеності даних:

- у зв'язку з необхідністю проходу для визначення ваги $\eta_i^{(w)}$ елемента «w» застосування методу арифметичного кодування збільшує час на обробку даних. Аналіз рис. 7 та рис. 8 дає змогу зробити наступні висновки по можливості застосування даних методів в системах криптографічного захисту:

- у порівнянні з методом арифметичного кодування зменшити час на обробку даних при кодуванні за рахунок відсутності проходу для визначення ваги $\eta_i^{(w)}$ елемента «w»;

- у порівнянні з методом арифметичного кодування даний метод, як правило, має нижчий коефіцієнт компресії;

- у зв'язку з тим, що до кінця обробки кодованих елементів неможливо визначити величину ваги $\eta_i^{(w)}$ елемента «w» застосування методу адаптивного арифметичного кодування в технологіях криптографічного захисту інформації зводиться до послідовної обробки даних.

Для загального аналізу проведено оцінку ефективності робити методів арифметичного кодування та адаптивного арифметичного кодування у системі криптографічного захисту інформації (рис. 9).

Аналіз рис. 9 вказав на те, що адаптивне кодування дозволяє отримати вищій коефіцієнт компресії та менший час обробки даних, ніж у адаптивного арифметичного кодування.

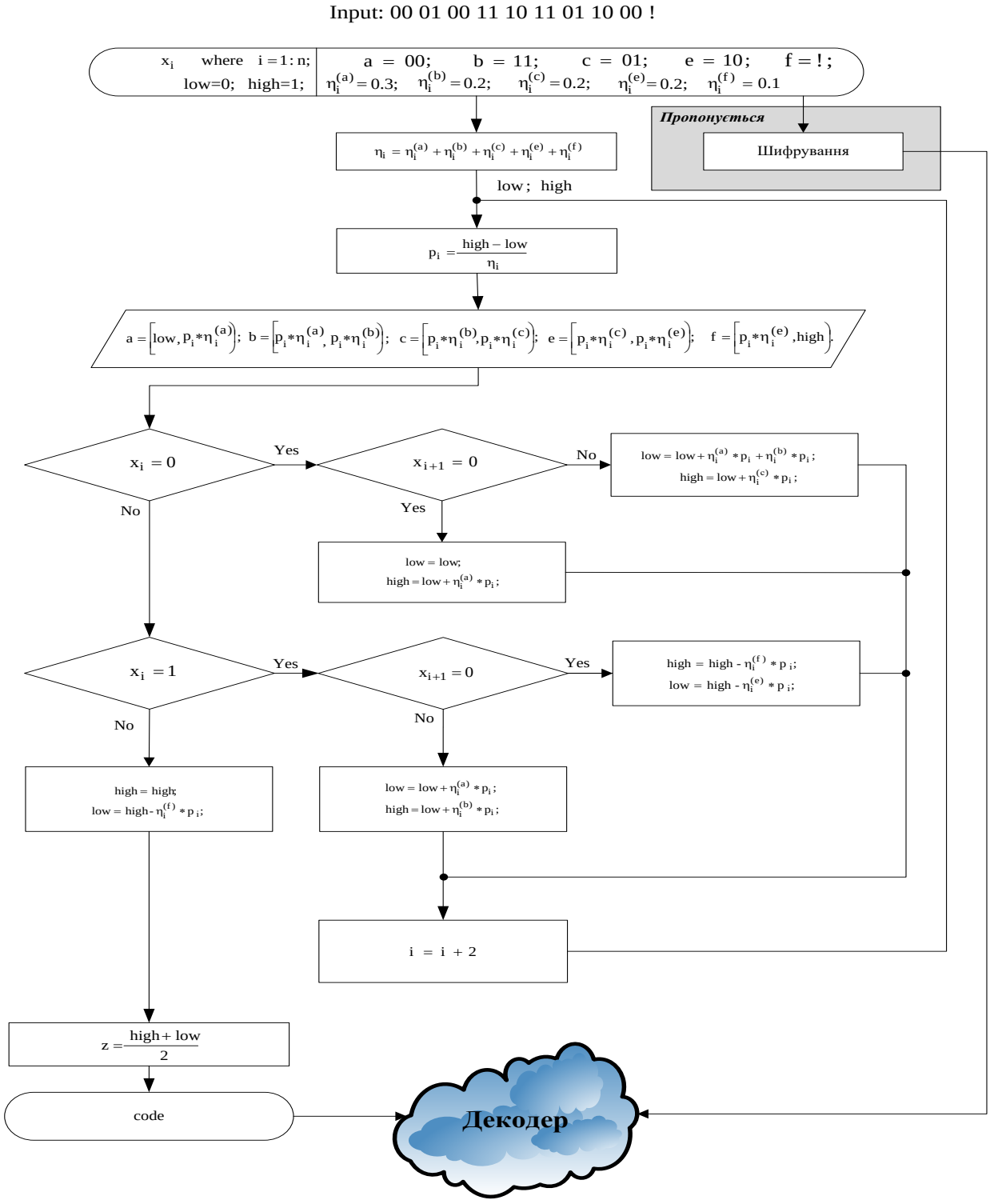
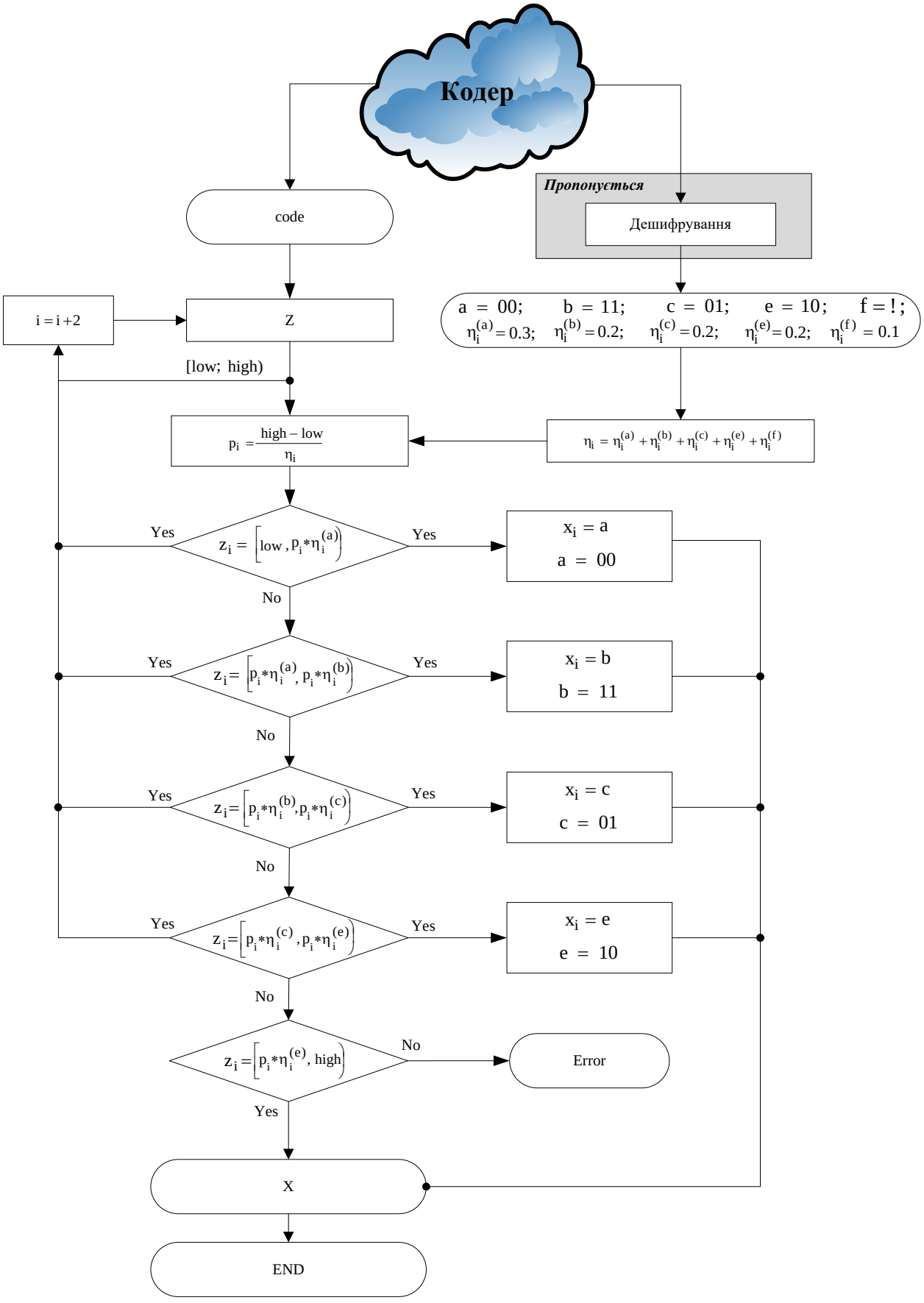


Рис. 5. Приклад роботи арифметичного кодування для бінарної послідовності з маркером стопу "!"



Output: 00 01 00 11 10 11 01 10 00

Рис. 6. Приклад роботи декодера арифметичного кодування для бінарної послідовності

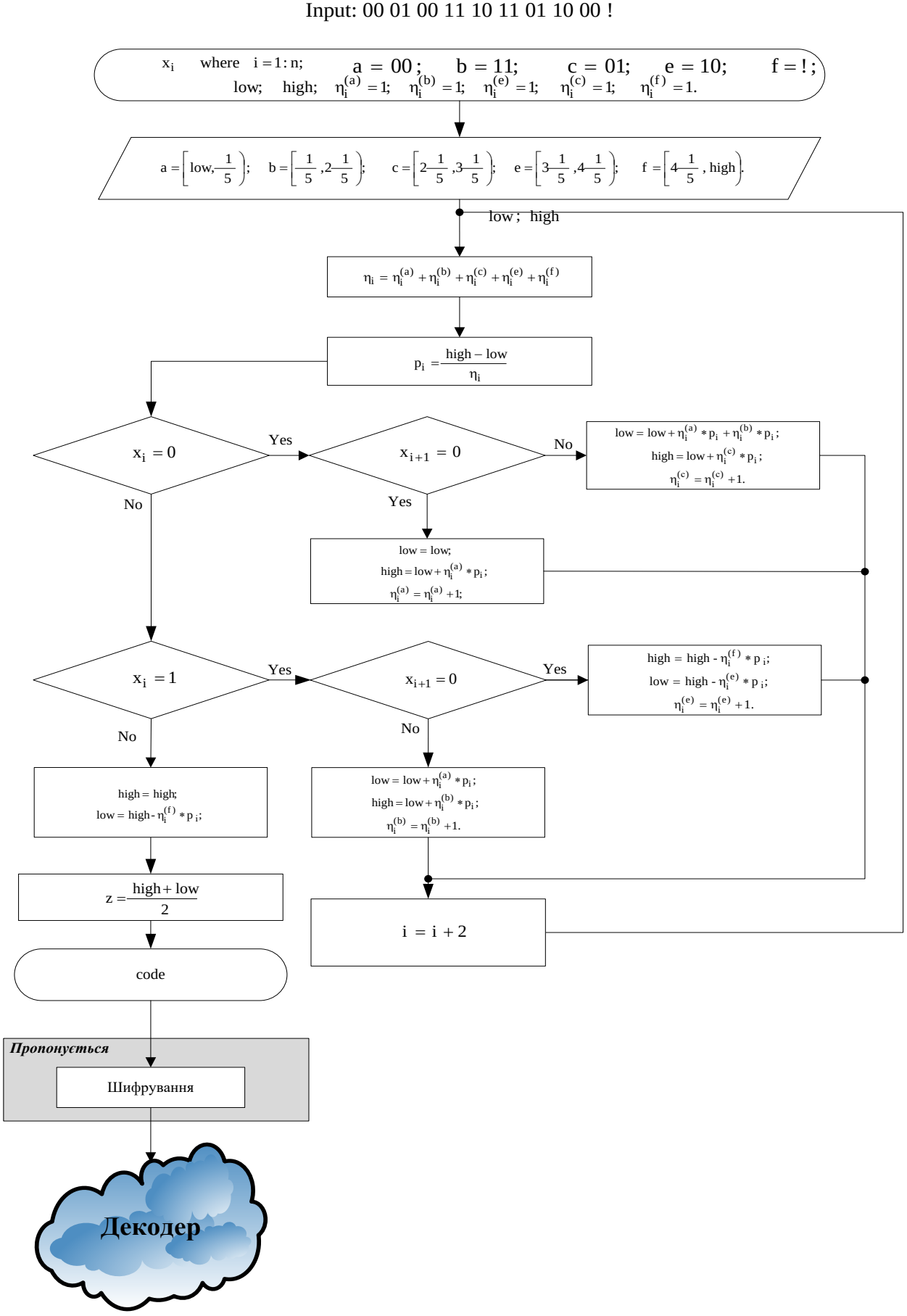
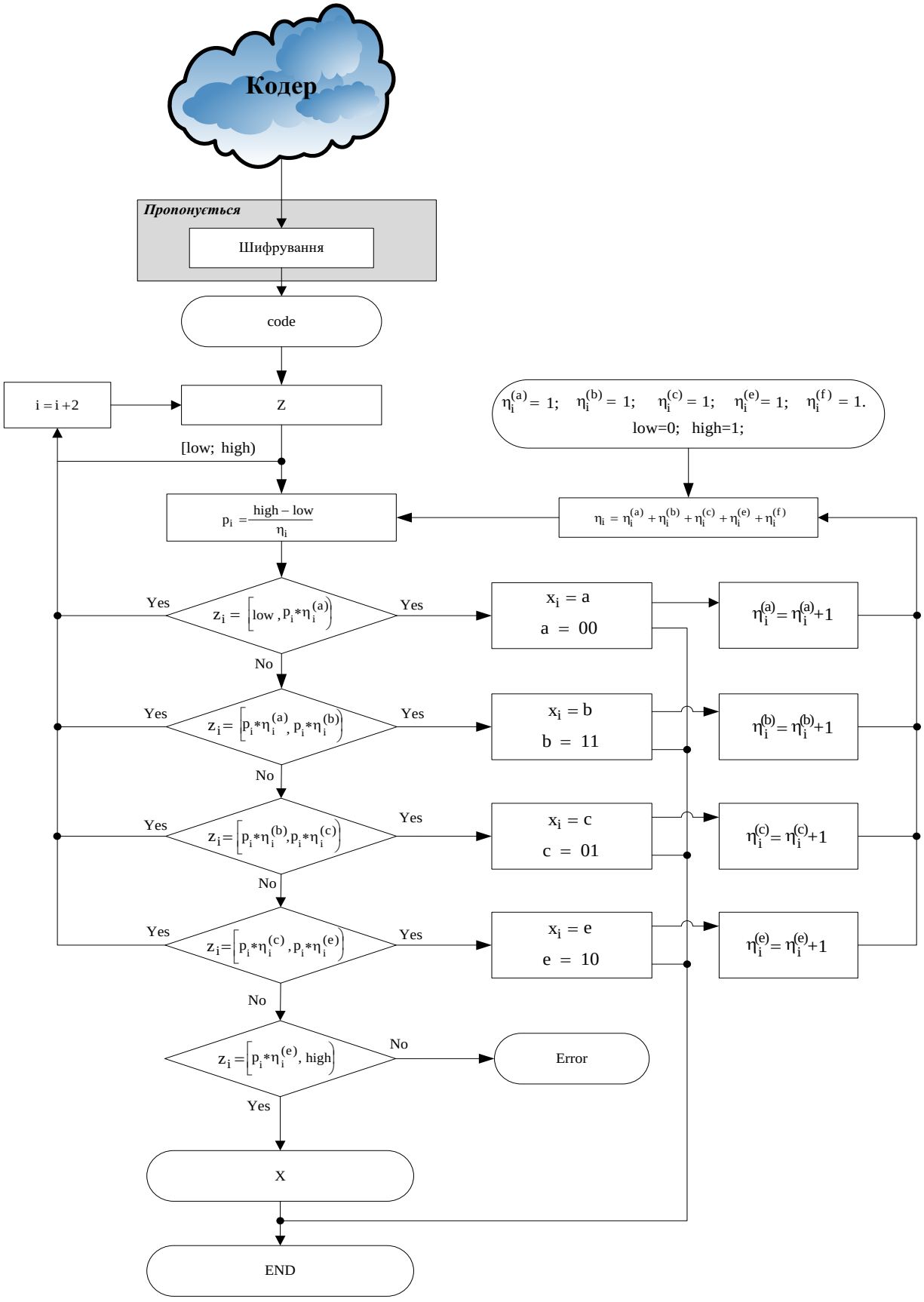


Рис. 7. Приклад роботи адаптивного арифметичного кодування для бінарної послідовності з маркером стопу "!"



Output: 00 01 00 11 10 11 01 10 00

Рис. 8. Приклад роботи декодера адаптивного арифметичного кодування для бінарної послідовності

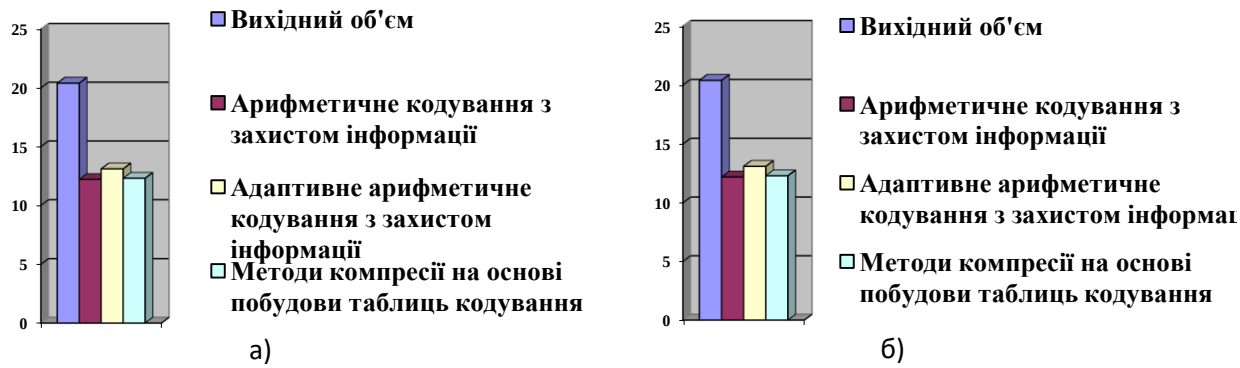


Рис. 9. Оцінка ефективності методів, що досліджується а) по об'єму даних б) по часу обробки

Таким чином, вважаємо, що арифметичне кодування є більш прийнятним рішенням для застосування в системах криптографічного захисту інформації у порівнянні з адаптивним арифметичним кодуванням та методами компресії на основі побудови таблиць кодування.

Висновки

В статті детально розглянуто арифметичне та адаптивне арифметичне кодування з позиції можливості застосування в системах криптографічного захисту інформації для систем критичної інфраструктури.

В результаті, аналіз методу арифметичного кодування дає змогу зробити наступні висновки по можливості застосування даних методів в системах криптографічного захисту:

- у зв'язку з важливістю значень ваги $\eta_i^{(w)}$ елемента «w» на і -тому кроці можна зробити висновок, що дана інформація є ключовою. Вилучення чи заміна значень ваги $\eta_i^{(w)}$ елемента «w» на і -тому кроці унеможливить коректне відтворення закодованої послідовності. При цьому варто відзначити, що величина ваги $\eta_i^{(w)}$ елемента «w» на кожному кроці рівна. Дана особливість дає можливість рахувати що застосування криптографічних даних для значень ваги $\eta_i^{(w)}$ елемента «w» може збільшити ступінь захищеності даних;

- у зв'язку з необхідністю проходу для визначення ваги $\eta_i^{(w)}$ елемента «w» застосування методу арифметичного кодування збільшує час на обробку даних.

Аналіз методу адаптивного арифметичного кодування дає змогу зробити наступні висновки по можливості застосування даних методів в системах криптографічного захисту:

- у порівнянні з методом арифметичного кодування зменшити час на обробку даних при кодуванні за рахунок відсутності проходу для визначення ваги $\eta_i^{(w)}$ елемента «w»;

- у порівнянні з методом арифметичного кодування даний метод, як правило, має нижчий коефіцієнт компресії;

- у зв'язку з тим, що до кінця обробки кодованих елементів неможливо визначити величину ваги $\eta_i^{(w)}$ елемента «w» застосування методу адаптивного арифметичного кодування в технологіях криптографічного захисту інформації зводиться до послідовної обробки даних.

Виходячи з цього, методи арифметичного кодування можливо застосовувати в системах криптографічного захисту з метою зменшення вихідного об'єму даних.

При чому, аналіз вказав на те, що адаптивне кодування дозволяє отримати вищій коефіцієнт компресії та менший час обробки даних, ніж у адаптивного арифметичного кодування.

Таким чином, вважаємо, що арифметичне кодування є більш прийнятним рішенням для застосування в системах криптографічного захисту інформації у порівнянні з адаптивним арифметичним кодуванням та методами компресії на основі побудови таблиць кодування.

Література

[1] Баранник В.В. *Основы теории структурно-комбинаторного стеганографического кодирования: монография* / В.В. Баранник, Д.В. Баранник. – Х.: Издательство «Лидер», 2017. – 256 с.

[2] Announcing the ADVANCED ENCRYPTION STANDARD // *Federal Information Processing Standards Publication* [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[3] Auer. S., Bliem A., Engel. D., Uhl. A., Unterweger. A. Bitstream-based JPEG Encryption in Real-time //*International Journal of Digital Crime and Forensics*, 2013. – 17 p.

[4] Barannik V., Barannik N., Ryabukha Yu., Barannik D. Indirect Steganographic Embedding Method Based On Modifications of The Basis of the Polyadic System // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 699-702.

[5] Barannik V., Barannik, V.: Binomial-Polyadic Binary Data Encoding by Quantity of Series of Ones // *15th IEEE International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET'2020)*, 2020. - pp. 775-780.

[6] Barannik V., Belikova T., Gurzhii P. The model of threats to information and psychological security, taking into account the hidden information destructive impact on the subconscious of adolescents // *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, 2019. - pp. 656 – 661.

[7] Barannik V., Krasnoruckiy A., Hahanova A. The positional structural-weight coding of the binary view of transformants // *East-West Design & Test Symposium (EWDTS)*. - Rostov-on-Don, 2013. - pp. 1-4.

[8] Barannik V.V., Ryabukha Yu.N., Kulitsa O.S. The method for improving security of the remote video information resource on the basis of intellectual processing of video frames in the telecommunication systems. Telecommunications and Radio Engineering, Vol. 76, No 9, 2017. - pp. 785-797.

[9] Barannik V., Shulgin S. The method of increasing accessibility of the dynamic video information resource // *2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, 2016, pp. 621-623.

[10] Barannik, V., Tarasenko, D. Method coding efficiency segments for information technology processing video // *4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2017. - pp. 551-555.

[11] Chen Ch.-Ch., Wu W.-J. A secure Boolean-based multi-secret image sharing scheme // *Journal of Systems and Software*, Vol. 92, 2014. - pp. 107-114.

[12] Chen T.-H., Wu Ch.-S. Efficient multi-secret image sharing based on Boolean operation. *Signal Processing*, Vol. 91, Iss. 1, 2011.- pp. 90-97.

[13] Deshmukh M., Nain N., Ahmed, M. An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic // *IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016. - pp. 690-697.

[14] DSTU 7624:2014: *Information Technology. Cryptographic protection of information. Symmetric block transformation algorithm.* Order of the Ministry of Economic Development of Ukraine № 1484, 2014.

[15] DSTU GOST 28147:2009: *Information processing system. Cryptographic protection. Cryptographic transformation algorithm* GOST 28147-89, 2008.

[16] Dufaux, F., Ebrahimi, T.: Toward a Secure JPEG. *Applications of Digital Image Processing* XXIX, Vol. 6312, 2006.

[17] Farajallah M. *Chaos-based crypto and joint crypto-compression systems for images and videos* [Електронний ресурс]. Режим доступу: https://hal.archives-ouvertes.fr / tel-01179610.

[18] Faraoun, K.M. A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology*, Vol. 17, 2014. - pp. 85–94.

[19] Honda T., Murakami Y., Yanagihara Y., Kumaki T., Fujino T. Hierarchical image-scrambling method with scramble-level controllability for privacy protection // *IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013. - pp. 1371-1374.

[20] *Information technology – JPEG 2000 image coding system: Secure JPEG 2000*. International Standard ISO/IEC 15444-8; ITU-T Recommendation T.807, 2007. - 108 p.

[21] Ji Sh., Tong X. , Zhang, M.: *Image encryption schemes for JPEG and GIF formats based on 3D baker with compound chaotic sequence generator* [Електронний ресурс]. Режим доступу: arXiv preprint. arXiv: 1208.0999.

[22] Executive Summary *JPEG Privacy & Security Abstract and Executive Summary* [Електронний ресурс]. Режим доступу: https://jpeg.org/items/ 20150910_ privacy_ security _su mmary.html.

[23] Kobayashi H., Kiya H.: Bitstream-Based JPEG Image Encryption with File-Size Preserving. // *IEEE 7th Global Conference on Consumer Electronics (GCCE)*, 2018. - pp. 1-4

[24] Korshunov, P. and Ebrahimi, T.: Using warping for privacy protection in video surveillance // *18th International Conference on Digital Signal Processing (DSP)*, 2013. - pp. 1-6.

[25] V. Barannik, V. Barannik, D. Havrylov, A. Sorokun.: Development Second and Third Phase of the Selective Frame Processing Method // *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019. - pp. 54-57.

[26] Minemura, K. and Moayed, Z. and Wong, K. and Qi, X. and Tanaka, K.: JPEG image scrambling without expansion in bitstream size // *19th IEEE International Conference on Image Processing*, 2012. - pp. 261-264.

[27] Naor M., Shamir A. Visual Cryptography. In: Proceedings of the Advances in Cryptology – *EUROCRYPT'94. Lecture Notes in Computer Science*, Vol. 950, 1995. - pp. 1-12.

[28] Phatak A. A Non-format Compliant Scalable RSA-based JPEG Encryption Algorithm. *International Journal of Image, Graphics and Signal Processing*, Vol. 8, No. 6, 2016. - pp. 64-71.

[29] Ramakrishnan S. *Cryptographic and Information Security Approaches for Images and Videos. CRC Press*, 2018. -962 p.

[30] Rivest R.L., Shamir A., Adleman L.M. A method for obtaining digital signatures and public-key cryptosystems // *Communications of the ACM*, (2) 21, 1978. - pp. 120–126.

[31] V. Barannik, M. Karpinski, V.Tverdokhleb, D.Barannik, V. Himenk, M. Aleksander The technology of the video stream intensity controlling based on the bit-planes recombination // *2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, 20-21 Sept. 2018, Lviv, Ukraine.

[32] Sharma, R. and Bollavarapu, S.: Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*, Vol. 117, No. 14, 2015/ - pp. 15-18.

[33] V. Barannik, D. Barannik, V. Fustii, M. Parkhomenko Evaluation of Effectiveness of Masking Methods of Aerial Photographs // *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2-6 July 2019, Lviv, Ukraine.

[34] Barannik V.V., Ryabukha Yu., Tverdokhleb V.V, Barannik D.V.: Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding // *Advanced Information and Communication Technologies, 2017 2nd International Conference*, 2017. - pp. 188-192.

[35] Tsai Ch.-L., Chen Ch.-J., Hsu, W.-L. Multimorphological image data hiding based on the application of Rubik's cubic algorithm // *IEEE International Carnahan Conference on Security Technology,* 2012. - pp. 135-139.

[36] Vasiliev, V.B., Okov, I.N., Strezhik, Yu.N., Ustinov, A.A., Shvetsov, N.V.Video data compression and protection in UAV information exchange radio channels //*Scientific and practical conference on Prospects for the development and use of complexes with unmanned aerial vehicles*, 2016. - pp. 202–204.

[37] Wong K.-W. Image encryption using chaotic maps. *Intelligent Computing Based on Chaos*, Vol. 184, 2009. -pp. 333–354.

[38] Wong K., Tanaka K. DCT based scalable scrambling method with reversible data hiding functionality // *4th International Symposium on Communications, Control and Signal Processing*, 2010. - pp. 1-4.

[39] Wu Yu., Agaian. S., Noonan J. Sudoku Associated Two Dimensional Bijections for Image Scrambling // *IEEE Transactions on multimedia* [Електронний ресурс]. Режим доступу: arXivpreprint.arXiv:1207.585 6v1.

[40] Yang, Ch.-N. and Chen, Ch.-H. and Cai, S.-R.: Enhanced Boolean-based multi secret image sharing scheme. *Journal of Systems and Software*, Vol. 116, 2016. - pp. 22-34.

[41] Yang. Y., Zhu B.B., Li S., Yu1, N. Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability. *EURASIP Journal on Information Security*, Vol. 2007, Article ID 56365, 2008. - 13 p.

[42] Yuan L., Korshunov. P., Ebrahimi T.Secure JPEG Scrambling enabling Privacy in Photo Sharing. // *11th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG)*, 2015. - pp. 1-6.

[43] Zhou Y., Panetta K., Agaian S., ChenC.L.P. Image encryption using P-Fibonacci transform and decomposition. *Optics Communications*, Vol. 285, Iss. 5, 2012. - pp. 594-608.

УДК 003.26:004.056.55:621.39(045)

В. Баранник, Д. Гаврилов, М. Пархоменко, С. Шульгин, В. Ерошенко Возможность применения метода арифметического кодирования В системах криптографической защиты информации

Аннотация. *В статье проведен анализ последних публикаций, который указал на стремительное создание данных различными типами носителей. Отмечено, что пятая часть созданных данных является критически важной и нуждается в защите. Для уменьшения объема данных предлагается использовать методы кодирования без построения таблицы кодирования. Именно поэтому, подробно рассмотрены методы арифметического и адаптивного арифметического кодирования с позиции возможности применения в системах криптографической защиты информации для систем критической инфраструктуры. В результате исследования для гарантированной защиты информации предлагается использовать технологию последовательной криптографической защиты информации (после кодирования) с применением адаптивного арифметического кодирования. Для систем с потоковой обработкой данных (технология селективной защиты информации) предлагается применять арифметическое кодирование. Под ключевой информацией в алгоритме арифметического кодирования понимаем вес каждого элемента, остальная информация дополнительной защиты не нуждается.*

Ключевые слова: *защита информации, арифметическое кодирование, адаптивное арифметическое кодирование, Большие Данные (Big Date).*

Barannik V., Parkhomenko M., Shulgin S., Havrylov D., Yroshenko V. The possibility of using the arithmetic coding method in the systems of cryptographic information protection

Abstract. *The article analyzes recent publications, which pointed to the rapid creation of data by various types of media. It was noted that a fifth of the data generated is critical and needs to be protected. To reduce the amount of data, it is proposed to use coding methods without building a coding table. That is why, the methods of arithmetic and adaptive arithmetic coding are considered in detail from the standpoint of the possibility of using them in cryptographic information protection systems for critical infrastructure systems. As a result of the study, for guaranteed information protection, it is proposed to use the technology of sequential cryptographic information protection (after coding) using adaptive arithmetic coding. For systems with streaming data processing (selective information protection technology), it is proposed to use arithmetic coding. By key information in the arithmetic coding algorithm we mean the weight of each element, the rest of the information does not need additional protection.*

Keywords: *information protection, arithmetic coding, adaptive arithmetic coding, Big Data.*

Бараннік Володимир Вікторович, д.техн.,наук, професор, професор кафедри штучного інтелекту і програмування, Харківського національного університету імені В.Н. Каразіна.
Баранник Владимир Викторович, д.техн.наук, профессор, профессор кафедры искусственного интеллекта и программирования, Харьковского национального университета имени В.Н. Каразина.
Volodymyr Barannik, Doctor of Technical Sciences, Professor, Professor Department, V.N. Karazin Kharkiv National University.

Гаврілов Дмитро Сергійович, аспірант, Харківського національного університету радіоелектроніки.
Гаврилов Дмитрий Сергеевич, аспирант, Харьковского национального университета радиоэлектроники.
Havrilov Dmitry, PhD student, Kharkov National University of Radio Electronics.

Шульгін Сергій Сергійович, докторант Харківського національного університету радіоелектроніки.
Шульгин Сергей Сергеевич, докторант Харьковского национального университета радиоэлектроники.
Shulgin Sergii, associate professor, Doctoral Student in Kharkov National University of Radio Electronics.

Пархоменко Максим Вікторович, викладач Харківського національного університету Повітряних Сил імені І. Кожедуба.
Пархоменко Максим Викторович, преподаватель Харьковского национального университета Воздушных Сил имени И. Кожедуба.
Parkhomenko Maksym, Combat use of ASC department, Ivan Kozhedub Kharkiv National Air Force University.

Ерошенко Валерій Петрович, викладач Харківського національного університету Повітряних Сил імені І.Кожедуба.
Ерошенко Валерий Петрович, преподаватель Харьковского национального университета Воздушных Сил имени И.Кожедуба.
Yeroshenko Valerii, associate professor, Ivan Kozhedub Kharkiv National Air Force University.

Отримано *13 листопада 2020 року*, затверджено редколегією *15 грудня 2020 року*