# ЗАСТОСУВАННЯ АЛГОРИТМУ RSA В ДРОБОВО-РАЦІОНАЛЬНИХ N-АРНИХ ФОРМАХ ПРИ ШИФРУВАННІ-ДЕШИФРУВАННІ МОНОХРОМНИХ ЗОБРАЖЕНЬ

*Ковальчук А.М., старший викладач,*
*Кустра Н.О.,канд.техн.наук, доцент,*
*Яцишин С.П., д.т.н., професор,*
*Національний університет «Львівська політехніка», Україна*
*e-mail:* akm0519@gmail.com

## Анотація

Основним базисом для захисту зображення є припущення, що зображення – це стохастичний сигнал. Але зображення є специфічним сигналом, який володіє, в додаток до типової інформативності (інформативності даних), ще й візуальною інформативністю, що привносить в питання захисту нові задачі.

Тому актуальною задачею є реалізація такого використання алгоритму RSA, що при шифруванні зображення:

– не погіршилася криптографічна стійкість алгоритму RSA;

– досягти повної зашумленості зображення для запобігання використанню методів візуальної обробки зображень.

Запропоновано алгоритм шифрування-дешифрування монохромних зображень з використанням елементів алгоритму RSA, як найбільш стійкого до несанкціонованого дешифрування сигналів, у дробово-раціональних формах порядку $n$. Запропонований алгоритм застосовано до зображень, в яких наявні строго виокремлені контури. Елементи алгоритму RSA використовуються для побудови коефіцієнтів дробово-раціональних афінних перетворень. Розроблений алгоритм має вищу криптографічну стійкість у порівнянні з алгоритмом RSA. Описано можливості використання елементів алгоритму RSA в афінних перетвореннях при шифруванні – дешифруванні зображень.

Наведено результати моделювання шифрування для криптографічних перетворень монохромних зображень заданої розмірності. Розроблено модифіковані моделі та алгоритмічні процедури процесів формування ключів, прямого та оберненого криптографічних перетворень, що зводяться до математичних поелементних операцій.

## Ключові слова

Шифрування, монохромне зображення, дробово-раціональне афінне перетворення, контур, дешифрування.

## Вступ

Необхідність вирішення теоретичних і практичних завдань інформаційної безпеки та досягнення необхідного рівня захисту інформації різного змісту зумовила в епоху інформаційних технологій та масових комунікацій і відповідний прискорений розвиток криптографії**.**

Зображення можна визначити як двовимірну функцію $f(x, y)$, де $x$ і $y$ - координати в просторі (конкретно, на площині). Значення $f(x, y)$ в будь-якій точці називається інтенсивністю або рівнем сірого в цій точці. Якщо величини $x$, $y$ і $f(x, y)$ приймають скінченне число дискретних значень, то кажуть про цифрове зображення. Цифровою обробкою зображень називають обробку цифрових зображень за допомогою комп'ютерів. Відмітимо, що цифрове зображення складається зі скінченного числа елементів, кожен з яких розташований в конкретному місці і набуває певного значення. Ці елементи називаються елементами зображення або пікселями.

Математично цифрове зображення відображається матрицею розмірності $n$ на $m$ інтенсивностей пікселів, де $n$ – число рядків зображення, $m$ – число стобців.

Найбільш поширеним і стійким алгоритмом шифрування інформації є алгоритм RSA [1, 2], який відноситься до найбільш вживаних алгоритмів з відкритим ключем. Безпека алгоритму RSA базується

на ресурсно затратній факторизації великих натуральних чисел. Використання алгоритму RSA [1, 2], як найбільш стійкого до несанкціонованого дешифрування, стосовно зображень, у яких строго виокремлені контури, не дає задовільних результатів. На зашифрованому зображенні можливо розрізнити основні контури вхідного зображення - має місце ефект неповного зашумлення.

Виокремлення контуру означає пошук максимумів модуля вектора градієнта [2, 3]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування в RSA базується на піднесенні до степеню по модулю деякого натурального числа.

Наявність в зображенні контурів є важливою характеристикою зображення. Задача виокремлення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають величини рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [4, 5].

При цьому, на контурі і на сусідніх до контуру пікселях піднесення до степеню значення яскравостей дає ще більший розрив [8-17].

По відношенню до зображення існують певні проблеми його шифрування, а саме частково зберігаються контури на різко флуктуаційних зображеннях.

Надалі будемо використовувати наступне означення афінного перетворення евклідового простору в декартових координатах: перетворення евклідового простору називається афінним, якщо це перетворення відображає кожну площину на площину.

## Недоліки

Експериментами [6, 7] встановлено, що в області контурів на зображенні при шифруванні можуть створюватися значні відхилення значень інтенсивностей пікселів, що унеможливлює розмивання цих контурів при деяких значеннях вибраних простих чисел.

## Мета роботи

Побудувати модифікацію алгоритму RSA, використовуючи дробово-раціональні афінні перетворення та різні елементи алгоритму RSA, для отримання повного візуального розмиття контурів зображення.

## 1. Методика шифрування

Елементами алгоритму RSA називають прості числа $P$ і $Q$ та числа $e$ та $d$, отримані з конгруенції $ed \equiv 1 \pmod{\varphi(N)}$, $N = P * Q$, де $\varphi(N)$ – функція Ейлера.

Приймемо, що зображенню у відповідність ставиться матриця кольорів (матриця інтенсивностей пікселів) [**4, 6, 7**]

$$\mathbf{C}=\begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,m} \end{pmatrix}.$$

Дробово-раціональна $n$-арна форма перетворення евклідового простору в декартових координатах має вигляд:

$$y = \frac{Ax^n - B}{Cx^n - D}, \quad \text{де} \quad n > 0 \text{ - натуральне число} \qquad (1)$$

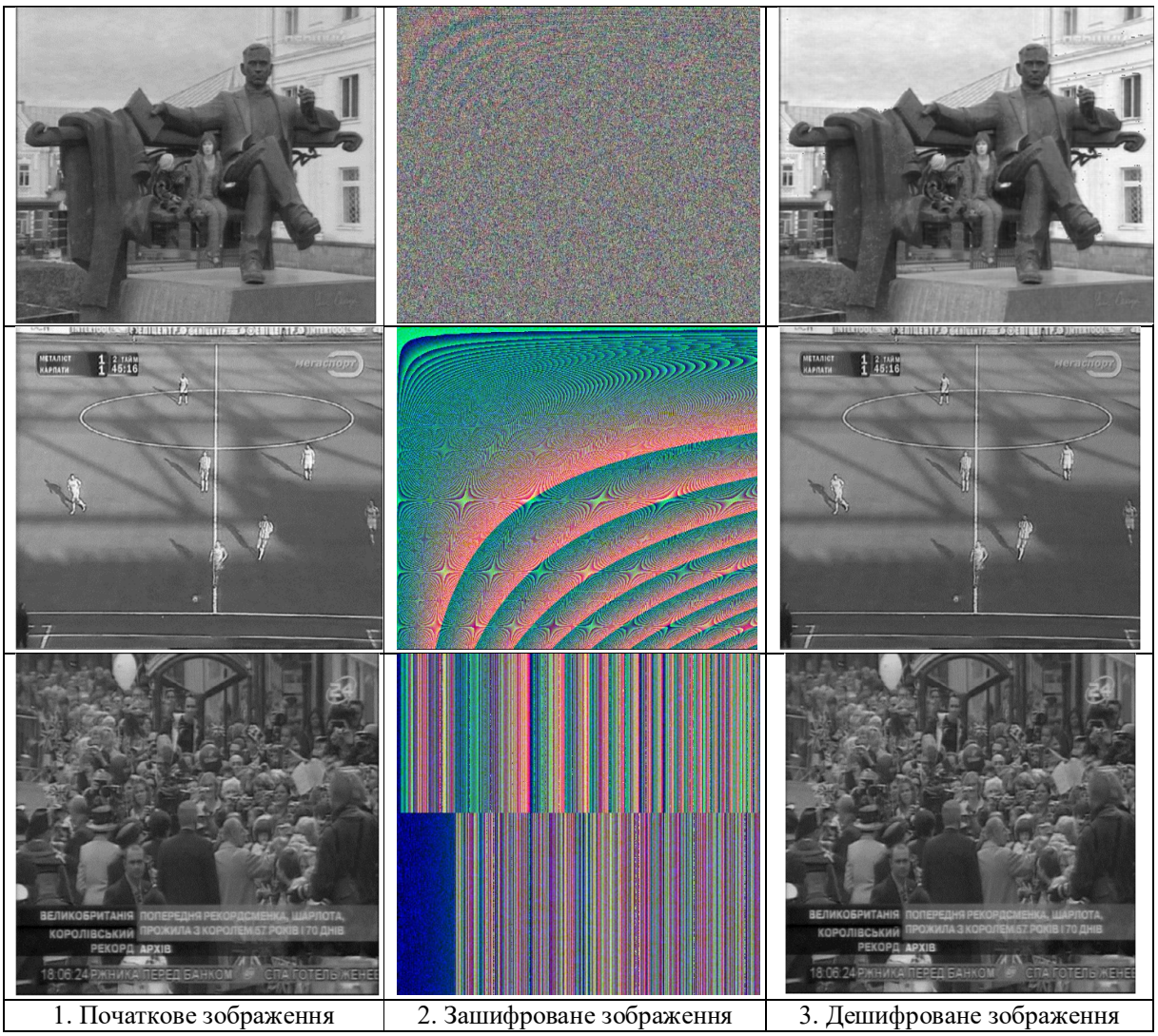
Відображення (1) переводить точки $x = \sqrt[n]{\frac{D}{C}}$ в точку $\infty$.

Обернене до (1) відображення має вигляд

$$x = \sqrt[n]{\frac{Dy - B}{Cy - A}} \quad , \qquad (2)$$

Обернене проективне відображення (2) переводить точку $y = \frac{A}{C}$ в точку ∞, тобто не є взаємно однозначним, якщо $A \neq D$. Це необхідно враховувати при шифруванні і дешифруванні для отримання достовірного дешифрованого зображення.

Шифрування відбувається поелементно за формулою (1), де $x = c_{i,j}$, $i = \overline{1,n}$, $j = \overline{1,m}$, $A = D = Q$, $B = P - Q$, $C = e - d$. Дешифрування проводиться по формулах оберненого перетворення (2) з тими ж коефіцієнтами $A = D = Q$, $B = P - Q$, $C = e - d$. Результати шифрування і дешифрування наведені на Рис.1 при $\boldsymbol{n} = 2$.




| 1. Початкове зображення | 2. Зашифроване зображення | 3. Дешифроване зображення |
|---|---|---|

Рис. 1. Результати шифрування

Запропонованим методом може бути зашифрована і текстова інформація, яка заздалегідь була приведена до графічного формату. Результати такого шифрування і дешифрування з використанням описаного методу шифрування наведені при $\boldsymbol{n} = 2$ на Рис.2 – 3.

## РОЗДІЛ 3

## Підвищення стійкості алгоритму RSA афінними перетвореннями

### 3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

#### 3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й $a$. При додатньому $a$ форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де $A, B, C, D$ - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел $x$ , $y$ відповідає пара цілих чисел $u$ і $v$, то кожне ціле число, подане формою $f$, подається формою $g$, і навпаки. В такому випадку говорять, що $f$ і $g$ еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Рис. 2. Початкове зображення.

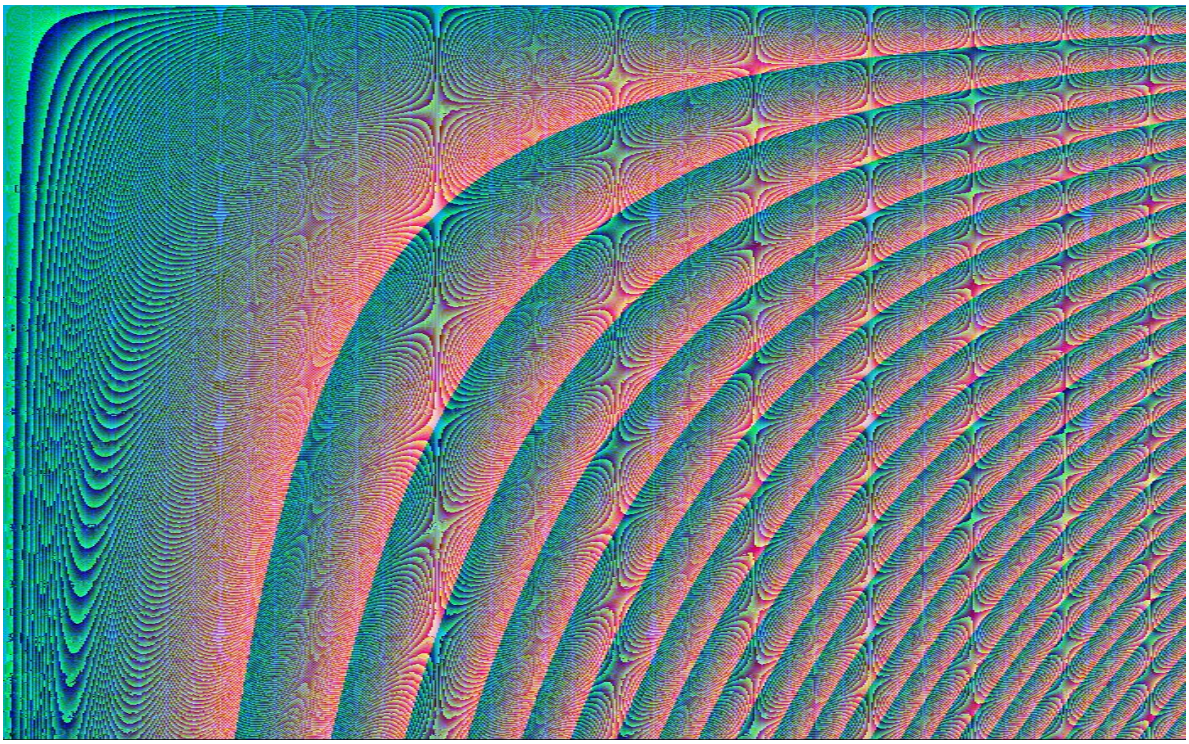
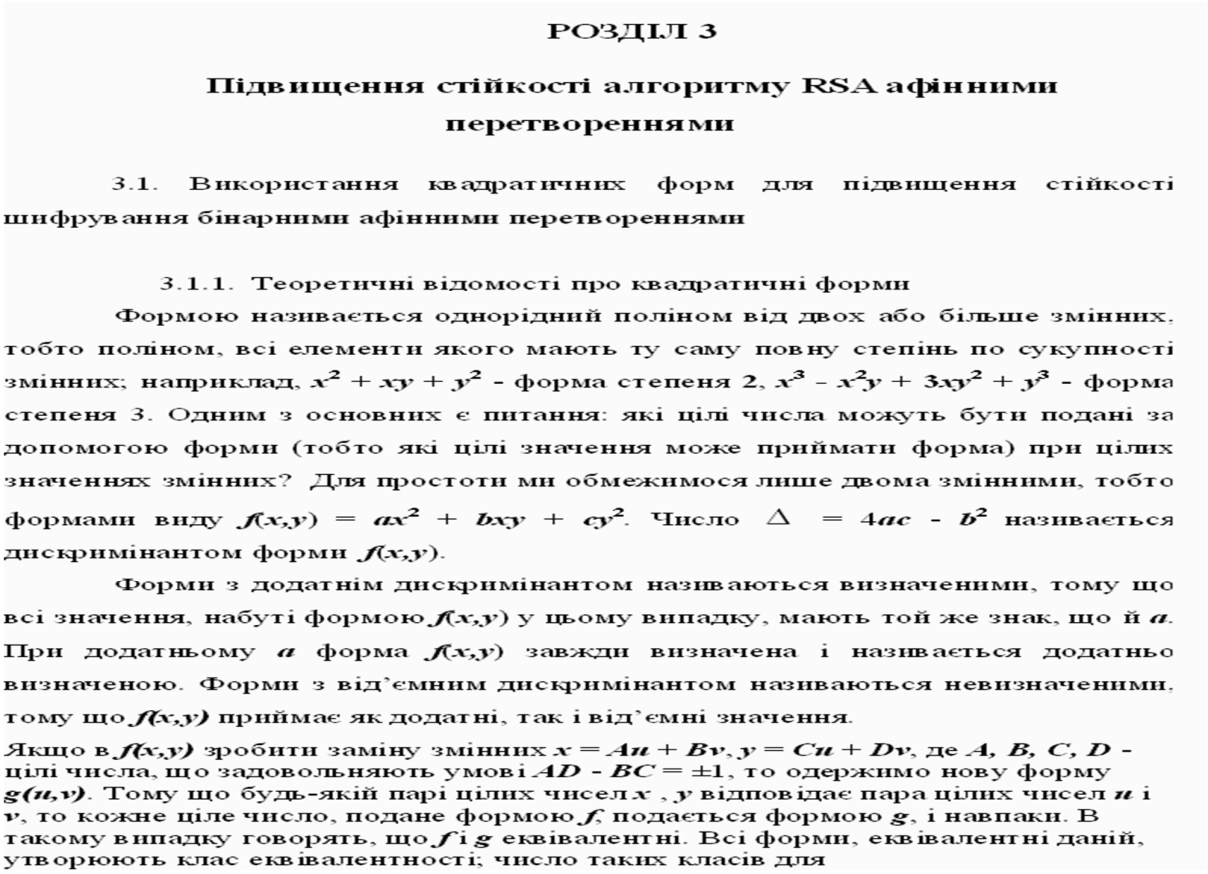


Рис. 3. Зашифроване зображення.



РОЗДІЛ 3

Підвищення стійкості алгоритму RSA афінними перетвореннями

3.1. Використання квадратичних форм для підвищення стійкості шифрування бінарними афінними перетвореннями

3.1.1. Теоретичні відомості про квадратичні форми

Формою називається однорідний поліном від двох або більше змінних, тобто поліном, всі елементи якого мають ту саму повну степінь по сукупності змінних; наприклад, $x^2 + xy + y^2$ - форма степеня 2, $x^3 - x^2y + 3xy^2 + y^3$ - форма степеня 3. Одним з основних є питання: які цілі числа можуть бути подані за допомогою форми (тобто які цілі значення може приймати форма) при цілих значеннях змінних? Для простоти ми обмежимося лише двома змінними, тобто формами виду $f(x,y) = ax^2 + bxy + cy^2$. Число $\Delta = 4ac - b^2$ називається дискримінантом форми $f(x,y)$.

Форми з додатнім дискримінантом називаються визначеними, тому що всі значення, набуті формою $f(x,y)$ у цьому випадку, мають той же знак, що й $a$. При додатньому $a$ форма $f(x,y)$ завжди визначена і називається додатньо визначеною. Форми з від'ємним дискримінантом називаються невизначеними, тому що $f(x,y)$ приймає як додатні, так і від'ємні значення.

Якщо в $f(x,y)$ зробити заміну змінних $x = Au + Bv$, $y = Cu + Dv$, де $A, B, C, D$ - цілі числа, що задовольняють умові $AD - BC = \pm 1$, то одержимо нову форму $g(u,v)$. Тому що будь-якій парі цілих чисел $x$ , $y$ відповідає пара цілих чисел $u$ і $v$, то кожне ціле число, подане формою $f$, подається формою $g$, і навпаки. В такому випадку говорять, що $f$ і $g$ еквівалентні. Всі форми, еквівалентні даній, утворюють клас еквівалентності; число таких класів для

Рис. 4. Дешифроване зображення.

З візуального порівняння зашифрованих зображень видно, що шифрування по матриці зображення при $n = 2$ відрізняються. Контури в обох зашифрованих зображеннях відсутні. Запропоновані модифікації застосовні до будь-якого типу зображень, але найбільші переваги досягаються у випадку використання зображень з чітко виокремленими контурами. Вказаний алгоритм може бути використаний при передачі закодованих графічних зображень.

Також візуально відрізняються незначно вхідні і дешифровані зображення. Тобто використання запропонованого алгоритму не погіршує якості зображення. Але за ситуації існування певних вимог і критеріїв якості, зазвичай необхідне певне число спроб підбору таких простих чисел $P$ і $Q$ та чисел $e$ і $d$ у конгруенції $ed \equiv 1 \pmod{\varphi(N)}$, $N = P * Q$ , щоб заданих критеріїв досягнення якості вхідного і дешифрованого зображення досягнути.

**Висновок**

На підставі числових експериментів з різними монохромними зображеннями при шифруванні та дешифруванні за допомогою описаного алгоритму встановлено, що запропонована модифікація має перевагу – підвищує криптографічну стійкість алгоритму RSA .

Описану модифікацію без жодних застережень можна використати і стосовно кольорових зображень. Однак, незалежно від типу зображення, зростає і розмір шифрованого зображення пропорційно до розміру вхідного зображення,.

## Література

[1] B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*, M.: Triumf, 2003, 815c. https://www.amazon.com/Applied-Cryptography-Protocols-Algorithms-Source/dp

[2] B. Jane. *Digital Image Processing*. Springer–Verlag Berlin Heidelberg, 2005, pp.583, https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp/3540592989

[3] R.C. Gonzales and R.E. Woods. *Digital image processing.* Prentice Hall, Upper Saddle River, NJ, 2ndedn,2002. https://www.amazon.com/Digital-Image-Processing-Algorithms-Applications/dp

[4] Tsmots I., Riznyk O., Rabyk V., Kynash Y., Kustra N., Logoida M. (2020) Implementation of FPGA-Based Barker's-Like Codes. In: Lytvynenko V., Babichev S., Wójcik W., Vynokurova O., Vyshemyrskaya S.,Radetskaya S. (eds) "*Lecture Notes in Computational Intelligence and Decision Making*". ISDMCI 2019. Advances in Intelligent Systems and Computing, vol 1020. Springer, Cham.
doi: 10.1007/978-3-030-26474-1_15.

[5] Rafael C. Gonzalez, Richard E. Woods, "*Digital Image Processing*", published by Pearson Education,Inc,Publishing as Prentice Hall, 2002, http://sdeuoc.ac.in /sites/default /files/sde_videos /Digital%20Image%20Processing%203rd%20ed.%20-%20R.%20Gonzalez%2C%20R.%20Woods-ilovepdf-compressed.pdf

[6] A. Kovalchuk, I. Izonin, C. Strauss, M. Podavalkina, N. Lotoshynska, N. Kustra. "*Image encryption and decryption schemes using linear and quadratic fractal algorithms and their systems*", CEUR Workshop Proceedings, Vol. 2533, 2019, pp. 139-150. https://doi.org/10.23939/istcmtm2020.04.025

[7] A. Kovalchuk, I. Izonin, Gregush Ml, M., N. Lotoshyiiska, "*An approach towards image encryption and decryption using quaternary fractional-linear operations*", Procedia Computer Science, Vol. 160, 2019, pp. 491-496. Conference Paper (Open Access), DOI > 10.1016 /j.procs. 2019.11.059.

[8] B. Girod "*The information theoretical significance of spatial and temporal masking in video signals*", Proc. of the SPIE Symposium on Electronic Imaging.1989.–Vol. 1077.– P.178–187, https://typeset.io/papers/the-information-theoretical-significance-of-spatial-and-2bas6i0mgw.

[9] Majid Rabbani, Rajan Joshi. "*An overview of the JPEG2000 still image compression standard*" , Eastman Kodak Company, Rochester, NY 14650, USA, Signal Processing: Image Communication. – 2002. – Vol. 17. – P. 3–48, https://scirp.org/reference/referencespapers.aspx?referenceid=727652

[10] S. X. Liao and M. Pawlak *On image analysis by moments* , IEEE Transaction on Pattern Analysis and Machine Intelligence. – 1996. – 18, No 3. – P. 254–266, https://ieeexplore.ieee.org/document/485554

[11] E.M. Haacke, R.W. Brown, M.R. Thompson and R. Vencatesan. *Magnetic Resonanse Imagin: Physical Principles and Sequence Design.* John Wiley & Sons, New York, 1999, https://www.wiley.com/ensg/Magnetic+Resonance+Imaging:+Physical+Principles+and+Sequence+Design,+2nd+Edition-p-9780471720850

[12] J.T. Kajiya. The rendering equation. *Computer Graphics,* 20: 143-150, 1986, https://dl.acm.org/doi/10.1145/15886.15902

[13] M. Sarfraz. *Introductory Chapter: On Digital Image Processing*. 2020, DOI: 10.5772 intechopen.92060, https://www.intechopen.com/chapters/71817

[14] Ehsan Samei, Donald J Peck, Projection X-ray Imaging, Hendee's Physics of Medical Imaging, 10.1002 9781118671016, (217-242), (2019), https://onlinelibrary.wiley.com/doi/10.1002/9781118671016.ch6

[15] Michael Vollmer, Klaus-Peter Mollmann, Fundamentals of Infrared Thermal Imaging, Infrared Thermal Imaging, 10.1002 9783527693306, (1-106), (2017), https://www.wiley.com/enus/Infrared+Thermal+Imaging:+Fundamentals,+Research+and+Applications,+2nd+Edition-p-9783527413515

[16] Usmonov, B., Evsutin, O., Iskhakov, A., Shelupanov, A., Iskhakova, A., & Meshcheryakov, R. (2017, November). The cybersecurity in development of IoT embedded technologies. In 2017 International Conference on Information Science and Communications Technologies (ICISCT) IEEE, pp. 1-4. DOI: 10.1109/ICISCT.2017.8188589.

[17] Wagh, D. P., Fadewar, H. S., & Shinde, G. N. (2020). Biometric Finger Vein Recognition Methods for Authentication. In Computing in Engineering and Technology pp. 45-53. DOI: 10.1007/978-981-32-9515-5_5.