УДК 004.032 DOI: 10.30748/soi.2019.156.12

В.Г. Красиленко[1], Д.В. Нікітович[1], Р.О. Яцковська[2], В.І. Яцковський[2]

[1] *Вінницький національний технічний університет, Вінниця*
[2] *Вінницький національний аграрний університет, Вінниця*

# МОДЕЛЮВАННЯ ПОКРАЩЕНИХ БАГАТОКРОКОВИХ 2D RSA АЛГОРИТМІВ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ТА СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

*Розглядаються нові модифікації криптосистеми RSA на 2D випадок, а саме, покращені багатокрокові моделі та алгоритми для криптографічних перетворень (КП) зображень і текстово-графічних документів (ТГД), що враховують їх специфіку та адаптуються до різних форматів. Наведені формули та алгоритмічні кроки процедур КП зображень чи матричних масивів. Модельними експериментами у програмному середовищі Mathcad продемонстровані функціональні можливості та переваги таких покращених багатокрокових 2D RSA моделей, сліпих електронних цифрових підписів та систем на їх основі для КП.*

***Ключові слова:*** *криптографічні перетворення, система 2D RSA, матричні багатокрокові моделі, зашифрування, розшифрування, моделювання, електронний підпис, алгоритм, тексто-графічний документ.*

## Вступ

За декілька останніх десятиріч суттєво зросла доля задач, в яких необхідно виконувати криптографічні перетворення (КП) над багатовимірними сигналами, серед яких важливе місце займають різноманітні кольорові зображення та 2D масиви, текстографічні документи (ТГД) конфіденційного характеру. А це призвело і до суттєвого зростання долі робіт, що присвячені зашифруванню та розшифруванню зображень, специфіка яких враховується при їх КП. Поява серед великого різноманіття криптографічних алгоритмів і протоколів, що використовуються в криптографії [1–11], робіт, присвячених методам та моделям, алгоритмам, орієнтованим на матричні спеціалізовані засоби [12–13], сприяла активізації досліджень у цьому напрямку [14–19]. З урахуванням збільшення сфер застосувань КП, вимог до них, в тому числі до їх ефективності, криптостійкості, актуальним завданням є покращення характеристик існуючих методів і засобів КП.

**Аналіз останніх досліджень і публікацій.** Вперше матричні моделі (ММ) були запропоновані в [12], а модифікації системи RSA на матричний випадок у [13], які пізніше були використані і для створення електронних цифрових підписів (ЕЦП) для любих ТГД: сліпих ЕЦП на основі матричних афінних шифрів [15], ЕЦП матричного типу на базі модифікацій алгоритму RSA і Ель-Гамаля на 2D випадок [16], де були продемонстровані їх можливості та переваги і введено підклас ММ матричного типу (МТ) або 2D. Але в [13; 16] наводилися результати моделювання таких ММ лише для невеликих (128×128 ел.) масивів чорно-білих зображень.

**Постановка проблеми.** Тому **метою даної роботи** є подальше вдосконалення, дослідження ММ, в тому числі і нових модифікацій 2D RSA для КП зображень (З), ТГД, для створення на їх основі ЕЦП МТ, шляхом моделювання вдосконалених ММ КП у Mathcad на конкретних З, ТГД та демонстрації цих процесів, їх криптограм, ЕЦП на їх основі. Перевірка їх функціональних можливостей і переваг дозволить оцінити характеристики, особливості застосувань вдосконалених багатокрокових ММ 2D RSA.

## Виклад основного матеріалу

Ідея узагальнення на 2D випадок класичного скалярного RSA та похідних від нього алгоритмів [13; 16; 20] полягає у виборі в якості ключів не скалярів, а відповідних матриць KEY(E) та KEY(D). Для цього вибираються таких два простих числа $k$ та $l$ або дві матриці $K$ та $L$ з елементами попарно простих чисел $k\_i,j$ та $l\_i,j$ , таких щоб їх добуток $n\_i,j$ трохи перевищував значення елемента масиву, що підлягає зашифруванню, наприклад, для З представлений байтом або трьома байтами кольорового формату. Ключі формуються як матриці, кожен елемент яких вибирається з множини значень відповідних скалярних ключів $e\_i,j$ та $d\_i,j$, тобто значення елементів KEY(E)$\_i,j$ та KEY(D)$\_i,j$ матричних ключів KEY(E) та KEY(D) вибираються з множини взаємно простих чисел, що задається відповідною функцією Ейлера від $n\_i,j$, яка і визначає потужність цієї множини. У загальному випадку 2D масив елементів $n\_i,j$ є матрицею різних чи однакових простих чисел, а потужність множини ключів залежить як від потужності множини допустимих значень для кожного елемента так і від кількості елементів у масиві, що забезпечує прийнятні високі для неї значення вже при практично застосовуваних розмірностях З.

Відомо, що не існує жодного ефективного алгоритму розв'язування задачі обчислення дискрет-

ного логарифма за модулем, а тому **розширення** та ускладнення задачі на 2D випадок, особливо за рахунок **збільшення потужностей множин** матричних ключів та матриць-модулів є першим фактором ускладнення розв'язування вище вказаної задачі. Для ще більшого її ускладнення ми пропонуємо так званий **багатокроковий алгоритм**, для якого базову процедуру (у RSA MT) поелементно-матричного піднесення у степінь за відповідними модулями (ПЕМПуСМ), описану в [13; 16], треба **повторити певну кількість разів**, як стороні першій так і другій з узгодженими приватними та публічними ключами. Таке повторення процедур ПЕМПуСМ сторонами з утворюваними черговими на попередніх кроках новими CMD (чи TV) покращує стійкість КП [20]. Але, як показали деякі модельні експерименти [16; 20], для специфічних видів З, ТГД, що містять фрагменти з рівними значеннями яскравості елементів, після процедур ПЕМПуСМ у криптограмах залишаються форми та види цих фрагментів.

Тому ми пропонуємо **додатково закривати** З публічним ключем KEY(E) 2-ї сторони перед процедурою ПЕМПуСМ першою стороною (зашифрування) та додатково відкривати цим же ключем після зворотної процедури ПЕМПуСМ другою стороною (розшифрування). Елементи криптограми CMD для явної матриці $T$ (чи закритої її версії) у RSA MT, обчислюються першою стороною при використанні публічного ключа KEYPD 2-ї сторони (його елементів $e\_i,j$) процедурою ПЕМПуСМ за формулою: $CMD\_i,j \equiv T\_i,j\hat{}\ e\_i,j \bmod n\_i,j$. Утворену і надіслану CMD 2 сторона аналогічною процедурою розшифровує, використовуючи свій приватний ключ OKEYD, обчислюючи $TV\_i,j \equiv CMD\_i,j\hat{}d\_i,j \bmod n\_i,j$ чи ще й розкриває, якщо $T$ було закрито. Це значно поліпшує якість та гістограмно-ентропійні характеристики таких покращених багатокрокових 2D RSA, як буде продемонстровано нижче.

На рис. 1–3 показані результати моделювання процесів КП на основі багатокрокового 2D RSA алгоритму. В одному з експериментів явний ТГД формату А4 (704×572 ел.), представлений матрицею ARD, коригувався до матриці ARDK, як і в [13], закривався та зашифровувався публічним для 2-ї сторони МК KEYPD (вибрану $m$ кількість разів), отримана 2-ю стороною криптограма CMD розшифровувалася приватним МК OKEYD ($m$ разів), а потім утворений DCMD розкривався публічним ключем KEYPD (формули на рис. 1). На рис. 2 показано вигляд З, ТГД: явних, зашифрованих, розшифрованих, що підтверджують адекватність ММ. Результати КП одного з кольорових З багатокроковим 2D RSA показані на рис. 3. Ентропія $R$, $G$, $B$ складових криптограми досягала 7,97–7,98 біт (майже 8!). Питання узгодження МК загального завадоподібного типу розглядались у попередніх роботах [17–18], були започатковані в [21], і тому тут їх не наводимо.


Рис. 1. Формули, що використовувались для моделювання 2D RSA алгоритму

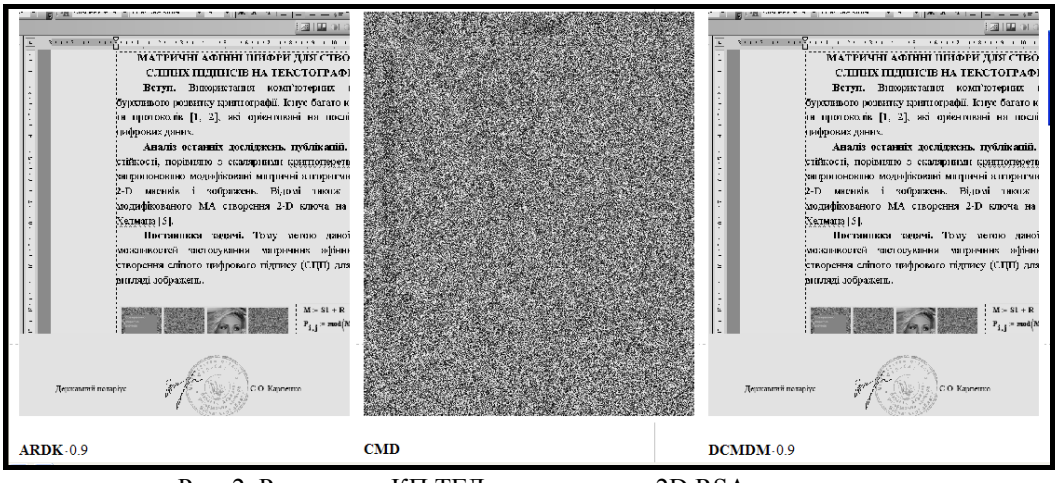


Рис. 2. Результати КП ТГД за допомогою 2D RSA алгоритму:
скоригований ТГД, криптограма CMD та розшифрований розкритий ТГД

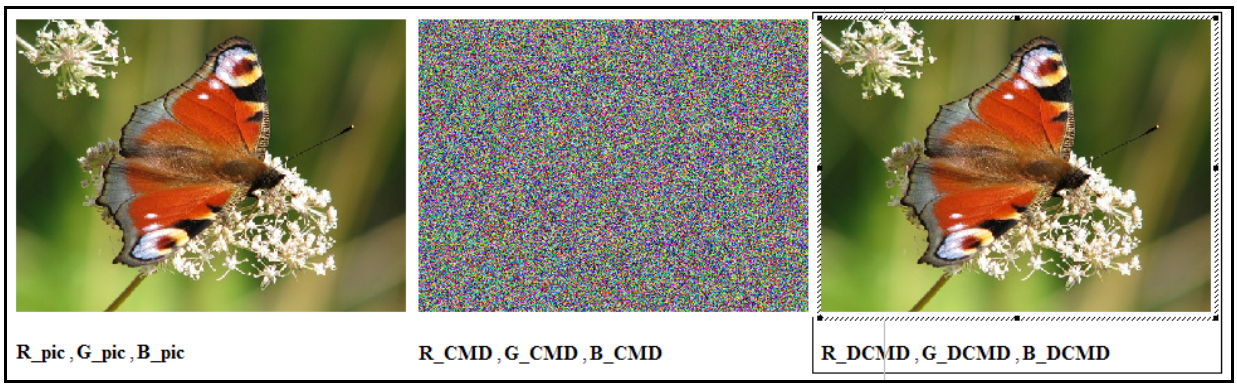


Рис. 3. Результати КП кольорового З за допомогою 2D RSA: явне З, його криптограма, розшифроване З

Розглянемо застосування багатокрокових процедур по-елементно-матричних піднесень у степінь за 2D-модулями, що базуються на основі запропонованих тут багатокрокових покращених 2D RSA МТ для створення сліпих електронних цифрових підписів (С_ЕЦП) 2D типу, використовуючи для цього узгоджені публічні та приватні МК (зображення), вибрані та створені у відповідності до описаних у попередніх роботах [17–18] процедур. Результати моделювання у Mathcad та дослідження процесів створення вдосконалених С_ЕЦП 2D типу, на основі багатокрокових ММ RSA алгоритмів показані на рис. 4–9.

Якщо для зображення (З), рис. 5, результати допустимі, то, як видно з рис. 6–8, для деяких ТГД є неприпустимим неякісне "закриття", тому нами запропоновано покращити С_ЕЦП уведенням додаткового адитивного закриття публічним МК, про що було вказано вище при розгляді пропозицій щодо вдосконалень базового 2D_RSA. Для цього був розроблений модуль, що показаний на рис. 8, а отримані з ним кращі результати показані на рис. 9.

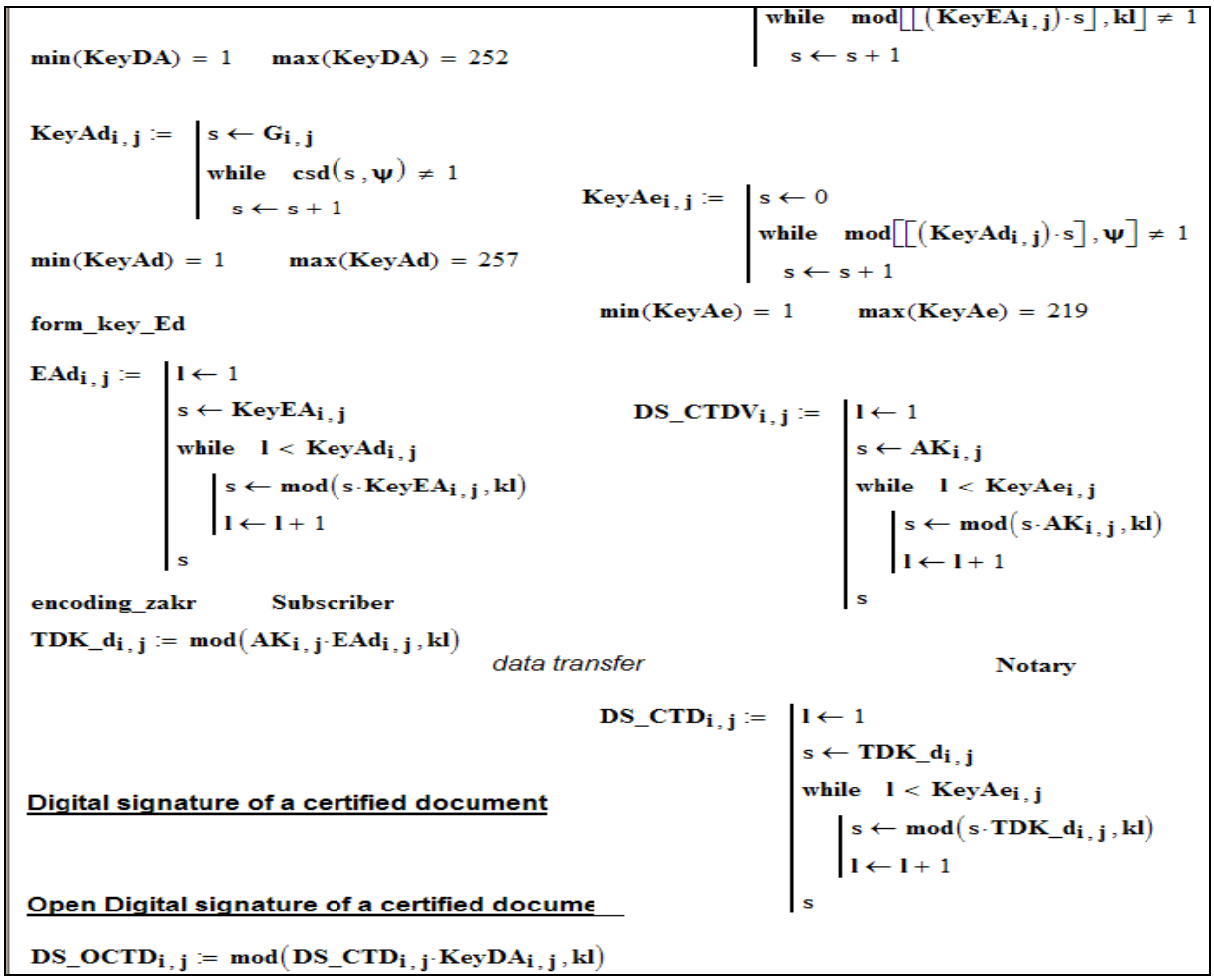


Рис. 4. Програмний модуль (вікно Mathcad), що використовувались для моделювання С_ЕЦП 2D типу на основі RSA алгоритму

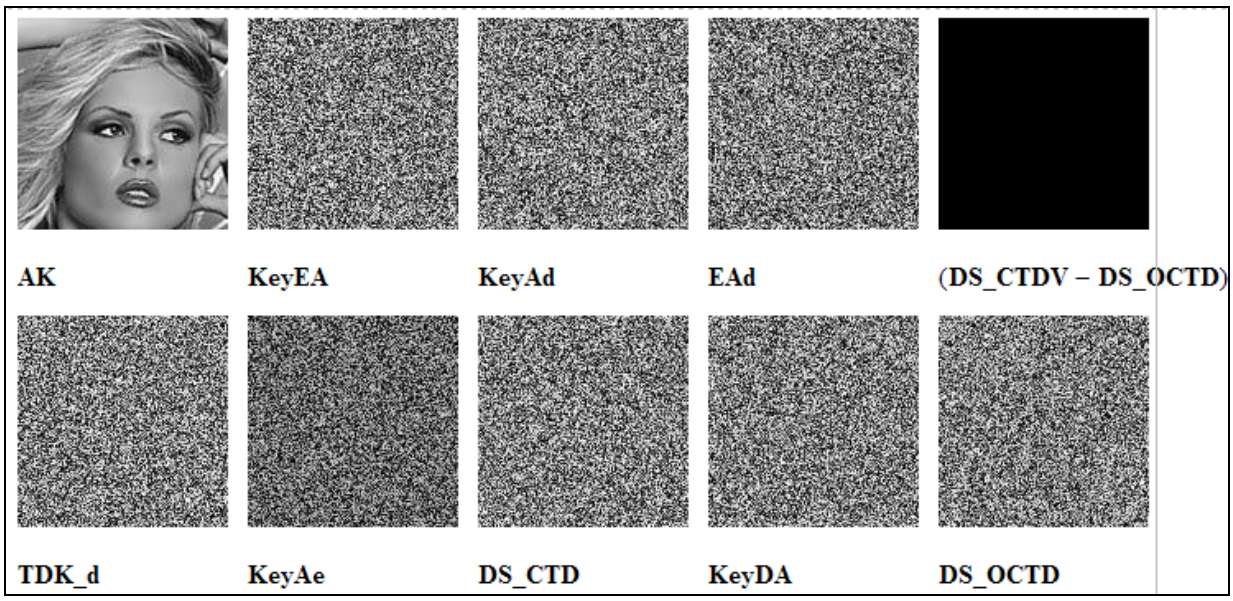


Рис. 5. Результати моделювання процесів створення та верифікації С_ЕЦП 2D типу RSA. У верхньому ряду зліва направо: З для підпису, МК KeyEA для закриття З, публічний МК KeyAd нотаріуса, створений ним МК EAd матричним піднесенням KeyEA у степінь за модулем, різницеве З для верифікації; у нижньому: закрите МК EAd З у виді TDK_*d*, що підписує нотаріус, його приватний МК KeyAe, закритий С_ЕЦП (DS_CTD), МК KeyDA (обернений до KeyEA), розкритий цим МК підписаний С_ЕЦП (DS_OCTD)

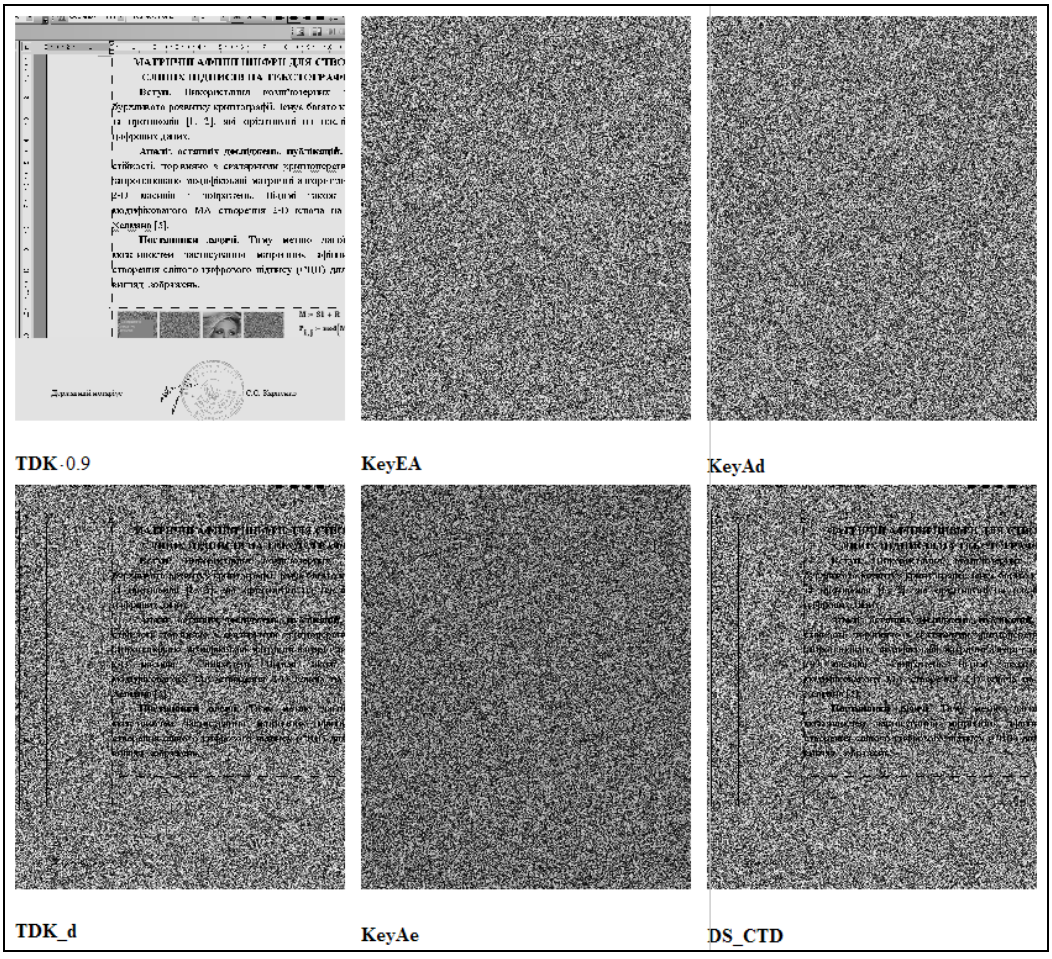


Рис. 6. Результати моделювання процесів створення та верифікації С_ЕЦП 2D типу RSA для ТГД, що підтверджують недостатність закриття. У верхньому ряду зліва направо: скоригований ТГД для підпису, МК KeyEA для закриття ТГД, публічний МК KeyAd нотаріуса; у нижньому: закритий ТГД у виді TDK_*d*, що підписує нотаріус, його приватний МК KeyAe, закритий С_ЕЦП (DS_CTD)

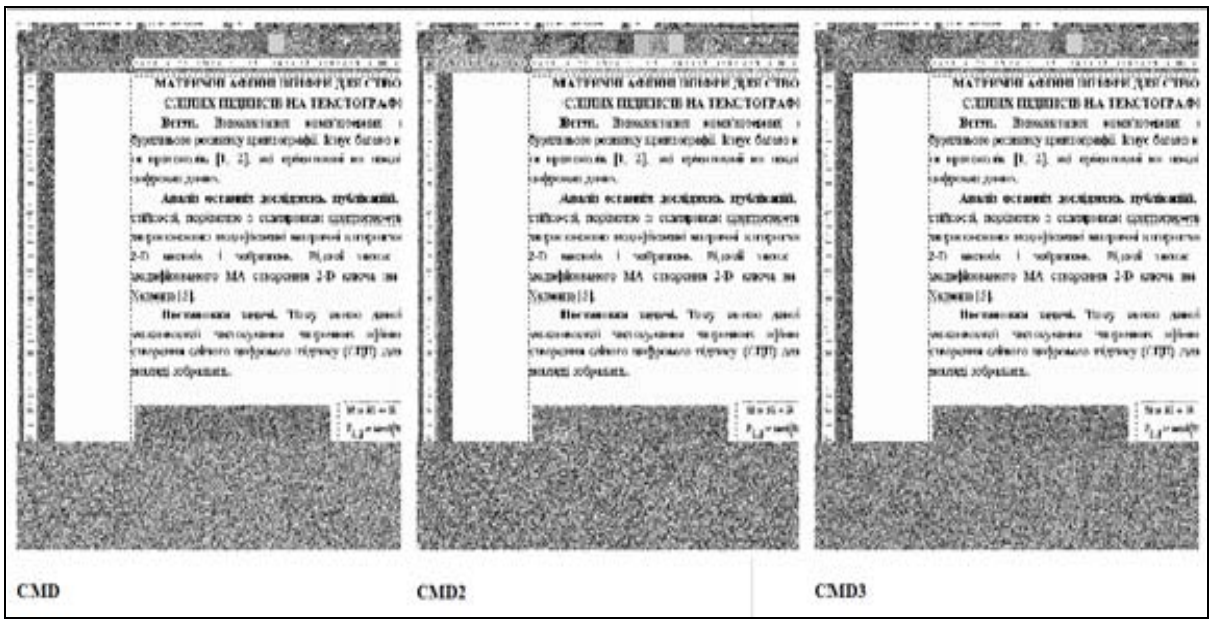


Рис. 7. Вигляд зашифрованих ТГД (ЕЦП) багатокроковим 2D RSA, відповідно: після 1-го (CMD), 2-го (CMD2) та 3-го (CMD3) кроків при використанні тільки приватного ключа. Висновок: проста багатокроковість і для ТГД (ЕЦП) не допомагає без адитивного закриття

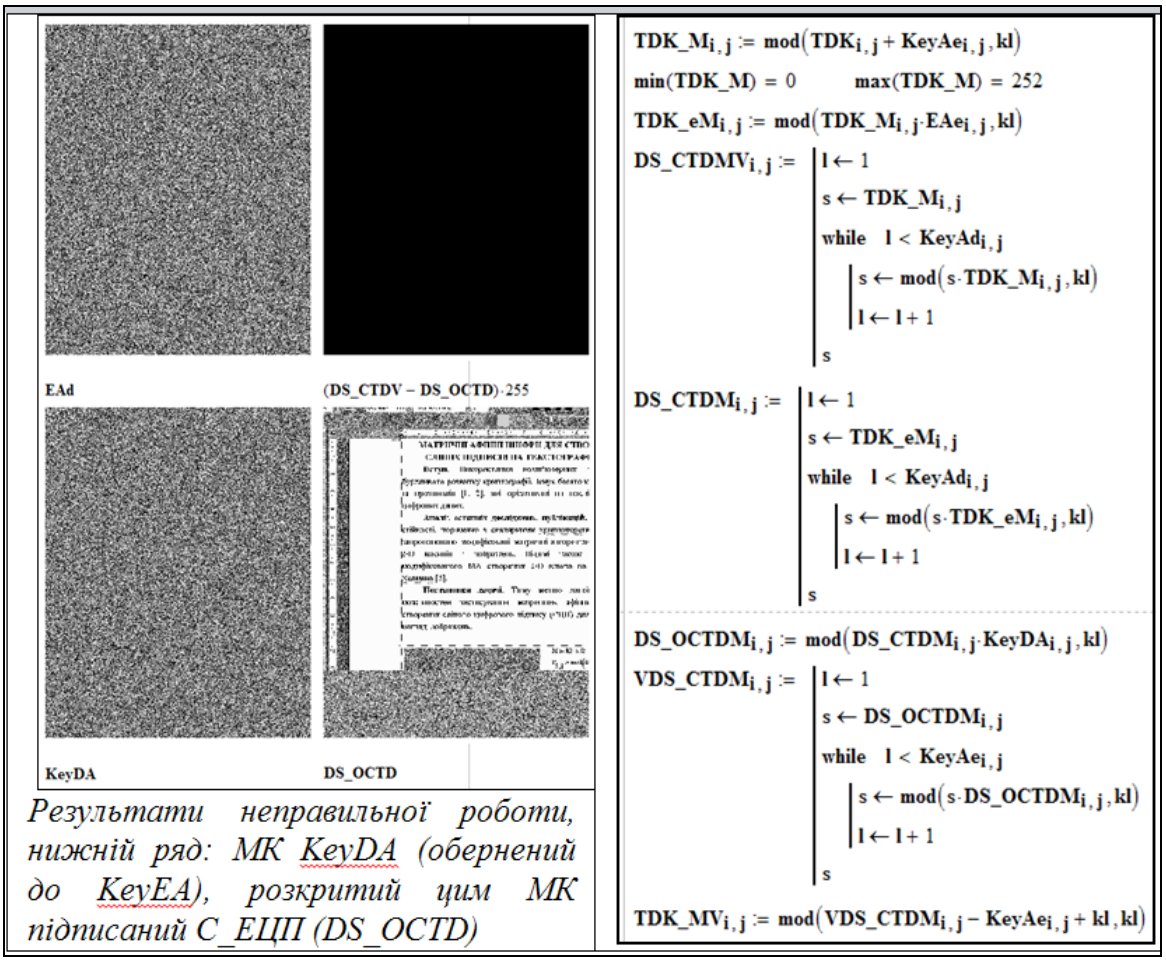


Рис. 8. Результати (ліворуч) моделювання С_ЕЦП для ТГД про недостатність закриття та додатково введений програмний модуль (вікно Mathcad, праворуч) для вдосконалення і моделювання покращеного С_ЕЦП 2D типу на основі 2D_RSA

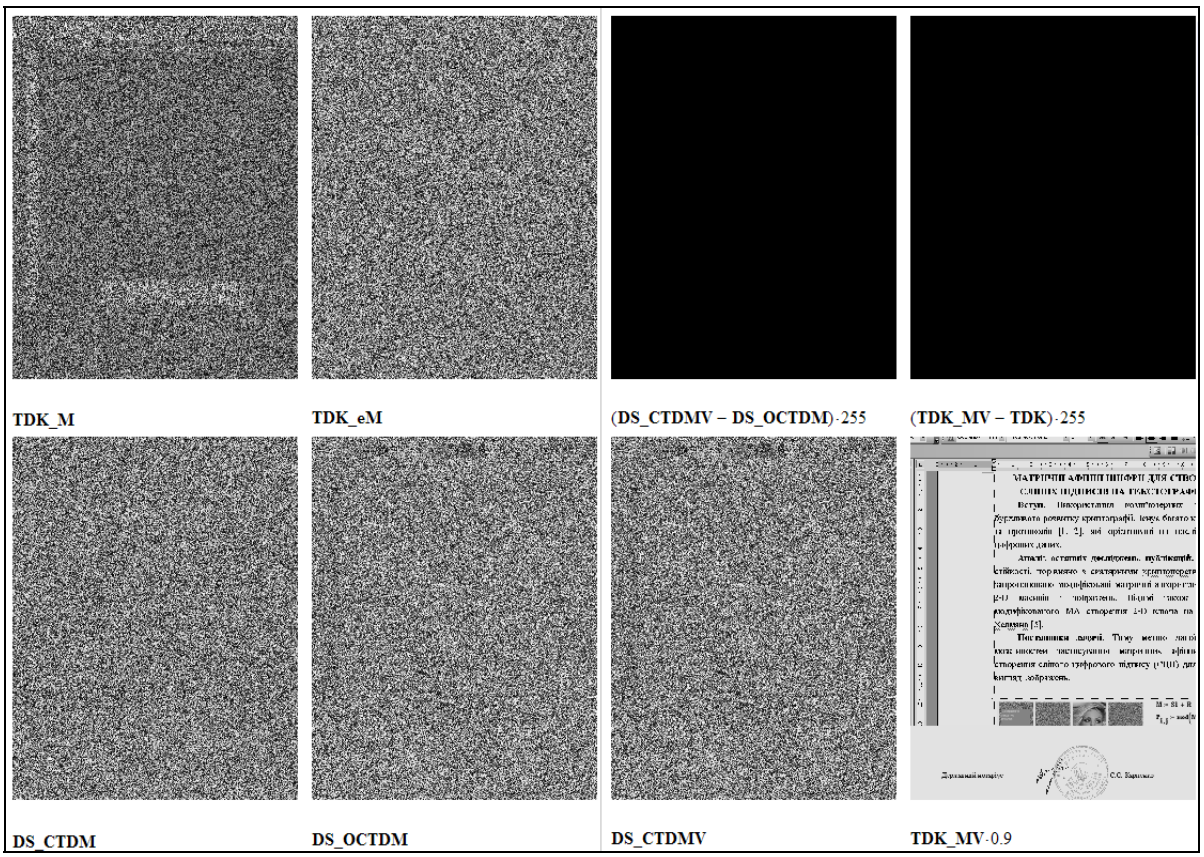


Рис. 9. Матриці-зображення, що формувалися в модельних експериментах та підтверджують правильну роботу процесів створення та верифікації **покращеного** С_ЕЦП 2D типу RSA. У верхньому ряду зліва направо: скоригований для підпису ТГД та зашифрований публічним МК KeyAe (TDK_M), закритий МК KeyEA (TDK_eM), верифікаційні різницеві; у нижньому: закритий С_ЕЦП (DS_CTDM), розкритий підписаний С_ЕЦП (DS_OCTDM), перевірені підписи

Як видно з наведених результатів моделювання у середовищі Mathcad, конкретних демонстрацій функціональних можливостей та переваг запропонованих покращених моделей та алгоритмів створення сліпих ЕЦП для конфіденційних документів, для великоформатних документів, підтверджено експериментально адекватність, правильність функціонування матричних моделей, їх верифікації, та досягнення значних покращень. Покращені С_ЕЦП враховують специфіку ТГД, адаптуються до різних форматів, мають кращі часові, гістограмно-ентропійні характеристики (виміряні розробленим програмним модулем ентропії явних та закритих ТГД, зображень з їх низки показали збільшення ентропії С_ЕЦП до 7,98–7,99 біт/ел. навіть для явних, що мали низькі значення ентропії, на порядок!).

## Висновки

Запропоновані, промодельовані багатокрокові 2D_RSA моделі та алгоритми КП зображень та текстово-графічних документів (ТГД), що враховують їх специфіку, адаптуються до різних форматів. Низкою експериментів показані недоліки базових моделей, показано, що для деяких зображень, особливо для ТГД зі значними фрагментами подібних за рівнем інтенсивності пікселів є недостатність надійного закриття (приховування) навіть багатокроковими 2D_RSA моделями, а тому останні потребують подальших удосконалень і це стало причиною визначення шляхів нових модифікацій з метою покращення їх характеристик. В роботі показано, що удосконалені багатокрокові 2D_RSA моделі та алгоритми КП можуть бути використані також для створення на їх основі більш вдосконалених, з кращими характеристиками, сліпих цифрових електронних підписів матричного типу. Наведені формули, описані алгоритмічні кроки процедур КП покращеними багатокроковими 2D_RSA, в тому числі при створенні на їх основі ЕЦП. Розробленим програмним модулем визначені ентропії інформаційних об’єктів на всіх процедурних кроках перетворень та проведено ентропійний та гістограм ний аналіз, який разом з низкою демонстрацій результатів модельних експериментів у Mathcad з різноманітними напівтоновими та кольоровими специфічними зображеннями підтвердили адекватність, функціональні можливості та переваги таких покращених 2D_RSA моделей, крипто-алгоритмів та систем на їх основі.

## Список літератури

1. Хорошко В.О. Методи та засоби захисту інформації / В.О. Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

2. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.: іл.

3**.** Коркішко Т. Алгоритми та процесори симметричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів: БаК, 2003. – 168 с.

4. Лужецький В. Методи шифрування на основі перестановки блоків змінної довжини / В. Лужецький, І. Горбенко // Захист інформації. – 2015. – Т. 17, № 2. – С. 169-175.

5. Білецький А.Я. Матричні аналоги протоколу Діффі-Хеллмана / А.Я. Білецький, А.А. Білецький, Р.Ю. Кандиба // Автоматика, вимірювання та керування: Вісник нац. ун-ту "Львівська політехніка". – 2012. – № 741. – С. 128-133.

6. Грицюк Ю.І. Математичні основи процесу генерування ключів переставляння з використанням шифру Кардано / Ю.І. Грицюк, П.Ю. Грицюк // Науковий вісник НЛТУ України. – 2015. – Вип. 25.10. – С. 311-323.

7. Грицюк Ю.І. Методи і засоби генерування QP-матриць Фібоначчі-ключів для реалізації криптографічних перетворень / Ю.І. Грицюк, П.Ю. Грицюк // Науковий вісник НЛТУ України. – 2015. – Вип. 25.6. – С. 334-351.

8. Белецкий А.Я. Модифицированный матричный асимметричный криптографический алгоритм Диффи – Хэллмана / А.Я. Белецкий, А.А. Белецкий, Д.А. Стеценко // Штучний інтелект. – 2010. – № 3. – С. 697-705.

9. Дудикевич В.Б. Крипто-кодовий захист інформації з недвійковим рівно ваговим кодуванням / В.Б. Дудикевич, О.О. Кузнєцов, Б.П. Томашевський // Сучасний захист інформації. – 2010. – № 2. – С. 14-23.

10. Kutter M. Digital Signature Of Color Images Using Amplitude Modulation / M. Kutter, F. Jordan, F. Bossen // Proc. of the SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.

11. Квєтний Р.Н. Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECC та RSA / Р.Н. Квєтний, Є.О. Титарчук, А.А. Гуржій // Інформаційні технології та комп'ютерна інженерія. – 2016. – № 3. – С. 38-43.

12. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Фламвицька // Вісн. нац. ун-ту "Львів. політехнік". – 2009. – № 658. – С. 59-63.

13. Красиленко В.Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2012 . – № 8(106). – С. 102-106.

14. Красиленко В.Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 3(101). – С. 53-61.

15. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60-63.

16. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 3(110). – Т. 2. – С. 18-22.

17. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – Х.: ХУПС, 2017. – Вип. 3(149). – С 151-157. https://doi.org/10.30748/soi.2017.149.30.

18. Красиленко В.Г. Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: Луцький національний технічний університет, 2017. – Вип. 26. – С 111-120.

19. Красиленко В.Г. Удосконалення та моделювання матричних афінних шифрів для криптографічних перетворень зображень / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2017. – Вип. 7. – С. 20-42.

20. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції "Інформаційні управляючі системи та технології" (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: ВидавІнформ НУ "ОМА", 2017. – С. 312 -318.

21. Красиленко В.Г. Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання / В.Г. Красиленко, В.І. Яцковський, Р.О. Яцковська // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 8(106). – С. 107-110.

## References

1. Khoroshko, V.O. and Chetkov, A.O. (2003), "*Metody ta zasoby zakhystu informatsii*" [*Methods and means of information protection*], Junior, Kyiv, 502 p.

2. Yemets, V., Melnyk, A. and Popovych, R. (2003), "*Suchasna kryptohrafiia: Osnovni poniattia*" [*Modern Cryptography: Basic Concepts*], BaK, Lviv, 144 p.

3. Korkishko, T., Melnyk, A. and Melnyk, V. (2003), "*Alhorytmy ta protsesory symetrychnoho blokovoho shyfruvannia*" [*Algorithms and processors of symmetric block encryption*], BaK, Lviv, 168 p.

4. Luzhetskyi, V. and Horbenko, I. (2015), "Metody shyfruvannia na osnovi perestanovky blokiv zminnoi dovzhyny" [Encryption methods based on permutation of variable length blocks], *Protection of information*, Vol. 17, No. 2, pp. 169-175.

5. Biletskyi, A.Ia., Biletskyi, A.A. and Kandyba, R.Iu. (2012), "Matrychni analohy protokolu Diffi-Khellmana" [Matrix analogues of the Diffie-Hellman protocol], *Automation, Measurement and Control: Bulletin of the National University Lviv Polytechnic University*, No. 741, pp. 128-133.

6. Hrytsiuk, Yu.I. and Hrytsiuk, P.Iu. (2015), "Matematychni osnovy protsesu heneruvannia kliuchiv perestavliannia z vykorystanniam shyfru Kardano" [Mathematical bases of the process of generating repositioning keys using Cardan cipher], *Scientific herald of NLTU of Ukraine*, Vol. 25.10, pp. 311-323.

7. Hrytsiuk, Yu.I. and Hrytsiuk, P.Iu. (2015), "Metody i zasoby heneruvannia QP-matryts Fibonachchi-kliuchiv dlia realizatsii kryptohrafichnykh peretvoren" [Methods and tools for generating QP matrices Fibonacci-keys for implementing cryptographic transformations], *Scientific herald of NLTU of Ukraine*, Vol. 25.6, pp. 334-351.

8. Beletskyi, A.Ia., Beletskyi, A.A. and Stetsenko, D.A. (2010), "Modyfikovanyy asymetrychnyy kryptohrafichnyy alhorytm Diffi-Khelmana" [Modified Diffie-Hellman Matrix Asymmetric Cryptographic Algorithm], *Artificial Intelligence*, No. 3, pp. 697-705.

9. Dudykevych, V.B., Kuznietsov, O.O. and Tomashevskyi, B.P. (2010), "Krypto-kodovyi zakhyst informatsii z nedviikovym rivno vahovym koduvanniam" [Crypto-code protection of information with non-binary equally weight encoding], *Modern information protection*, No. 2, pp. 14-23.

10. Kutter, M., Jordan, F. and Bossen, F. (1997), Digital Signature Of Color Images Using Amplitude Modulation, *Proc. of the SPIE Storage and Retrieval for Image and Video Databases*, Vol. 3022, pp. 518-526.

11. Kvietnyi, R.N., Tytarchuk, Ye.O. and Hurzhii, A.A. (2016), "Metod ta alhorytm obminu kliuchamy sered hrup korystuvachiv na osnovi asymetrychnykh shyfriv ECC ta RSA" [Method and algorithm for key exchange among user groups based on asymmetric ECC and RSA ciphers], *Information Technology and Computer Engineering*, No. 3, pp. 38-43.

12. Krasilenko, V.G. and Flavitskaya, Yu.A. (2009), "Modeliuvannia matrychnykh alhorytmiv kryptohrafichnoho zakhystu" [Modeling of Matrix Cryptographic Protection Algorithms], *Herald of the National University Lviv Polytechnic University*, No. 658, pp. 59-63.

13. Krasilenko, V.G. and Grabovlyak, S.K., (2012), "Modyfikatsii systemy RSA dlia stvorennia na yii osnovi matrychnykh modelei ta alhorytmiv dlia zashyfruvannia ta rozshyfruvannia zobrazhen" [Modifications of the RSA system for creating on its basis matrix models and algorithms for encrypting and decrypting images], *Information Processing Systems*, No. 8 (106), pp.102-106.

14. Krasilenko, V.G. and Grabovliak, S.K. (2012), "Matrychni afinno-perestanovochni alhorytmy dlia shyfruvannia ta deshyfruvannia zobrazhen" [Matrix affine and permutational algorithms for encryption and decryption of images], *Information Processing Systems*, No. 3(101), pp. 53-61.

15. Krasilenko, V.G. and Grabovliak, S.K. (2011), "Matrychni afinni shyfry dlia stvorennia tsyfrovykh slipykh pidpysiv na tekstohrafichni dokumenty", [Matrix Affinity Ciphers to Create Digital Blind Signatures for Textual Documents], *Information Processing Systems*, No. 7 (97), pp. 60-63.

16. Krasilenko, V.G., Yatskovska, R.O. and Trifonova, Yu.M. (2013), "Demonstratsiia protsesiv stvorennia slipykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu do-kumentatsiiu na osnovi modelei matrychnoho typu" [Demonstration of processes for creation of blind electronic digital signatures on text-graphic documentation based on matrix-type models], *Information Processing Systems*, No. 3 (110), pp. 18-22.

17. Krasilenko, V.G. and Nikitovich, D.V. (2017), "Modeliuvannia protokoliv uzghodzhennia sekretnoho matrychnoho kliucha dlia kryptohrafichnykh peretvoren ta system matrychnoho typu", [Simulation of the protocols for reconciling the secret matrix key for cryptographic transformations and matrix-type systems], *Information Processing Systems*, No. 3(149), pp. 151-157. https://doi.org/10.30748/soi.2017.149.30.

18. Krasilenko, V.G. and Nikitovich, D.V. (2017), "Modeliuvannia bahatokrokovykh ta bahatostupenevykh protokoliv uzghodzhennia sekretnykh matrychnykh kliuchiv" [Modeling of multi-step and multi-protocol protocols for the harmonization of secret matrix keys], *Komp'iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo: naukovyi zhurnal*, No. 26, Lutskyi natsionalnyi tekhnichnyi universytet, Lutsk, pp. 111-120.

19. Krasilenko, V.G. and Nikitovich, D.V. (2017), "Udoskonalennia ta modeliuvannia matrychnykh afinnykh shyfriv dlia kryptohrafichnykh peretvoren zobrazhen" [Improvement and simulation of matrix affine ciphers for cryptographic transformations], *Elektronika ta informatsiini tekhnolohii: zbirnyk naukovykh prats*, No. 7, Lvivskyi natsionalnyi universytet imeni Ivana Franka, Lviv, pp. 20-42.

20. Krasilenko, V.G. and Nikitovich, D.V. (2017), "Vdoskonalennia ta modeliuvannia elektronnykh tsyfrovykh pidpysiv matrychnoho typu dlia teksto-hrafichnykh dokumentiv" [Improvement and modeling of digital signature of matrix type for text-graphic documents], *Materialy VI mizhnarodnoi naukovo-praktychnoi konferentsii "Informatsiini upravliaiuchi systemy ta tekhnolohii" (IUST-Odesa-2017),* Odeskyi natsionalnyi morskyi universytet, Odesa, pp. 312-318.

21. Krasilenko, V.G., Yatskovsky, V.I. and Yatskovska, R.O. (2012), "Alhorytmy formuvannya dvovymirnykh klyuchiv dlya matrychnykh alhorytmiv kryptohrafichnykh peretvoren′ zobrazhen′ ta yikh modelyuvannya" [Algorithms for the formation of two-dimensional keys for matrix algorithms of cryptographic transformations of images and their modeling], *Information Processing Systems*, No. 8 (106), pp. 107-110.

*Надійшла до редколегії 30.01.2019*
*Схвалена до друку 19.02.2019*

***Відомості про авторів:***

**Красиленко Володимир Григорович**
кандидат технічних наук доцент
старший науковий співробітник
Вінницького національного технічного університету,
Вінниця, Україна
https://orcid.org/0000-0001-6528-3150

**Нікітович Діана Вікторівна**
диспетчер факультету
Вінницького національного технічного університету,
Вінниця, Україна
https://orcid.org/0000-0002-8907-1221

**Яцковська Римма Олександрівна**
асистент
Вінницького національного аграрного університету,
Вінниця, Україна
https://orcid.org/0000-0001-6093-8058

**Яцковський Віктор Іванович**
кандидат технічних наук
старший викладач
Вінницького національного аграрного університету,
Вінниця, Україна
https://orcid.org/0000-0002-3645-1140

***Відомості про авторів:***

**Vladimir Krasilenko**
Candidate of Technical Sciences Associate Professor
Senior Research of Vinnytsia National
Technical University,
Vinnytsia, Ukraine
https://orcid.org/0000-0001-6528-3150

**Diana Nikitovich**
Dispatcher of Faculty
of Vinnytsia National Technical University,
Vinnytsia, Ukraine
https://orcid.org/0000-0002-8907-1221

**Rymma Yatskovska**
Assistant Lecturer
of Vinnitsa National Agrarian University,
Vinnitsa, Ukraine
https://orcid.org/0000-0001-6093-8058

**Viktor Yatskovskyi**
Candidate of Technical Sciences
Senior Instructor
of Vinnitsa National Agrarian University,
Vinnitsa, Ukraine
https://orcid.org/0000-0002-3645-1140

## МОДЕЛИРОВАНИЕ УСОВЕРШЕНСТВОВАННЫХ МНОГОШАГОВЫХ 2D RSA АЛГОРИТМОВ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ И СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В.Г. Красиленко, Д.В. Никитович, Р.А. Яцковская, В.И. Яцковский

*Рассматриваются новые модификации криптосистемы RSA на 2D случай, а именно, улучшенные многошаговые модели и алгоритмы для криптографических преобразований (КП) изображений и тексто-графических документов (ТВД), учитывающие их специфику и адаптирующиеся к различным форматам. Приводятся формулы и алгоритмические шаги процедур КП изображений или матричных массивов. Проведен гистограммно-энтропийный анализ. Экспериментами в программной среде Mathcad продемонстрированы функциональные возможности и преимущества таких улучшенных многошаговых 2D RSA моделей, слепых электронных цифровых подписей и систем на их основе для КП.*

***Ключевые слова:*** *криптографические преобразования, система 2D RSA, матричные многошаговые модели, шифрование, расшифровка, моделирование, электронная подпись, алгоритм, тексто-графический документ.*

## MODELING OF IMPROVED MULTI-STAGE 2D RSA ALGORITHM FOR CRYPTOGRAPHIC TRANSFORMATIONS AND BLIND ELECTRON DIGITAL SIGNATURE

V. Krasilenko, D. Nikitovich, R. Yatskovska, V. Yatskovskyi

*We consider new modifications of the RSA cryptosystem for the 2D case, namely, improved multi-step models and algorithms for cryptographic transformations (CP) of images and text-graphic documents (TGD), taking into account their specifics and adapting to different formats. It is shown that for some special images for their better encryption additional procedures for their closure are needed, along with the multi-step cryptographic transformations. To this end, and to ensure operation with the same keys, it has been proposed to additionally close the document with the public key of the second party before the encryption procedure with the first party and additionally open it with the same key after the reverse decryption procedure by the second party. To test the proposed RSA modifications of the matrix type, a series of experiments was carried out using the Mathcad software environment. Formulas, program modules, their fragments corresponding to the algorithmic steps of the cryptographic transformation procedures, examples of explicit and transformed images, matrix arrays and their digital signatures are suggested. A histogram-entropy analysis was carried out, which showed a significant (by an order of magnitude!) increase in the entropy of cryptograms and digital signatures to 7.98 - 7.99 bits / pixel even for explicit text-graphic documents with low initial entropy. Experiments in the Mathcad software environment on a variety of examples of encryption of special halftone and color images and TGD demonstrated the functionality and advantages of such improved multi-step 2D RSA models, as well as blind electronic digital signatures and systems based on them.*

***Keywords:*** *cryptographic transformations, 2D RSA system, matrix multi-step models, encryption, decryption, simulation, electronic signature, algorithm, text and graphic document.*