УДК 004.056.55:003.26.09 DOI: 10.46972/2076-1546.2020.19.06

О. В. Самчишин, І. В. Гуменюк, К. В. Сметанін, О. С. Бойченко

МЕТОД ШИФРУВАННЯ / РОЗШИФРУВАННЯ ДАНИХ НА ОСНОВІ ПІКСЕЛЬНОГО АЛФАВІТУ МОНОХРОМНОГО ЗОБРАЖЕННЯ

Удосконалення доступності інформаційних технологій та зростання об'єму цифрового трафіка призводить до актуалізації проблеми захисту даних. Особливо значущою є проблема передачі конфіденційних даних незахищеними каналами зв'язку, наприклад, мережею Інтернет. Останнім часом спостерігається значне збільшення кількості кібератак, зокрема спроб перехоплення та крадіжки конфіденційної інформації. Її захист у комп'ютерних інформаційно-телекомунікаційних системах є пріоритетним завданням. На сьогоднішній день одним із найбільш надійних методів захисту інформації справедливо вважається шифрування. Криптографічні перетворення даних є найбільш ефективним засобом системи зберігати конфіденційність інформації в ході її введення, виведення, передачі, обробки та зберігання, а також протистояти її руйнуванню, розкраданню чи спотворенню. Але найефективнішим способом забезпечення захищеності інформації є суміщене використання стеганографічних і криптографічних засобів. З метою гарантування високої стійкості зашифрованої інформації під час передачі її каналами мережі інформаційно-телекомунікаційних систем та зниження рівня загрози несанкціонованого доступу до неї або атаки на шифр запропоновано змінити підхід щодо розв'язання задачі шифрування даних. Запропоновано метод шифрування / розшифрування цифрової текстової інформації на основі піксельного алфавіту монохромного зображення, який ґрунтується на приховуванні або деформації графічних даних. Такий підхід дозволяє забезпечити високу стійкість зашифрованої інформації та значно зменшити рівень загрози несанкціонованого доступу до неї або атаки на шифр за рахунок кодування кожного символу динамічним випадковим числом з діапазону його значень та приховування шифрованого тексту в позиції графічних даних з урахуванням таємного ключа, який відомий тільки відправнику та адресату.

Ключові слова: *шифрування / розшифрування даних; криптографічний алгоритм; цифрова стеганографія; інформаційно-телекомунікаційна система.*

Постановка проблеми в загальному вигляді. На сьогодні важливим чинником, що впливає на політичну й економічну складові національної безпеки, є ступінь захищеності інформації й інформаційного середовища. Особливо актуальною є проблема передачі конфіденційних даних незахищеними каналами зв'язку, наприклад, мережею Інтернет. Через стрімкий розвиток засобів обчислювальної техніки й відкритих мереж передачі даних виникає нагальна потреба в забезпеченні шифрування інформації в режимі реального часу. Хоча сьогодні застосовують багато алгоритмів шифрування, проте сучасні стандарти шифрування є досить повільними, оскільки передбачають велику кількість операцій [2]. Отже, виникає необхідність у розробці алгоритму шифрування, який міг би здійснювати це на порядок швидше. Найефективнішим способом забезпечення конфіденційності інформації є суміщене використання стеганографічних і криптографічних засобів.

Аналіз останніх досліджень і публікацій. Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації від несанкціонованого доступу. В останні роки з розвитком ІТ-індустрії кількість спроб отримати несанкціонований доступ до конфіденційної інформації збільшилася, а проблемами інформаційної безпеки зацікавилися багато вчених та фахівців різних країн [3, 4]. Це свідчить про те, що потреба в захисті конфіденційної інформації значно зросла.

З-поміж великої кількості різноманітних методів захисту від несанкціонованого доступу особливе місце займають криптографічні методи.

Аналіз останніх досліджень і публікацій показав, що найбільшу популярність у комп'ютерній стеганографії здобули підходи, що використовують у ролі контейнера зображення [6].

Найбільш близьким способом, який розглядається як аналог розробленого авторами методу, є шифрування та розшифрування цифрових даних, переданих або збережених з використанням методу передачі пріоритетних пікселів [1], за яким здійснюється кодування та декодування цифрових даних, переданих або збережених із використанням пріоритетного способу передачі пікселів інформаційного вмісту, що підлягає захисту. Кожна група пікселів містить значення позиції, що використовується як пріоритетне, йому присвоюється хоча б один ключ, за допомогою якого значення позиції пікселя або групи пікселів за запитом шифруються чи розшифровуються. Але цей спосіб не дозволяє забезпечити достатню криптостійкість та унеможливити успішну атаку на шифр за рахунок можливості визначення пріоритетності пікселів або значень їх позицій під час передачі зашифрованого повідомлення, а також має невисоку швидкодію шифрування та розшифрування цифрової текстової інформації за рахунок високої операційної складності алгоритму шифрування, який застосовується в ньому.

Формулювання завдання дослідження. З метою забезпечення високої стійкості зашифрованої інформації для передачі її каналами мережі інформаційно-телекомунікаційних систем (ІТС) та зниження рівня загрози несанкціонованого доступу до неї або атаки на шифр запропоновано змінити підхід щодо розв'язання задачі шифрування даних. Тому необхідно розробити метод шифрування цифрової текстової інформації, який ґрунтується на приховуванні або деформації графічних даних, який не мав би недоліків аналогу.

Виклад основного матеріалу. Терміни, які використовуються в запропонованому методі:

Повідомлення – вихідне текстове повідомлення;

Довжина – кількість символів Повідомлення;

Нормативний алфавіт – символи Повідомлення (літери української абетки, цифри 0–9, спеціальні та символи пунктуації), яке шифрується та передається каналами мережі ІТС;

Алфавіт шифрування – статичні діапазони значень яскравостей пікселів монохромного зображення (0–255), які присвоюються кожному символу Нормативного алфавіту;

Шифрування – процес заміни Нормативного алфавіту Повідомлення елементами Алфавіту шифрування;

Шифротекст – результат Шифрування;

Ключ – позиції із визначеним інтервалом розміщення пікселів на графічних даних з яскравістю, що відповідають Алфавіту шифрування;

Стегоповідомлення – результат приховування Шифротексту;

Відправник – користувач, який здійснює Шифрування Повідомлення та передачу Шифротексту;

Адресат – користувач, який отримує та розшифровує Шифротекст у Повідомлення;

Програма – комп'ютерна програма, яка здійснює Шифрування Повідомлення та розшифрування Шифротексту.

Поставлене завдання вирішується в такий спосіб: у методі шифрування / розшифрування даних на основі піксельного алфавіту монохромного зображення, за яким визначають Ключ, кожному елементу Нормативного алфавіту присвоюють статичний діапазон значень яскравості пікселів монохромного зображення. Формується Алфавіт шифрування, за яким здійснюється Шифрування Повідомлення та приховується Шифротекст у цифрове зображення шляхом його деформації, зокрема кодування значення яскравості пікселів, що відповідають Алфавіту шифрування, на позиції з визначеним Ключем. Після передачі Адресату та отримання Стегоповідомлення відбувається його розшифрування в Повідомлення з використанням Алфавіту шифрування за визначеним Ключем.

Такий підхід дозволяє забезпечити високу стійкість зашифрованої інформації та значно зменшити рівень загрози несанкціонованого доступу до неї або атаки на шифр за рахунок Шифрування кожного символу Повідомлення динамічним випадковим числом із діапазону значень відповідного символу. Значне зниження рівня загрози несанкціонованого доступу до інформації або атаки на шифр досягається за рахунок приховування Шифротексту в позиції графічних даних із урахуванням Ключа, який відомий Відправнику та Адресату.

Шифрування / розшифрування даних на основі піксельного алфавіту монохромного зображення проводиться за декілька етапів.

1. Формування Алфавіту шифрування, за яким кожному символу Нормативного алфавіту присвоюються статичний діапазон значень яскравостей пікселів монохромного зображення (0–255) для: літер української абетки; літер англійської абетки; цифр 0–9; спеціальних символів.

2. Перетворення Нормативного алфавіту Повідомлення в Шифротекст.

3. Формування Ключа (визначення початкового положення першого елемента Шифротексту та інтервалу наступних).

4. Формування Стегоповідомлення (приховування Шифротексту або деформація графічних даних значеннями Алфавіту шифрування в позиції, що визначені Ключем).

5. Передача (приймання) Стегоповідомлення.

6. Розшифрування Стегоповідомлення (визначення значень яскравостей пікселів у позиціях, заданих Ключем, перетворення їх у Нормативний алфавіт та формування Повідомлення).

Етап формування Алфавіту шифрування. Для множини всіх доступних символів, які використовуються в Повідомленні, задаються статичні діапазони значень, що знаходяться в межах $\left[000;255\right]$, а саме:

літер української абетки (табл. 1): $B_1 = \left\{b_{"а"}, b_{"б"}, .., b_{"я"}\right\}$, $B_1 \in \left[000;095\right]$;

літер англійської абетки (табл. 2): $B_2 = \{b_{"a"}, b_{"b"}, .., b_{"z"}\}$, $B_2 \in [096; 173]$;

цифр (табл. 3): $B_3 = \{b_{"0"}, b_{"1"}, .., b_{"9"}\}$, $B_3 \in [174; 203]$;

спеціальних символів (табл. 4): $B_4 = \{b_{"?"}, b_{"!"}, .., b_{"пробіл"}\}$, $B_4 \in [204; 255]$.

Таблиця 1

Алфавіт шифрування літер української абетки

Нормативний алфавіт	А (а)	Б (б)	В (в)	Г (г)	Д (д)	Е (е)	Є (є)	Ж (ж)
Алфавіт шифрування	000–002	003–005	006–008	009–011	012–014	015–017	018–020	021–023
Нормативний алфавіт	З (з)	И (и)	І (і)	Ї (ї)	Й (й)	К (к)	Л (л)	М (м)
Алфавіт шифрування	024–026	027–029	030–032	033–035	036–038	039–041	042–044	045–047
Нормативний алфавіт	Н (н)	О (о)	П (п)	Р (р)	С (с)	Т (т)	У (у)	Ф (ф)
Алфавіт шифрування	048–050	051–053	054–056	057–059	060–062	063–065	066–068	069–071
Нормативний алфавіт	Х (х)	Ц (ц)	Ч (ч)	Ш (ш)	Щ (щ)	Ь (ь)	Ю (ю)	Я (я)
Алфавіт шифрування	072–074	075–077	078–080	081–083	084–086	087–089	090–092	093–095

Таблиця 2

Алфавіт шифрування літер англійської абетки

Нормативний алфавіт	A (a)	B (b)	C (c)	D (d)	E (e)	F (f)	G (g)	H (h)	
Алфавіт шифрування	096–098	099–101	102–104	105–107	108–110	111–113	114–116	117–119	
Нормативний алфавіт	I (i)	J (j)	K (k)	L (l)	M (m)	N (n)	O (o)	P (p)	Q (q)
Алфавіт шифрування	120–122	123–125	126–128	129–131	132–134	135–137	138–140	141–143	144–146
Нормативний алфавіт	R (r)	S (s)	T (t)	U (u)	V (v)	W (w)	X (x)	Y (y)	Z (z)
Алфавіт шифрування	147–149	150–152	153–155	156–158	159–161	162–164	165–167	168–170	171–173

Таблиця 3

Алфавіт шифрування цифр

Нормативний алфавіт	0	1	2	3	4	5	6	7	8	9
Алфавіт шифрування	174–176	177–179	180–182	183–185	186–188	189–191	192–194	195–197	198–200	201–203

Таблиця 4

Алфавіт шифрування спеціальних символів

Нормативний алфавіт	?	!	.	,	%	=	+	/	:
Алфавіт шифрування	204–206	207–209	210–212	213–215	216–218	219–221	222–224	225–227	228–230
Нормативний алфавіт	;	'	\	_	<	>	(	)	Пробіл
Алфавіт шифрування	231–233	234–236	237–239	240–242	243–245	246–248	249–251	252–254	255

Особливість формування Алфавіту шифрування полягає в поданні його в тріадній (трицифровій) формі, при цьому кожен його елемент відповідає величині яскравості пікселя монохромного зображення, який приховуватиметься в (або деформовуватиме) графічні дані, зокрема растрове зображення RGB-моделі.

Етап перетворення Нормативного алфавіту Повідомлення у Шифротекст. Для кожного окремого Нормативного алфавіту

$$M = \{m_1, m_2, .., m_i\};\ i = \overline{1,n},$$

де n – Довжина Повідомлення, здійснюється заміна на випадкове значення із заданого йому діапазону Алфавіту шифрування. Наприклад, $b_{"a"} = [000; 002]$ (літера "А" української абетки може бути замінена числами: 000, 001 та 002), у результаті чого формується Шифротекст:

$$G = \{rand(b_m)_i\},$$

де $rand$ – функція генерування випадкових чисел.

Етап формування Ключа. Для Шифротексту обирається значення початкового положення першого його елемента $k_1(x, y)$, яке відповідає розташуванню першого пікселя монохромного зображення, та наступних з урахуванням визначених інтервалів (горизонтального – Δx, вертикального – Δy). У результаті цього формується Ключ Шифрування, розмірність якого повинна бути не менша Довжини Повідомлення:

$$K = \{k_i(x, y)\};\ 1 \le x \le (w-1),\ 1 \le y \le (h-1),$$

де w – ширина зображення;

h – його висота.

Формування Стегоповідомлення. Пікселі з яскравостями, які відповідають значенням сформованого Шифротексту, розміщуються в позиції (x_i, y_i), визначеній Ключем $K = \{k_i(x, y)\}$. У такій спосіб здійснюється приховування Шифротексту в графічні дані або деформація растрового зображення RGB-моделі.

Результатом цього етапу є Стегоповідомлення у вигляді $S = \{G, K\}$.

Етап передачі (приймання) Стегоповідомлення. Відправлення Відправником та приймання Адресатом Стегоповідомлення здійснюється з використанням наявних мережевих протоколів передачі даних. На цьому етапі визначається доступність Відправника та Адресата до мережі, формується таблиця маршрутизації, окреслюються маршрути з мінімальною вартістю з'єднання, за якими здійснюється безпосередня передача Стегоповідомлення.

Етап розшифрування Стегоповідомлення. За отриманим Стегоповідомленням $S = \{G, K\}$ Адресат із використанням відомого Ключа $K = \{k_i(x, y)\}$, переданого окремо альтернативними каналами зв'язку, визначає позиції пікселів (x_i, y_i), оцінює значення їх яскравостей, формує Шифротекст $G = \{(b_m)_i\}$, за заздалегідь відомим Алфавітом шифрування здійснює послідовне його перетворення в Нормативний алфавіт та Повідомлення:

$$M = \{(b_{m_1} \to m_1), (b_{m_2} \to m_2), .., (b_{m_i} \to m_i)\}.$$

Суть методу шифрування / розшифрування даних на основі піксельного алфавіту монохромного зображення пояснюється за допомогою ілюстрації (див. рис. 1–4), де показано один із можливих варіантів Шифрування Повідомлення (див. рис. 1, 2) та розшифрування Шифротексту (див. рис. 3, 4).

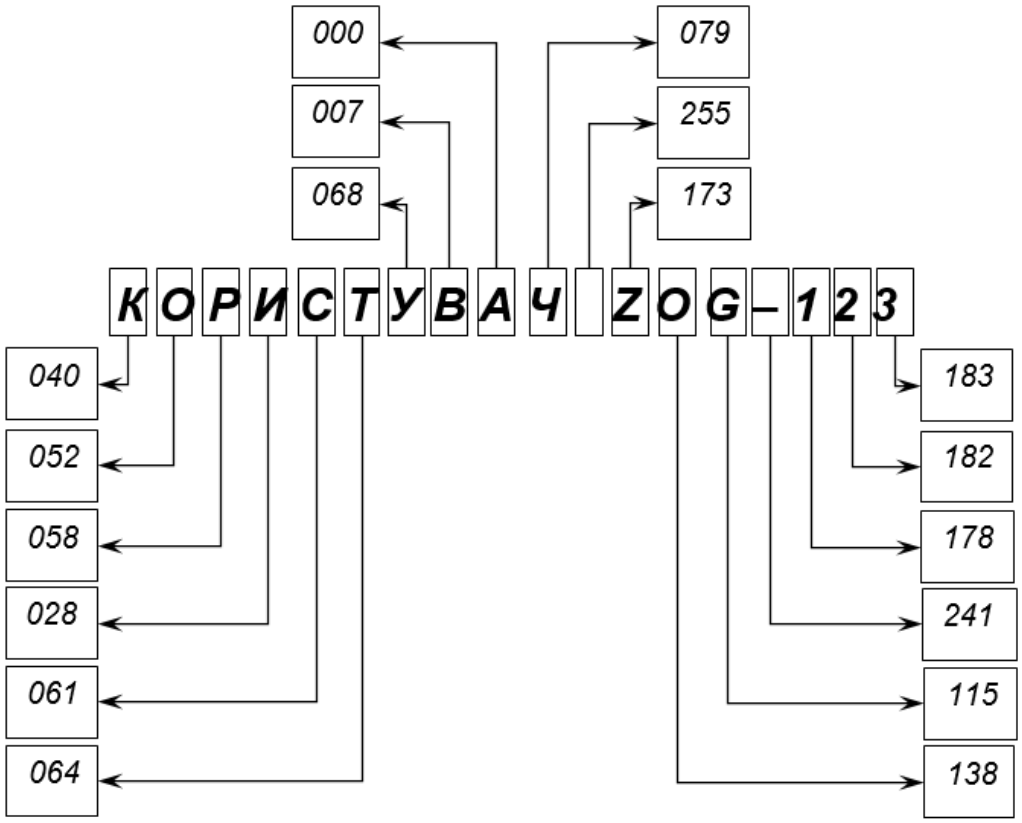

Рис. 1. Перетворення Нормативного алфавіту Повідомлення в Шифротекст

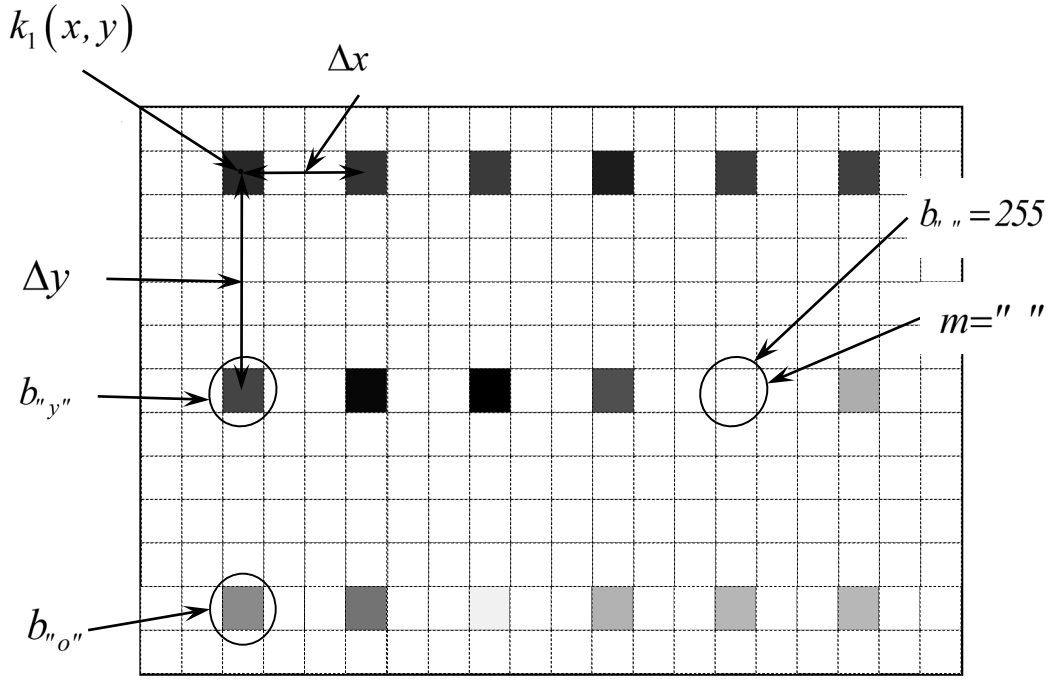

Рис. 2. Формування Ключа та Стегоповідомлення

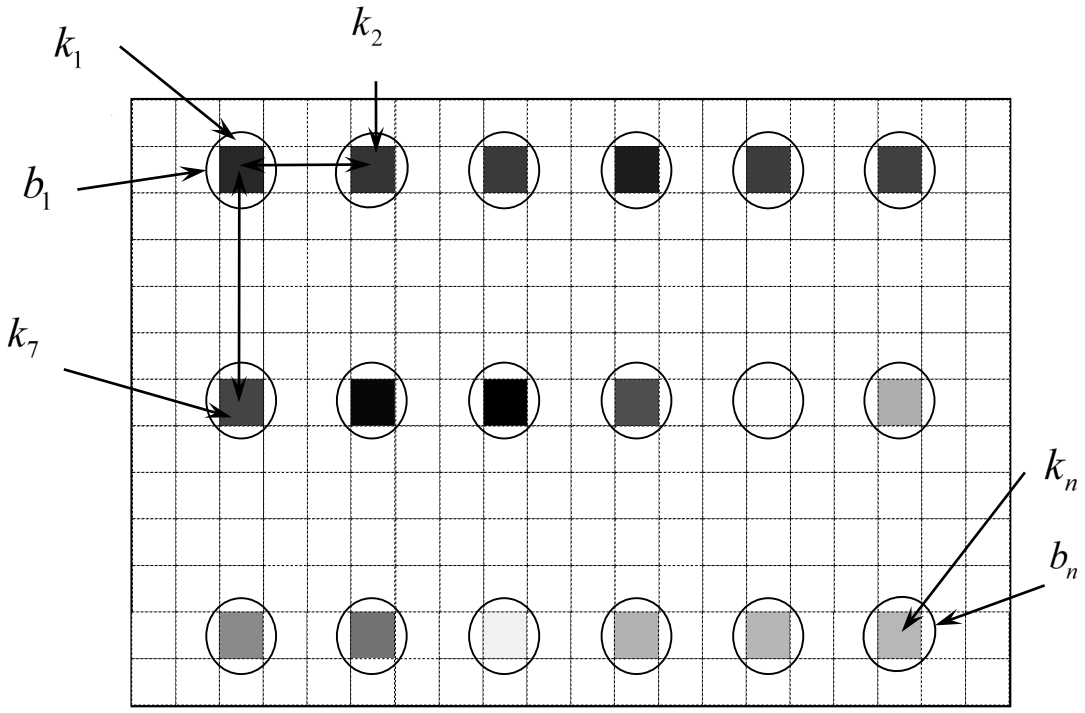

Рис. 3. Розшифрування Стегоповідомлення

Отже, у зазначеному методі здійснюється Шифрування та розшифрування цифрових даних за таким алгоритмом: визначають Ключ; присвоюють кожному елементу Нормативного алфавіту статичний діапазон значень яскравості пікселів монохромного зображення; формують Алфавіт шифрування; шифрують Повідомлення з використанням Алфавіту шифрування; формують Стегоповідомлення шляхом задання значення яскравості пікселів, що відповідають Алфавіту шифрування, на позиціях,

визначених Ключем, приховують Шифротекст у цифрове зображення; здійснюють передачу Адресату та отримання Стегоповідомлення; розшифровують Стегоповідомлення в Повідомлення з використанням Алфавіту шифрування за визначеним Ключем.

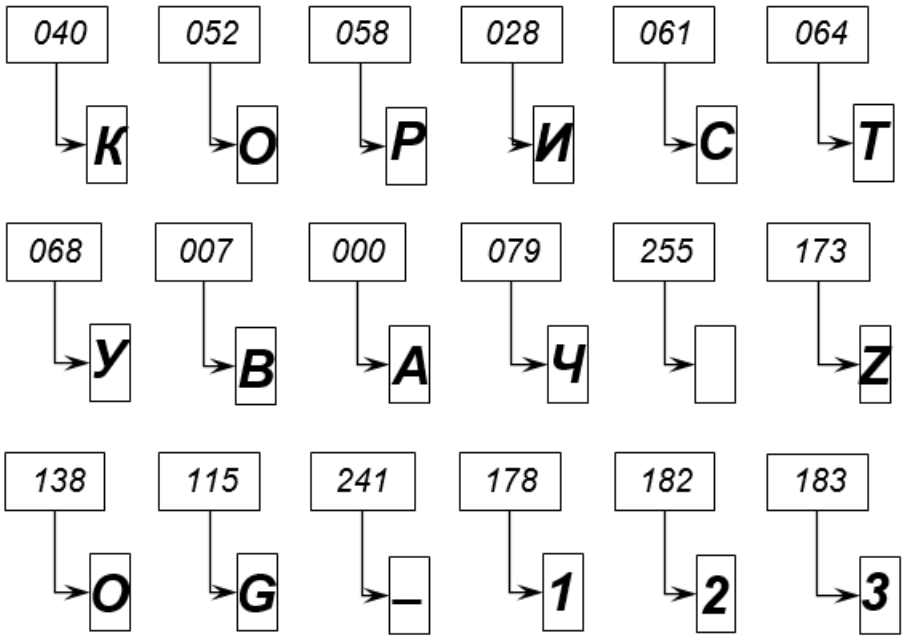

Рис. 4. Перетворення в Нормативний алфавіт та Повідомлення

Для автоматизації шифрування / розшифрування Повідомлення розроблено програму “Програмне забезпечення для шифрування / дешифрування даних на основі піксельного алфавіту зображення” (“PixelEncoder 1.0.0.0”) [5]. Програма дозволяє реалізувати:

1) формування Ключа та Алфавіту шифрування;

2) введення Повідомлення, визначення його Довжини та формування Шифротексту;

3) приховування Шифротексту або деформацію графічних даних значеннями Алфавіту шифрування Шифротексту в позиції, визначеній Ключем;

4) розшифрування Шифротексту.

Висновки. Запропонований метод забезпечує: високу стійкість зашифрованої інформації; зменшення рівня загрози несанкціонованого доступу до Повідомлення або атаки на шифр за рахунок Шифрування кожного символу Повідомлення динамічним випадковим числом з діапазону значень яскравості відповідного символу; зниження рівня загрози несанкціонованого доступу до Повідомлення за рахунок приховування Шифротексту в позиції графічних даних із урахуванням Ключа, який відомий лише Відправнику та Адресату.

Розроблений метод шифрування / розшифрування даних на основі піксельного алфавіту монохромного зображення доцільно застосовувати для ефективного функціонування мереж ІТС у ході передачі інформації каналами зв’язку в умовах наявності загрози здійснення несанкціонованого доступу до неї або атаки на шифр в інтересах забезпечення високої стійкості зашифрованої інформації.

СПИСОК ЛІТЕРАТУРИ

1. Method for encrypting and decrypting digital data transmitted or stored using the prioritized pixel transmission method: German patent. de № 10229976a1, МПК H04 L9/14, H04 N7/24, declared 03.07.2002, published 22.01.2004. URL: https://patentimages.storage.googleapis.com/ef/10/4c/c9f4a4c0617dd9/de10229976a1.pdf (last accessed: 08.09.2019).
2. Криптографія: загальні визначення, класифікація, асиметричні та симетричні криптоалгоритми, їх порівняння. 2014. URL: https://dehtyarov09.wordpress.com/2014/03/16/криптографія-загальні-визначення-кл-2 (дата звернення: 08.09.2019).
3. Хорошко В. А., Чекатков А. А. Методи й засоби захисту інформації. Київ : Юніор, 2003. 504 с.
4. Захист інформації в телекомунікаційних системах. URL: http://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah (дата звернення: 03.10.2019).
5. Програмне забезпечення для шифрування / дешифрування даних на основі піксельного алфавіту зображення. Свідоцтво про реєстрацію авторського права на твір № 101123. Дата реєстрації 09.12.2020.
6. Хорошко В. А., Шелест М. Е. Введение в компьютерную стеганографию. Киев : Нац. авіаційний ун-т, 2002. 152 с.

Подано 30.12.2020

REFERENCES

1. *Method for encrypting and decrypting digital data transmitted or stored using the prioritized pixel transmission method*: German patent. de № 10229976a1, МПК H04 L9/14, H04 N7/24, declared 03.07.2002, published 22.01.2004. Retrieved from https://patentimages.storage.googleapis.com/ef/10/4c/c9f4a4c0617dd9/de10229976a1.pdf.
2. *Kryptohrafiia: zahalni vyznachennia, klasyfikatsiia, asymetrychni ta symetrychni kryptoalhorytmy, yikh porivniannia [Cryptography: general definitions, classification, asymmetric and symmetric cryptoalgorithms, their comparison]*. (2014). Retrieved from https://dehtyarov09.wordpress.com/2014/03/16/kryptohrafiia-zahalni-vyznachennia-kl-2 [in Ukrainian].
3. Khoroshko, V. A., & Chekatkov, A. A. (2003). *Metody y zasoby zakhystu informatsii [Methods and means of information protection]*. Kyiv [in Ukrainian].
4. *Zakhyst informatsii v telekomunikatsiinykh systemakh [Information protection in telecommunication systems]*. (2019). Retrieved from http://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah [in Ukrainian].
5. *Prohramne zabezpechennia dlia shyfruvannia / deshyfruvannia danykh na osnovi pikselnoho alfavitu zobrazhennia. Svidotstvo pro reiestratsiiu avtorskoho prava na tvir [Software for encrypting / decrypting data based on the pixel alphabet of the image. Certificate of copyright registration for the work]* № 101123. Date of registration 09.12.2020 [in Ukrainian].
6. Khoroshko, V. A., & Shelest, M. E. (2002). *Vvedenie v komp'iuternuiu steganografiiu [Introduction to computer steganography]*. Kyiv [in Russian].

O. V Samchyshyn, I. V. Humeniuk, K. V. Smetanin, O. S. Bojchenko

METHOD OF ENCRYPTION/DECRYPTION OF DATA ON THE BASIS OF THE PIXEL ALPHABET OF MONOCHROME IMAGE

Improving the availability of information technology and increasing the volume of digital traffic leads to an important problem of data protection. A particularly pressing issue is the problem of transmitting confidential data through unsecured communication channels, such as the Internet. Recently, there has been a significant increase in the number of cyberattacks, including attempts to intercept and steal confidential information transmitted through global information networks. Information security in computer information and telecommunication systems is a priority. To date, one of the most reliable methods of protecting information is rightly considered to be encryption. Cryptographic data transformations are the most effective way for a system to maintain the confidentiality of information as it is entered, output, transmitted, processed, and stored, and to resist its destruction, theft, or distortion. But the most effective way to ensure the confidentiality of information is the combined use of steganographic and cryptographic means. In order to ensure high stability of encrypted information when transmitting it through the network of information and telecommunications systems and reduce the threat of unauthorized access to it or attack on the cipher, it is proposed to change the approach to solving the problem of data encryption. A method of encrypting / decrypting digital text information based on the pixel alphabet of a monochrome image, which is based on hiding or distorting graphic data, is proposed. This approach allows you to ensure high stability of encrypted information and significantly reduce the risk of unauthorized access to confidential information or attack on the cipher by encrypting each character with a dynamic random number from the range of values of the corresponding character and hiding the encrypted text in the position of graphic data. sender and recipient only.

Keywords: *data encryption / decryption, cryptographic algorithm, digital steganography, information and telecommunication system.*