$$f\left(Y,X\right)=C_{YX}^{q-1}C_{YX}^{q-2}\ldots C_{YX}^{1}C_{YX}^{0},$$
$$C_{YX}^{q}\in\left[0,1\right],\ f\left(Y,X\right)\in\left[0,2^{q}-1\right]. \quad (1)$$

Like digital watermarks, quantum watermarks aim to protect the copyright of an image and authenticate its owner by means of visible or invisible signals (mostly logos) embedded in the image container (or media). Most quantum watermarking strategies are based on FRQI for media images and watermark logos. The NEQR model [2, 4, 6], which stores color information in the ground state of a quantum sequence, uses a total of 2n+q qubits to represent an image, where n represents position coordinate information and q represents color information. This allows for precise manipulation of color information and makes certain image operations that were previously complex simple and convenient.

References

1. P. Q Le., F. Dong and K. Hirota "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," Quantum Information Processing, vol. 10, pp. 63–84, 04 2010.

2. Y. J. Zhang, K. Lu, Y. Gao and M. Wang "Neqr: a novel enhanced quantum representation of digital images," Quantum Information Processing, vol. 12, pp. 2833–2860, 2013.

3. M. A. Nielsen and I. L. Chuang Quantum computation and quantum information. Cambridge University Press, 2019.

4. Methods of Information Protection Based on Quantum Image Steganography / O.I. Fediushyn, Y.V. Holovko, et al. Radiotekhnika: All-Ukr. Sci. Interdep. Mag. 2024. № 218.

5. Venegas-Andraca S. and Bose S. Storing, processing, and retrieving an image using quantum mechanics, in Proc. SPIE Conf. Quantum Information and Computation, (2003), pp. 134–147.

6. RG. Zhou, Luo et al. A Novel Quantum Image Steganography Scheme Based on LSB. Int J Theor Phys 57, 1848–1863 (2018). https://doi.org/10.1007/s10773-018-3710-x.

ДОСЛІДЖЕННЯ МНОЖИНИ ТРИРОЗРЯДНИХ ЛОГІЧНИХ ОПЕРАЦІЙ ДЛЯ МАТРИЧНОГО КРИПТОПЕРЕТВОРЕННЯ

Антоненко О.О., Приступа А.Ю., Емінов Р.Т., Можаєв О.О.
Харківський національний університет Внутрішніх справ, Харків, Україна

Основу гарантування інформаційної безпеки в інформаційно-телекомунікаційних системах становлять криптографічні методи та засоби захисту інформації. Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має являти собою сукупність організаційно-технічних та криптографічних заходів [1,2].

В основі криптографічних методів лежить поняття криптографічного перетворення інформації, створеного за певними математичними законами, з метою виключити доступ до цієї інформації сторонніх користувачів, а також з метою забезпечення неможливості безконтрольного отримання інформації з боку тих самих осіб [3].

Метою доповіді є побудова методики синтезу логічних функцій на основі методу перебору, що дозволить повисити ефективність збору інформації про логічні функції декількох змінних, які можуть використовуватися в криптографії, та визначення їх особливостей.

В доповіді наводяться результати досліджень множини трирозрядних логічних операцій для матричного криптоперетворення. Наведені дані показують, що для синтезу трирозрядних операцій криптографічного перетворення можуть використовуватися різні елементарні логічні операції.

На основі аналізу експериментальних досліджень встановлено, що шість операцій утворюють групу операцій криптографічного перетворення, в якій повторне перетворення інформації другою операцією приведе до перетворення інформації третьою операцією з цієї групи.

Список літератури

1. Глинчук, Людмила Ярославівна. Криптологія [Текст] : навч.-метод. посіб. / Л. Я. Глинчук ; Східноєвроп. нац. ун-т ім. Лесі Українки. - Луцьк : ВежаДрук, 2014. - 163 с. : рис., табл. - Бібліогр.: с. 157-158.

2. Горбенко, Іван Дмитрович. Прикладна криптологія. Теорія. Практика. Застосування / Горбенко І. Д., Горбенко Ю. І. ; Харк. нац. ун-т радіоелектроніки, Х. : Форт, 2013. - 878 с.

3. Козіна, Г. Л. Криптографія від історії до сучасних стандартів [Текст] : навч. посіб. / Г. Л. Козіна. - Запоріжжя : НУ "Запорізька політехніка", 2020. - 192 с.

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВБУДОВУВАННЯ ДАНИХ В ЧАСТОТНУ ОБЛАСТЬ ЗОБРАЖЕНЬ

Лисенко С.О., Стрєлка Р.В., Єрмак В.М., Рог В.Є.
Харківський національний університет Внутрішніх справ, Харків, Україна

Інформація є одним з цінних предметів сучасного життя. Отримання доступу до неї з появою глобальних комп'ютерних мереж стало неймовірне простим. В той же час, легкість і швидкість такого доступу значно підвищили і загрозу неавторизованого доступу до інформації. Завдання надійного захисту авторських прав, конфіденційних даних від несанкціонованого доступу є однією з давніх й невирішених на сьогодні проблем. Приховування факту існування вбудованих даних при їх передачі, зберіганні або обробці є завданням стеганографії - науки, яка вивчає способи і методи приховання конфіденційних відомостей [1, 2].

Метою доповіді є дослідження процесу вбудовування даних в частотну область зображень, що дозволить покращити захист авторських прав в ряді прикладних галузей. В доповіді було розглянуто автоматизовану систему управління виробництвом друкарської продукції та створення систем приховання даних на основі різних стеганографічних методів. В результаті аналізу методів вбудовування даних в просторову та частотну області зображень встановлено, що найбільш простим з точки зору практичної