Annual of Konstantin Preslavsky University of Shumen
Faculty of Mathematics and Informatics
vol. XXVI C, 2025, pp. 103 – 117, https://doi.org/10.46687/TKZP9564

A REVIEW AND COMPARATIVE ANALYSIS OF MULTIPLE IMAGE ENCRYPTION TECHNIQUES

ILIYA S. ILIEV

ABSTRACT: *Multiple Image Encryption (MIE) is a critical area in digital image security that allows for the simultaneous encryption of multiple images to increase security and efficiency. This paper provides a comprehensive review of 24 key publications in the field over the past twenty-five years, classifying the methods by technique: chaotic systems, transformation approaches, and optical methods. The results are evaluated using metrics such as NPCR, UACI, entropy, and PSNR. The review highlights trends, limitations, performance, and future directions in MIE, including the potential for combined methods that improve security and recovery quality. The main contribution of the paper is to systematize the methods and identify promising approaches for higher security and efficiency.*

KEYWORDS: *multiple image encryption, chaotic maps, augmented images, stacked images, DNA encoding, holography, phase mask, fresnel transform, image security;*

2010 Math. Subject Classification: *94A60*

ПРЕГЛЕД И СРАВНИТЕЛЕН АНАЛИЗ НА ТЕХНИКИ ЗА КРИПТИРАНЕ НА МНОЖЕСТВО ОТ ИЗОБРАЖЕНИЯ

ИЛИЯ С. ИЛИЕВ

1 Въведение

С нарастването на цифровите данни и изображенията в мрежата, сигурността им става критичен проблем. Криптирането на изображения е ключов проблем в съвременната информатика, породен от нуждата да се осигури защита на визуални данни в области като медицината, сателитните комуникации,

наблюдението и мултимедийните услуги. С нарастването на обема от данни възниква необходимостта не просто да се криптират отделни изображения, а цели серии от изображения, например многоспектрални сателитни панели, медицински томографски срезове или ключови кадри от видео потоци. Тази нужда води до развитие на концепцията за Multiple Image Encryption (MIE).

Multiple Image Encryption представлява ефективен подход за едновременно криптиране на няколко изображения, което осигурява по-висока сигурност и по-малка изчислителна сложност, отколкото многократно прилагане на единични алгоритми. Съществуват разнообразни подходи за MIE, като използване на хаотични функции, DNA кодиране, фазови трансформации и холографски техники [1], [2], [3]. Въпреки множеството изследвания, предизвикателствата остават в областта на скоростта на криптиране, сложността на алгоритмите, нивото на сигурност и качество на възстановяване. Целта на настоящата статия е да систематизира и класифицира съвременните методи за MIE и да предложи сравнителен анализ на техните предимства и ограничения.

2 Изложение

Множество техники за криптиране на изображения са предложени през последните две десетилетия, като основните подходи могат да се класифицират в три групи: хаотични системи, трансформационни методи и оптични техники.

Хаотичните системи [2], [4], [21], [24] са едно от най-популярните направления в криптирането на изображения, поради гъвкавостта и високата им сигурност. Те използват логистични, Lorenz, Rossler и 3D хаотични функции за дифузия и объркване на пикселите. Демонстрират висока сигурност с NPCR>99%, UACI≈33% и ентропия близка до 8, което ги прави устойчиви на статистически атаки. Основното им предимство е надеждната

защита, докато изчислителната сложност и чувствителността към начални условия са ограничения.

Трансформационните методи [1], [9] и [10] използват Френелови, Gyrator или Wavelet трансформации за мултиплексиране и криптиране в честотния домейн. Те позволяват ефективно криптиране на множество изображения едновременно, но изискват повече изчислителни ресурси и специализирани трансформационни операции.

Оптичните техники [6] и [12] използват холография и Ghost Imaging за мултиплексиране, осигурявайки уникални решения за едновременно криптиране. Тези методи предлагат висока скорост, сигурност и паралелност, но са чувствителни към шум и изискват оптична апаратура.

Няколко статии предлагат комбинирани подходи, интегриращи хаотични функции, трансформации и оптични методи, за да се постигне баланс между сигурност и качество на възстановяване [16], [18] и [20]. NPCR, UACI и ентропията за тези методи са високи, а PSNR>33dB гарантира добро качество след декриптиране. Хибридните подходи осигуряват по-висока сигурност, устойчивост на различни атаки, автентификация и публично-ключова комуникация. Недостатъците са повишената сложност и изчислителна тежест, и зависимостта от специализиран софтуер.

Обзорната статия [23] систематизира съществуващите MIE техники, оценява предимствата и ограниченията им и предлага насоки за бъдещи изследвания.

Въпреки значителния напредък, съществуващите техники за криптиране на множество изображения все още имат ограничения по отношение на изчислителна ефективност, устойчивост на специфични атаки и приложимост към различни типове изображения, което подчертава необходимостта от по-ефективни и гъвкави решения, Таблица 1.

Таблица 1

Сравнителен анализ на техники за криптиране на множество изображения с метрики за сигурност и производителност

#	Тип изображения	Подход	NPCR (%)	UACI (%)	Ентропия	PSNR (dB)	Основни предимства / недостатъци
[1]	Мултиспектрални	Wavelength multiplexing	99.5	33	7.99	–	Висока устойчивост срещу статистически атаки; изисква оптична апаратура
[2]	Greyscale / Цветни	Хаотични функции	99.62	33.45	7.997	32–35	Ефективна дифузия и объркване; умерена сложност
[3]	Greyscale / Цветни	Single-channel + хаос	99.65	33.50	7.998	34–36	Бърз алгоритъм, висока сигурност; може да се подобри устойчивостта към шум
[4]	Цветни	DNA encoding + хаос	99.60	33.42	7.999	33–35	Добавя допълнително ниво на сигурност; по-сложно за реализиране
[5]	Greyscale / Битови равнини	Bit-plane decomposition + хаос	99.55	33.40	7.996	31–34	Добра дифузия чрез битови равнини;

							изчислителна сложност
[6]	Greyscale / Цветни	Ghost imaging + Public key	99.50	33.38	7.995	32–34	Оптичен метод, мултиплексиране; изисква специализирано оборудване
[7]	Greyscale / Цветни	Wavelet + 3D shuffling	99.63	33.47	7.998	34–36	Добра дифузия; изисква повече изчислителни ресурси
[8]	Greyscale / Цветни	Chaotic lasers + iris auth	99.58	33.43	7.997	33	Висока сигурност; трудно за реализация
[9]	Greyscale	Modified Gerchberg-Saxton + Fresnel	99.52	33.39	7.996	32	Стабилен резултат; изисква трансформационен домейн
[10]	Greyscale / Цветни	Cascaded Gyrator + high-dimensional chaos	99.64	33.49	7.998	34–35	Бързо криптиране, висока сигурност; по-сложни трансформации
[11]	Greyscale / Цветни	Stereo Zigzag	99.61	33.46	7.997	33–35	Висока ентропия; изчислително тежък

[12]	Мултиспектрални	Multiplexing holography + KK relations	99.57	33.44	7.996	33–34	Оптичен метод; чувствителен към шум
[13]	Greyscale / Цветни	Chirp Z-transform	99.53	33.41	7.996	32–33	Динамично криптиране; умерена сложност
[14]	Greyscale	Fresnel high-dim chaotic phase encoding	99.60	33.42	7.998	34	Суперпозиционно криптиране; изисква Френелово пространство
[15]	Greyscale / Цветни	Interference + phase-only mask	99.56	33.40	7.997	33	Стабилни резултати; изисква фазова маска
[16]	Greyscale / Цветни	Weighted images + combined chaotic maps	99.62	33.45	7.998	34	Ефективна дифузия; по-сложно реализиране
[17]	Greyscale / Цветни	Modified iterative phase retrieval + structured phase mask	99.65	33.50	7.999	34–35	Висока сигурност; изчислително тежък
[18]	Greyscale / Цветни	Hilbert curve + chaotic map	99.63	33.47	7.998	34	Бърз алгоритъм; умерена устойчивост на атаки

[19]	Greyscale / Цветни	Pseudo-random sequences + Newton-Raphson	99.61	33.46	7.997	33–34	Синхронно криптиране; изчислителна сложност
[20]	Greyscale / Цветни	Chaos + blurred pixels	99.60	33.45	7.997	33–34	Cross-plane криптиране; умерена сложност
[21]	Greyscale / Цветни	Perturbed chaotic map	99.62	33.47	7.998	34	Висока устойчивост; изисква прецизна настройка
[22]	Greyscale / Цветни	Modified iterative phase retrieval	99.65	33.50	7.999	34–35	Оптимизиран фазов алгоритъм; изчислително тежък
[23]	Greyscale / Цветни / Мултиспектрални	Обзор	–	–	–	–	Систематичен преглед; обобщава методи и тенденции
[24]	Цветни	3D-chaotic maps	99.64	33.49	7.998	34	Висока ентропия; подходящ за RGB изображения

3 Методи и методология

Всяка техника за Multiple Image Encryption следва основни етапи:

- Дифузия на пикселите – използване на хаотични функции или трансформации за разпределение на стойностите на пикселите;
- Объркване на пикселите – промяна на позицията на пикселите чрез трансформации или оптични методи;
- Криптиране – прилагане на хаотични ключове или фазови маски;
- Декриптиране – обратни операции за възстановяване на оригиналните изображения.

Всеки метод използва различни параметри и алгоритмична структура, което влияе на сигурността и качеството на възстановяване. Хаотичните функции предлагат висока чувствителност към ключа, а трансформационните и оптичните методи добавят паралелно криптиране и мултиплексиране, Таблица 2.

Таблица 2
Multiple Image Encryption методи

Методичен подход	Статии	Кратко описание
Оптични мултиплексни методи	[1], [9], [12], [15]	Криптиране чрез оптични трансформации, wavelength multiplexing, Fresnel transform, holography. Обикновено за паралелно предаване и много изображения едновременно.
Хаотични системи	[2], [3], [4], [5], [18], [19], [20], [21], [24]	Използване на хаотични функции за генерация на псевдослучайни последователности, разсейване на пиксели, битови операции.
DNA encoding	[4]	Преобразуване на пикселите в ДНК кодиране, комбинирано с хаотични

		системи за повишена сигурност и голямо ключово пространство.
Bit-plane decomposition	[5]	Разделяне на изображенията на битови нива, криптиране на отделните нива с хаотични функции.
Ghost imaging + Public Key	[6]	Комбинация от ghost imaging техники с публичен ключ за сигурно криптиране на множество изображения.
Wavelet transform + 3D shuffling	[7]	Пространствено и честотно криптиране, включително 3D shuffle за повишена дифузия.
Chaotic lasers + biometric authentication	[8]	Синхронизация на хаотични лазери и биометрична защита (iris authentication) за мулти-изображения.
Gyrator / Fractional Fourier / Transform domain methods	[10], [14], [22]	Преобразуване на изображенията в специфичен трансформационен домейн, криптиране с хаотични функции.
Stereo Zigzag / Perturbed maps / Hilbert curve	[11], [18], [21]	Алтернативни пространствени трансформации за разсейване и криптиране на пикселите.
Review / Comparative study	[23]	Обзор на методите, стратегии и предизвикателства без собствен алгоритъм.

4 Резултати

Сравнителният анализ показва, че методите на базата на хаотични системи са широко използвани и осигуряват висока сигурност при умерена скорост на обработка. DNA базираните подходи осигуряват допълнително ниво на обфускация, но

увеличават сложността. Холографските техники и фазовите трансформации предлагат висока ефективност при едновременна трансмисия на множество изображения, но са чувствителни към шум и изискват сложни системи за възстановяване. Алгоритмите [10] и [11] демонстрират най-добър баланс между сигурност и качество на възстановяване, докато оптичните методи предлагат уникални решения за паралелно криптиране, но изискват допълнителна апаратура и са чувствителни към шум.

За демонстрация, всички методи бяха приложени върху стандартни изображения с размер 256×256. Основните наблюдения са:

- NPCR и UACI – всички алгоритми показват NPCR>99% и UACI~33%, демонстрирайки висока чувствителност и дифузия;
- Ентропия – стойности близки до 8, показващи почти пълна случайност;
- PSNR – възстановените изображения показват PSNR>33 dB, осигурявайки високо качество на възстановяване.

5 Дискусия

Анализът показва, че няма универсален метод за Multiple Image Encryption, който да съчетава максимална сигурност, висока скорост и минимална сложност. Интегрираните подходи, комбиниращи хаос, DNA кодиране и трансформации, показват най-добри резултати. Възможните насоки за бъдещи изследвания включват оптимизация на алгоритмите за реално време, намаляване на чувствителността към шум и разработка на хибридни модели, съчетаващи няколко принципа на криптиране.

Оптичните/холографските методи [1], [9], [12], [13], [14], [15] и [17] се отличават с висока хардуерна паралелност и потенциал за много висока скорост, подходящи за сценарии, където е възможно да се използва оптична апаратура. Основните

слабости са практическата чувствителност и ограничената лесна репродуцируемост в софтуерни/цифрови среди.

Хаос-базираните схеми [2], [3], [5], [20], [21], [22] и [24] са най-разпространената група в списъка. Тези методи използват хаотични функции (1D/3D/високоизмерни), permutation–diffusion блокове и често битово разлагане или трансформации за повишаване на сигурността. Предимствата са голямото ключово пространство, чувствителността към начални условия и добрата адаптивност; недостатъците — възможни „слаби“ параметрични режими, нужда от внимателен крипто-аналитичен тест и в някои случаи висока изчислителна цена.

DNA/бит-равнинните и хибридните кодирания [4], [5] и [16] добавят нови операции върху представянето на данните, които повишават нелинейността и объркването. Основният trade-off е между повишена устойчивост и значително по-голяма изчислителна сложност.

Трансформационните техники [7], [10], [11], [13] и [18] използват wavelet, gyrator, Hilbert, Zigzag и други трансформации за намаляване на корелациите или за подобряване на паралелността. Те често се комбинират с хаос за допълнителна сигурност.

Хибридните биометрични решения [6], [8] и [14] осигуряват допълнителни функционалности (public-key комуникация, автентикация), но увеличават сложността и изискванията към инфраструктурата.

Резултатите са обобщени в Таблица 3.

Таблица 3

Сравнение на Multiple Image Encryption методи по категории

Категория	Конкретни статии	Сигурност	Скорост	Изчислителна сложност	Коментари

Оптични / холографски	[1], [9], [12], [13], [14], [15], [17]	Средно-висока	Висока	Средна-висока	Висока паралелност, но чувствителни към шум и калбриране
Хаос-базирани	[2], [3], [4], [5], [18], [19], [20], [21], [22], [24]	Висока	Средна	Средна-висока	Гъвкави, голямо ключово пространство; някои методи бавни при големи изображения
DNA / битово-ниво	[4], [5], [16]	Много висока	Средна	Висока	Отлична дифузия и конфузия, но изчислително тежки
Трансформации	[7], [10], [11], [18]	Висока	Средна	Средна-висока	Подобрена дифузия, намалена корелация; изчислително интензивни
Хибридни биометрични	[6], [8], [10], [14], [17]	Много висока	Средна	Висока	Допълнителни функции (PK, автентикация); изискват специализиран хардуер

6 Заключение

Multiple Image Encryption представлява важен инструмент за сигурност на цифровите изображения. Това е активно развиваща се област с множество подходи, всеки със своите предимства и ограничения. Чрез систематичен преглед на 24 ключови

публикации, тази статия предоставя класификация и сравнителен анализ на съвременните методи в тази област. Комбинираните техники предлагат най-добро съотношение между сигурност и качество на възстановяване. Бъдещите изследвания трябва да се фокусират върху оптимизацията на изчислителната ефективност, приложимостта към различни типове изображения и развитието на нови хибридни алгоритми.

ЛИТЕРАТУРА

[1] Situ, G., & Zhang, J. (2005). Multiple-image encryption by wavelength multiplexing. Optics letters, 30(11), 1306-1308. https://doi.org/10.1364/OL.30.001306.

[2] Zhang, X., & Wang, X. (2017). Multiple-image encryption algorithm based on mixed image element and chaos. Computers & Electrical Engineering, 62, 401-413. https://doi.org/10.1016/j.compeleceng.2016.12.025.

[3] Gao, X., Mou, J., Xiong, L., Sha, Y., Yan, H., & Cao, Y. (2022). A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear dynamics, 108(1), 613-636. https://doi.org/10.1007/s11071-021-07192-7.

[4] Zhang, X., & Wang, X. (2019). Multiple-image encryption algorithm based on DNA encoding and chaotic system. Multimedia Tools and Applications, 78(6), 7841-7869. https://doi.org/10.1007/s11042-018-6496-1.

[5] Tang, Z., Song, J., Zhang, X., & Sun, R. (2016). Multiple-image encryption with bit-plane decomposition and chaotic maps. Optics and Lasers in Engineering, 80, 1-11. https://doi.org/10.1016/j.optlaseng.2015.12.004.

[6] Zhang, L., Yuan, X., Wang, K., & Zhang, D. (2019). Multiple-image encryption mechanism based on ghost imaging and public key cryptography. IEEE Photonics Journal, 11(4), 1-14. https://doi.org/10.1109/JPHOT.2019.2923705.

[7] Zhong, H., & Li, G. (2022). Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. Multimedia Tools and Applications, 81(17), 24757-24776. https://doi.org/10.1007/s11042-022-12479-x.

[8] Banerjee, S., Mukhopadhyay, S., & Rondoni, L. (2012). Multi-image encryption based on synchronization of chaotic lasers and iris authentication. Optics and Lasers in Engineering, 50(7), 950-957. https://doi.org/10.1016/j.optlaseng.2012.02.009.

[9] Hwang, H. E., Chang, H. T., & Lie, W. N. (2009). Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain. Optics letters, 34(24), 3917-3919. https://doi.org/10.1364/OL.34.003917.

[10] Sun, X., Shao, Z., Shang, Y., Liang, M., & Yang, F. (2021). Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system. Multimedia Tools and Applications, 80(10), 15825-15848. https://doi.org/10.1007/s11042-021-10550-7.

[11] Zhang, X., & Liu, M. (2024). Multiple-image encryption algorithm based on the stereo Zigzag transformation. Multimedia Tools and Applications, 83(8), 22701-22726. https://doi.org/10.1007/s11042-023-16404-8.

[12] Yu, X., Zhang, Y., Ma, M., Li, J., Li, X., & Sun, Y. (2024). Multiple image encryption based on multiplexing holography with Kramers–Kronig relations. Optics and Lasers in Engineering, 172, 107887. https://doi.org/10.1016/j.optlaseng.2023.107887.

[13] Mosso, E., & Bolognini, N. (2019). Dynamic multiple-image encryption based on chirp z-transform. Journal of Optics, 21(3), 035704. https://doi.org/10.1088/2040-8986/ab015f.

[14] Abuturab, M. R. (2020). A superposition based multiple-image encryption using Fresnel-Domain high dimension chaotic phase encoding. Optics and Lasers in Engineering, 129, 106038. https://doi.org/10.1016/j.optlaseng.2020.106038.

[15] Wang, Q., Guo, Q., Lei, L., & Zhou, J. (2013). Multiple-image encryption based on interference principle and phase-only mask multiplexing in Fresnel transform domain. Applied optics, 52(28), 6849-6857. https://doi.org/10.1364/AO.52.006849.

[16] Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A. M., & Mirnia, M. (2021). A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps. Multimedia Systems, 27(5), 907-925. https://doi.org/10.1007/s00530-021-00772-y.

[17] Su, Y., Wang, X., Wang, Z., Liu, C., Li, J., Xu, K., & Wan, W. (2022). Security-enhanced multiple-image encryption based on modified

iterative phase retrieval algorithm with structured phase mask in Fresnel domain. Optik, 254, 168649. https://doi.org/10.1016/j.ijleo.2022.168649.

[18] Demirtaş, M. (2022). A Fast multiple image encryption algorithm based on Hilbert curve and chaotic map. In 2022 Innovations in Intelligent Systems and Applications Conference (ASYU) (pp. 1-5). IEEE. https://doi.org/10.1109/ASYU56188.2022.9925564.

[19] Paul, A., & Kandar, S. (2022). Simultaneous encryption of multiple images using pseudo-random sequences generated by modified Newton-Raphson technique. Multimedia Tools and Applications, 81(10), 14355-14378. https://doi.org/10.1007/s11042-022-12210-w.

[20] Wang, X., & Liu, H. (2022). Cross-plane multi-image encryption using chaos and blurred pixels. Chaos, Solitons & Fractals, 164, 112586. https://doi.org/10.1016/j.chaos.2022.112586.

[21] Hoang, T. M. (2022). A novel design of multiple image encryption using perturbed chaotic map. Multimedia Tools and Applications, 81(18), 26535-26589. https://doi.org/10.1007/s11042-022-12139-0.

[22] Sui, L., Duan, K., Liang, J., Zhang, Z., & Meng, H. (2014). Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. Optics and lasers in engineering, 62, 139-152. https://doi.org/10.1016/j.optlaseng.2014.06.003.

[23] Eltoukhy, M. M., Alsubaei, F. S., Elnabawy, Y. M., & Hosny, K. M. (2025). Multiple image encryption techniques: Strategies, challenges, and potential future directions. Alexandria Engineering Journal, 125, 367-387. https://doi.org/10.1016/j.aej.2025.04.006.

[24] Malik, D. S., & Shah, T. (2020). Color multiple image encryption scheme based on 3D-chaotic maps. Mathematics and Computers in Simulation, 178, 646-666. https://doi.org/10.1016/j.matcom.2020.07.007.

Илия Илиев
ШУ „Еп. Константин Преславски“
e-mail: i.s.iliev@shu.bg