International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

ЗАЩИТЕНО СКРИВАНЕ НА ИЗОБРАЖЕНИЕ В ИЗОБРАЖЕНИЕ ЧРЕЗ ХАОС-БАЗИРАНА LSB СТЕГАНОГРАФИЯ

Христина Стойчева[1]

[1]*Технически университет - Габрово, България*
e-mail: hsstoycheva@tugab.bg

A CHAOS-BASED LSB STEGANOGRAPHY APPROACH FOR SECURE IMAGE-IN-IMAGE HIDING

Hristina Stoycheva[1]

[1]*Technical University of Gabrovo, Bulgaria*
e-mail: hsstoycheva@tugab.bg

Abstract

This paper proposes a chaos-based LSB steganography approach for secure image-in-image hiding. The approach combines chaotic permutation, bidirectional chained diffusion, and Least Significant Bit (LSB) embedding. Chaotic sequences generated by the Lorenz system are used to control the permutation and diffusion of the secret image and to determine the embedding positions within the RGB cover image. The encrypted image is converted into a bitstream and embedded into chaos-selected LSB positions. Experimental results show an encrypted-image entropy of 7.9971 bit/pixel and correlation coefficients close to zero. Differential analysis based on 100 one-bit modifications yields mean NPCR and UACI values of 99.7864% and 33.4322%, respectively. The stego image achieves a PSNR of 52.9034 dB and an SSIM of 0.9964, while the secret image is recovered exactly with the correct key. A change of 10^{-12} in the Lorenz initial condition results in a BER close to 50%, indicating high end-to-end key sensitivity.

Keywords: LSB steganography; Lorenz chaotic system; image encryption; image hiding.

ВЪВЕДЕНИЕ

Бързото развитие на цифровите комуникационни технологии съществено променя начина, по който информацията се създава, съхранява, обработва и обменя. Наред с повишаването на достъпността и ефективността на информационния обмен нарастват и рисковете, свързани със сигурността на данните, предавани през отворени и незащитени комуникационни мрежи, където те могат да бъдат прихванати, модифицирани или неправомерно използвани [1-4]. Поради това осигуряването на конфиденциалност, цялостност и автентичност остава основно изискване към съвременните комуникационни системи.

За защита на информацията широко се използват криптографски и стеганографски подходи. Криптографията защитава съдържанието чрез преобразуването му в неразбираема форма [5-8], докато стеганографията прикрива самото наличие на чувствителна информация чрез вграждането ѝ в подходящ носител [9-13]. Комбинирането на двата подхода позволява реализиране на двустепенна защита. В този контекст нараства интересът към хибридни схеми, използващи хаотични системи [14], поради тяхната чувствителност към началните условия и параметрите, сложната апериодична динамика и възможността за генериране на последова-

Print ISSN: 1313-230X, Online ISSN: 3033-1404

телности с подходящи статистически характеристики [15].

В настоящия доклад се предлага хаос-управляван подход за LSB стеганография за защитено скриване на изображение в изображение. Секретното изображение се подлага на хаотична пермутация и двупосочна верижна дифузия, след което полученото криптирано изображение се преобразува в битов поток и се вгражда в най-младшите битове на RGB компонентите на покриващото изображение. Позициите за вграждане също се определят чрез хаотична последователност, поради което коректното възстановяване изисква както правилно определяне на позициите за извличане, така и успешно изпълнение на обратните криптографски преобразувания.

ИЗЛОЖЕНИЕ

Хаотична система на Лоренц

В предложения подход като източник на хаотични последователности се използва системата на Лоренц, описвана чрез следните уравнения:

$$\begin{aligned} \dot{x} &= -\sigma x + \sigma y \\ \dot{y} &= -xz + \rho x - y \\ \dot{z} &= xy - \beta z \end{aligned} \qquad (1)$$

където x, y и z са променливи на състоянието, а σ, ρ и β са параметрите на системата.

Системата на Лоренц се характеризира с чувствителност към началните условия и системните параметри, което я прави подходяща за генериране на последователности, използвани при криптографски и стеганографски преобразувания. В предложения подход генерираната хаотична траектория се използва за управление на пермутацията и дифузията на секретното изображение, както и за определяне на позициите за стеганографско вграждане.

LSB стеганография

LSB (Least Significant Bit) е най-младшият бит в двоичното представяне на числова стойност и има най-малка тежест при нейното формиране. При 8-битово цифрово изображение промяната на този бит изменя съответната пикселна или цветова стойност най-много с единица:

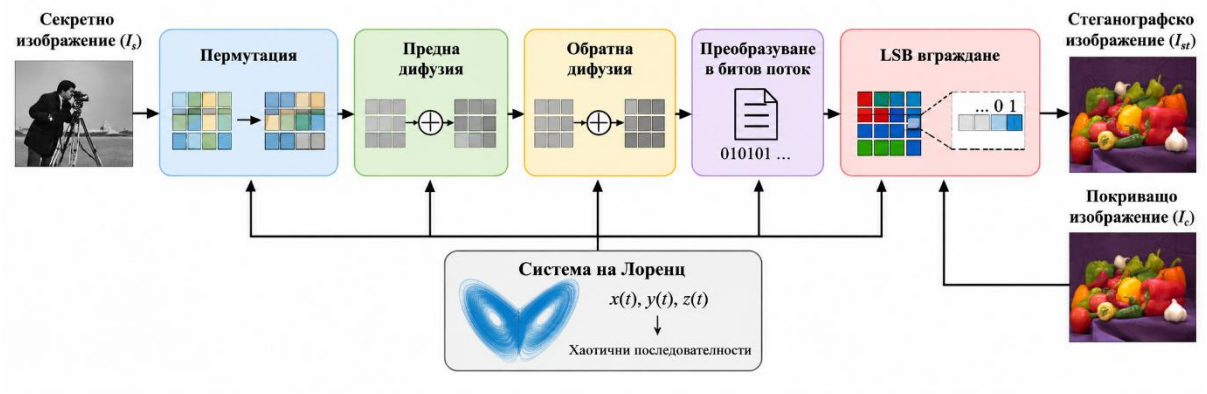
$$|p - p'| \leq 1. \qquad (2)$$

Това свойство позволява вграждане на информация с минимално изменение на визуалните характеристики на покриващото изображение.

В предложения подход криптираното секретно изображение се преобразува в битов поток, който се вгражда в LSB на псевдослучайно избрани RGB компоненти, като позициите се определят от хаотична последователност.

ХАОС-БАЗИРАН ПОДХОД ЗА СКРИВАНЕ НА ИЗОБРАЖЕНИЕ

Предложеният подход съчетава хаотична пермутация, двупосочна верижна дифузия и LSB стеганографско вграждане, като отделните етапи се управляват чрез последователности, генерирани от системата на Лоренц (Фигура 1). Секретното изображение първоначално се подлага на криптографска обработка, целяща едновременно нарушаване на пространствената зависимост между пикселите и разпространение на локалните изменения върху криптираното изображение. За тази цел след отстраняване на преходния процес, генерираната хаотична траектория се разделя на четири не-припокриващи се сегмента. Сегментът X_1 се използва за формиране на индексната последователност за пермутация, Y_2 и Z_3 участват съответно във права и обратна дифузия, а X_4 определя реда на позициите за стеганографско вграждане.



Фигура 1. *Блокова схема на предложения хаос-управляван подход*

По този начин различните операции се управляват от отделни части на хаотичната траектория и не се използват повторно едни и същи хаотични стойности.

След пермутацията върху секретните данни последователно се прилагат права и обратна дифузия, при което всеки обработван елемент зависи както от съответната хаотична ключова стойност, така и от резултата от предходния етап на веригата. Полученото криптирано изображение се преобразува в битов поток, който се вгражда в най-младшите битове на RGB компонентите на покриващото изображение. За разлика от последователното LSB вграждане, използваните позиции се определят чрез хаотичната последователност X_4, което води до псевдослучайно пространствено разпределение на скритите битове в покриващото изображение.

При приемната страна процесът се изпълнява в обратен ред. Чрез генериране на идентичните хаотични последователности първо се възстановяват позициите за извличане на битовия поток, след което последователно се прилагат обратните права и обратна дифузия и обратната пермутация. По този начин възстановяването на секретното изображение зависи от коректното възпроизвеждане на параметрите и началните условия на хаотичната система, както и от правилното изпълнение на всички обратни преобразувания.

Хаотична пермутация и двупосочна верижна дифузия

Секретното изображение се представя като едномерен вектор P. От хаотичния сегмент X_1 се формира индексната последователност:

$$\Pi = argsort(X), \mathrm{P}' = \mathrm{P}(\Pi). \quad (3)$$

След пермутацията се прилага двупосочна верижна дифузия с ключови последователности K^{f} и K^{b}, генерирани съответно от Y_2 и Z_3. При $F_0 = IV^{\mathrm{f}}$ *права дифузия* се определя чрез:

$$F_{\mathrm{i}} = mod(p'_{\mathrm{i}} + F_{\mathrm{i}}{}^{-1}, 256) XOR\ k^{\mathrm{f}}_{\mathrm{i}}, \quad i = 1, \ldots, N. \quad (4)$$

При $C_{\mathrm{n}+1} = IV^{\mathrm{b}}$ *обратната дифузия* се описва като:

$$C_{\mathrm{i}} = mod(F_{\mathrm{i}} + C_{\mathrm{i}}{}^{+1}, 256) XOR\ k^{\mathrm{b}}{}_{\mathrm{i}}, \quad i = N, \ldots, 1. \quad (5)$$

Получената последователност C представлява криптираното секретно изображение. Верижната зависимост в двете направления осигурява разпространение на локалните изменения върху криптираното изображение.

Хаос-управлявано LSB вграждане

Криптираната последователност C се преобразува в битов поток $B = \{b_1, b_2, \ldots, b_l\}$, като за всеки 8-битов елемент битовете се подреждат от най-старшия към най-младшия бит (MSB-first). Покриващото RGB изображение се представя като едномерен вектор V, а редът на позициите за вграждане се определя от $\Pi_{\mathrm{e}} = argsort(X_4)$.

В първите L позиции от Π_e най-младшият бит на съответния RGB компонент се заменя с текущия бит от B:

$$LSB(v\Pi_e(i)) = b_i, i = 1, \ldots, L. \quad (6)$$

Полученото изображение представлява стеганографското изображение.

Извличане и възстановяване

В приемната страна се генерират същите хаотични последователности чрез използване на идентични параметри и начални условия на системата на Лоренц. Първо се възстановява редът на позициите $\Pi_e = argsort(E)$ и от съответните LSB позиции се извлича бинарният поток $B' = \{b'_1, b'_2, \ldots, b'_l\}$.

След преобразуването му обратно в 8-битови стойности се получава криптираната последователност $C' = \{c'_1, c'_2, \ldots, c'_n\}$. След това се изпълнява обратната двупосочна дифузия.

$$F_i = mod\left((C_i \, XOR \, k^b_i) - C_{i+1}, 256\right), \quad i = N, \ldots, 1, \quad (7)$$

$$p'_i = mod\left((F_i \, XOR \, k^f_i) - F_i^{-1}, 256\right), \quad i = 1, \ldots, N, \quad (8)$$

при $C_{n+1} = IV^b$ и $F_0 = IV^f$.

Накрая се изпълнява обратната пермутация $P(\Pi) = P'$ и се възстановява оригиналното секретно изображение.

ЕКСПЕРИМЕНТАЛНИ РЕЗУЛТАТИ И ДИСКУСИЯ

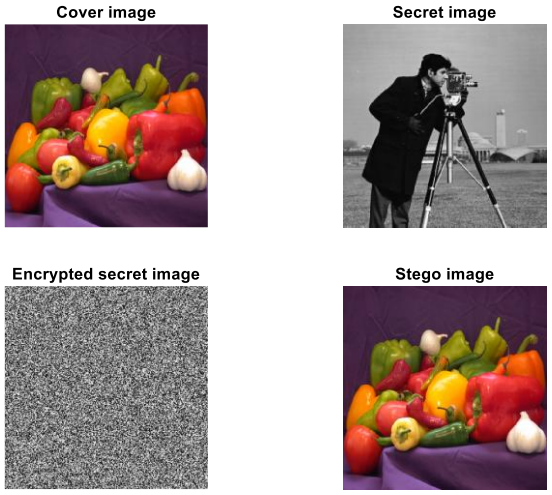
Предложеният подход е реализиран в MATLAB. Експерименталното изследване оценява статистическите характеристики на криптираното изображение, устойчивостта към минимални изменения на входните данни, качеството на стеганографското вграждане, точността на възстановяване и чувствителността към секретния ключ.

Експериментална постановка

Като покриващо изображение се използва RGB изображението peppers.png, а като секретно – 8-битовото черно-бяло изображение cameraman.tif. Основните параметри са обобщени в Таблица 1.

Таблица 1. *Основни параметри*

Параметър	**Стойност**
Покриващо изображение	peppers.png
Размер	512 × 512 × 3
Секретно изображение	cameraman.tif
Размер	256 × 256
Размер на битовия поток	524 288 bit
Налични LSB позиции	786 432
Използване на капацитета	66.67%
σ, ρ, β	10, 28, 8/3
x_0, y_0, z_0	0.1, 0.2, 0.3
Стъпка h	0.01
Отхвърлени начални итерации	5000
Forward IV / Backward IV	158 / 79



Фиг 2. ***(a)*** *покриващо изображение;*
(b) *секретно изображение;*
(c) *криптирано секретно изображение;*
(d) *стеганографско изображение*

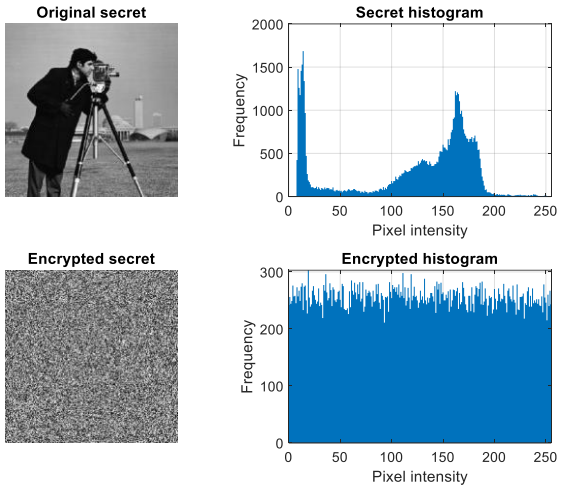
Статистически и диференциален анализ

Статистическите свойства на криптираното изображение се оценяват чрез информационна ентропия и корелация между съседни пиксели. Получените резултати са представени в Таблица 2.

Таблица 2. *Статистически характеристики*

Показател	**Секретно**	**Криптирано**
Ентропия, bit/pixel	7.009716	7.997096
rH	0.933475	0.005270
rV	0.959223	0.001720
rD	0.908664	−0.002975

Ентропията на криптираното изображение е близка до теоретичния максимум от 8 bit/pixel, а корелацията между съседните пиксели практически се елиминира. Това се потвърждава и от значително поравномерното хистограмно разпределение.



Фигура 3. *Секретно и криптирано изображение и съответните им хистограми*

Чувствителността към изменение на входните данни е изследвана чрез 100 теста. При всеки тест се инвертира само LSB на един пиксел: $p' = p\ XOR\ 1$, т.е. $|p' - p| = 1$. Получени са средни стойности NPCR = 99.7864% и UACI = 33.4322%, при диапазони съответно 99.5667–99.9939% и 32.9358–36.6119%. Резултатите показват силно разпространение на минималната входна промяна вследствие на двупосочната верижна дифузия.

Качество на стеганографското изображение и чувствителност към ключа

Качеството на стеганографското изображение, точността на възстановяване и чувствителността към ключа са обобщени в Таблица 3. При анализа на чувствителността само началното условие x_0 се изменя с $\Delta x_0 = 10^{-12}$, като всички останали параметри се запазват непроменени.

Таблица 3. *Числови резултати*

Показател	**Резултат**
MSE	0.333228
PSNR, dB	52.9034
Среден SSIM	0.996388
Променени RGB компоненти, %	33.3228
Максимална абсолютна промяна	1
Exact recovery при коректен ключ	1
MSE при коректно възстановяване	0
BER при $\Delta x_0 = 10^{-12}$, %	50.0895
MSE при грешен ключ	9466.971176
PSNR при грешен ключ, dB	8.3687
SSIM при грешен ключ	0.007661
Корелация при грешен ключ	−0.003420

Получените PSNR и SSIM показват високо сходство между покриващото и стеганографското изображение, като максималната промяна на RGB компонент е единица. При коректен ключ секретното изображение се възстановява без загуба. Изменението на x_0 само с 10^{-12} води до $BER \approx 50\%$, нисък SSIM и практически нулева корелация, което показва висока чувствителност на целия процес на извличане и възстановяване към изменения на ключа.



Фиг. 4*. Чувствителност към ключа: (a) оригинално секретно изображение; (b) възстановено изображение при коректен ключ; (c) възстановено изображение при* $\Delta x_0 = 10^{-12}$.

ЗАКЛЮЧЕНИЕ

В работата е предложен хаос-управляван подход за защитено скриване на изображение в изображение, съчетаващ хаотична пермутация, двупосочна верижна

дифузия и LSB стеганография. Експерименталните резултати показват висока ентропия на криптираното изображение - 7.9971 bit/pixel, практически нулева корелация между съседни пиксели и силна чувствителност към еднобитови изменения, със средни стойности NPCR = 99.7864% и UACI = 33.4322%.

Стеганографското изображение запазва високо сходство с покриващото изображение (PSNR = 52.9034 dB, SSIM = 0.9964), като при коректен ключ секретното изображение се възстановява точно. Изменение на началното условие на системата на Лоренц с 10^{-12} води до BER ≈ 50%, което показва висока чувствителност на схемата към секретния ключ.

БЛАГОДАРНОСТИ: *Този доклад и изследванията в него са реализирани по проект „Изследване на интелигентни методи, архитектури и технологии за защита на данни в комуникационните мрежи“, договор НИП2026-22/2026г. към УЦНИТ при ТУ – Габрово.*

ЛИТЕРАТУРА

[1] Guo, S., Wang, Y., Zhang, N., Su, Z., Luan, T. H., Tian, Z., & Shen, X., A survey on semantic communication networks: Architecture, security, and privacy. IEEE communications surveys & tutorials, 2024, 27(5), 2860-2894.

[2] Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., & Smirnov, O., Wireless network encryption: Stream ciphers, computational modeling, and security analysis. In Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024 (pp. 367-390). CRC Press.

[3] Mehic, M., Michalek, L., Dervisevic, E., Burdiak, P., Plakalovic, M., Rozhon, J., ... & Voznak, M., Quantum cryptography in 5G networks: A comprehensive overview. IEEE Communications Surveys & Tutorials, 2023, 26(1), 302-346.

[4] Attkan, A., & Ranga, V., Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 2022, 8(4), 3559-3591.

[5] Subramani, S., M, S., A, K., & Svn, S. K., Review of security methods based on classical cryptography and quantum cryptography. Cybernetics and Systems, 2025, 56(3), 302-320.

[6] Sasikumar, K., & Nagarajan, S., Comprehensive review and analysis of cryptography techniques in cloud computing. 2024, IEEE Access, 12, 52325-52351.

[7] Sahu, S. K., & Mazumdar, K., State-of-the-art analysis of quantum cryptography: applications and future prospects. Frontiers in Physics, 2024, 12, 1456491.

[8] Mulani, A. O., Godase, V. V., Takale, S. R., & Ghodake, R. G., Image authentication using cryptography and watermarking. International Journal of Image Processing and Smart Sensors, 2025, 1(2), 27-34.

[9] Song, B., Wei, P., Wu, S., Lin, Y., & Zhou, W., A survey on deep-learning-based image steganography. Expert Systems with Applications, 2024, 254, 124390.

[10] Kombrink, M. H., Geradts, Z. J. M. H., & Worring, M., Image steganography approaches and their detection strategies: A survey. ACM Computing Surveys, 2024, 57(2), 1-40.

[11] Wani, M. A., & Sultan, B., Deep learning based image steganography: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2023, 13(3), e1481.

[12] Driss, M., Berriche, L., Atitallah, S. B., & Rekik, S., Steganography in iot: A comprehensive survey on approaches, challenges, and future directions. IEEE Access, 2025, 13, 74844-74875.

[13] Azam, M. H. N., Ridzuan, F., Sayuti, M. N. S. M., Azni, A. H., Zakaria, N. H., & Potdar, V., A systematic review on cover selection methods for steganography: Trend analysis, novel classification and analysis of the elements. Computer Science Review, 2025, 56, 100726.

[14] Agarwal, M., & Ratan, R., A Review on Chaos-Based Cryptography and Steganography: Hybrid Frameworks. Procedia Computer Science, 2026, 282, 914-929.

[15] Dinu, A., From chaos to security: A comparative study of Lorenz and Rössler systems in cryptography. Cryptography, 2025, 9(3), 58.