# Security Analysis of an Image Encryption Scheme Based on a New Secure Variant of Hill Cipher and 1D Chaotic Maps

George Teşeleanu[1,2] [a]

[1] *Advanced Technologies Institute, 10 Dinu Vintilă, Bucharest, Romania*

[2] *Simion Stoilow Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei, Bucharest, Romania*

Keywords: Image Encryption Scheme, Chaos Based Encryption, Cryptanalysis.

Abstract: In 2019, Essaid *et al.* introduced a chaotic map-based encryption scheme for color images. Their approach employs three improved chaotic maps to dynamically generate the key bytes and matrix required by the cryptosystem. It should be noted that these parameters are dependent on the size of the source image. According to the authors, their method offers adequate security (*i.e.* 279 bits) for transmitting color images over unsecured channels. However, we show in this paper that this is not the case. Specifically, we present two cryptanalytic attacks that undermine the security of Essaid *et al.*'s encryption scheme. In the case of the chosen plaintext attack, we require only two chosen plaintexts to completely break the scheme. The second attack is a a chosen ciphertext attack, which requires two chosen ciphertexts and compared to the first one has a rough complexity of $2^{24}$. The attacks are feasible due to the fact that the key bits and matrix generated by the algorithm remain unaltered for distinct plaintext images.

## 1 INTRODUCTION

The exponential increase in social media usage has led to a heightened concern for the security of digital images, particularly with regards to theft and unauthorized distribution. Consequently, this issue has gained significant attention, prompting numerous researchers to develop various image encryption techniques. Chaotic maps have emerged as a favored approach for encrypting images, largely due to their high sensitivity to previous states, initial conditions, or both. This desirable feature makes it challenging to anticipate their behavior or outputs, thus giving rise to numerous novel cryptographic algorithms based on chaos. We refer the reader to (Zolfaghari and Koshiba, 2022; Muthu and Murali, 2021; Hosny, 2020; Özkaynak, 2018) for some surveys of such proposals. Regrettably, due to inadequate security analysis and a lack of design guidelines, a significant number of image encryption schemes based on chaos have been found to contain critical security vulnerabilities. To illustrate our point, we provide a list of compromised schemes in Table 1. Please be aware that the list is not exhaustive.

In (Essaid et al., 2019b) a chaos based encryption scheme is proposed. The authors use the Enhanced Logistic Map (ELM), Enhanced Chebyshev Map (ECM) and Enhanced Sine Map (ESM) as pseudorandom number generators (PRNGs). Using these three PRNGs, Essaid *et al.* randomly generate the necessary key bytes. Then, the ELM PRNG is used to generate a key matrix of size $2 \times 2$, such that the first element of the matrix is invertible modulo 256. Since ELM, ECM and ESM are simply used as PRNGs and the scheme's weakness is independent of the employed generators, we omit their description and simply consider the key bytes and matrix as being randomly generated.

This paper presents our security analysis of the Essaid *et al.* scheme. Specifically, we describe a chosen plaintext attack and a chosen ciphertext attack, which enables an attacker to decrypt all images of a particular size. To accomplish this, it is necessary to obtain the ciphertexts of two chosen plaintexts or the plaintexts of two chosen ciphertexts. Note that in the chosen plaintext scenario, we reduce the scheme's security from 279 bits to 0 bits, while in the chosen ciphertext scenario we reduce it to roughly 24 bits.

**Structure of the Paper.** We provide the necessary preliminaries in Section 2. An alternative mathematical description of Essaid *et al.*'s scheme is outlined

[a] https://orcid.org/0000-0003-3953-2744



Teşeleanu, G.
Security Analysis of an Image Encryption Scheme Based on a New Secure Variant of Hill Cipher and 1D Chaotic Maps.
DOI: 10.5220/0012356600003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 745-749
ISBN: 978-989-758-683-5; ISSN: 2184-4356

Table 1: Broken chaos based image encryption algorithms.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Scheme | (Yen and Guo, 2000) | (Matoba and Javidi, 2004) | (Wang et al., 2012) | (Huang et al., 2014) | (Khan, 2015) | (Song and Qiao, 2015) | (Chen et al., 2015) |
| Broken by | (Li and Zheng, 2002) | (Wang et al., 2019) | (Arroyo et al., 2013) | (Wen et al., 2021) | (Alanazi et al., 2021) | (Wen et al., 2019) | (Hu et al., 2017) |
| Scheme | (Hu et al., 2017) | (Niyat et al., 2017) | (Hua and Zhou, 2017) | (Pak and Huang, 2017) | (Liu et al., 2018) | (Shafique and Shahid, 2018) | (Sheela et al., 2018) |
| Broken by | (Li et al., 2019a) | (Li et al., 2018) | (Yu et al., 2021) | (Wang et al., 2018) | (Ma et al., 2020) | (Wen and Yu, 2019) | (Zhou et al., 2019) |
| Scheme | (Wu et al., 2018) | (Yosefnezhad Irani et al., 2019) | (Khan and Masood, 2019) | (Pak et al., 2019) | (Mondal et al., 2021) | (Essaid et al., 2019a) | |
| Broken by | (Chen et al., 2020) | (Liu et al., 2020) | (Fan et al., 2021) | (Li et al., 2019b) | (Li et al., 2021) | (Teşeleanu, 2023) | |

Algorithm 1: Encryption algorithm.

**Input:** A plaintext $P$, three secret keys $k_1$, $k_2$ and $k_3$, and a secret matrix $h$
**Output:** A ciphertext $C$

**for** $i \in [0, HW)$ **do**
  **if** $i = 0$ **then**
    $\begin{pmatrix} C_0 \\ T_0 \end{pmatrix} \leftarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} P_0 \\ k_{1,0} \end{pmatrix} + \begin{pmatrix} k_{2,0} \\ k_{3,0} \end{pmatrix} \bmod 256$
    $S_1 \leftarrow T_0 + P_1 \bmod 256$
  **else**
    $\begin{pmatrix} C_i \\ T_i \end{pmatrix} \leftarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} S_i \\ k_{1,i} \end{pmatrix} + \begin{pmatrix} k_{2,i} \\ k_{3,i} \end{pmatrix} \bmod 256$
    $S_{i+1} \leftarrow T_i + P_{i+1} \bmod 256$
**return** $C$
SetAlFnt

Algorithm 2: Decryption algorithm.

**Input:** A ciphertext $C$, three secret keys $k_1$, $k_2$ and $k_3$, and a secret matrix $h$
**Output:** A plaintext $P$

**for** $i \in [0, HW)$ **do**
  **if** $i = 0$ **then**
    $P_0 \leftarrow a^{-1} \cdot (C_0 - b \cdot k_{1,0} - k_{2,0}) \bmod 256$
    $tmp \leftarrow c \cdot P_0 + d \cdot k_{1,0} + k_{3,0} \bmod 256$
  **else**
    $P_i \leftarrow a^{-1} \cdot (C_i - b \cdot k_{1,i} - k_{2,i}) \bmod 256$
    $P_i \leftarrow P_i - tmp \bmod 256$
    $tmp \leftarrow c \cdot a^{-1} \cdot (C_i - b \cdot k_{1,i} - k_{2,i}) \bmod 256$
    $tmp \leftarrow temp + d \cdot k_{1,i} + k_{3,i} \bmod 256$
**return** $P$
SetAlFnt

in Section 3. In Sections 4 and 5 we show how an attacker can recover the secret values in a chosen plaintext/ciphertext scenario. We conclude in Section 6.

# 2 PRELIMINARIES

**Notations.** In this paper, the subset $\{1, \ldots, s-1\} \in \mathbb{N}$ is denoted by $[1, s)$. The action of selecting a random element $x$ from a sample space $X$ is represented by $x \stackrel{\$}{\leftarrow} X$, while $x \leftarrow y$ indicates the assignment of value $y$ to variable $x$. By $H$ and $W$ we denote an image's height and width. Hexadecimal numbers will always contain the prefix 0x.

## 2.1 Essaid *et al.* Image Encryption Scheme

In this section we present Essaid *et al.*'s encryption (Algorithm 1) and decryption (Algorithm 2) algorithms as described in (Essaid et al., 2019b). Before the encryption/decryption process starts, the image is always converted into a vector of size $H \cdot W$. At the end, the resulting vector is translated back into an image of size $H \times W$. Please note that both the key bytes $k_{1,i}$, $k_{2,i}$, and $k_{2,i}$, and the matrix $h$ values $a$, $b$, $c$, and $d$ are generated randomly. Also, $a$ is always invertible modulo 256.

# 3 A NEW LOOK AT ESSAID *et al.*'s SCHEME

In this section we provide an equivalent description of the scheme presented in (Essaid et al., 2019b). We first start with studying Algorithm 1.

**Lemma 3.1.** *Let $C_i$ and $T_i$ be the variables from Algorithm 1. Then we can rewrite them as follows*

$$C_i \equiv a \sum_{j=0}^{i} c^{i-j} P_j + \alpha_i \bmod 256,$$

$$T_i \equiv c \sum_{j=0}^{i} c^{i-j} P_j + \beta_i \bmod 256,$$

*where* $\beta_{-1} = 0$ *and*

$$\alpha_i \equiv a\beta_{i-1} + bk_{1,i} + k_{2,i} \bmod 256,$$
$$\beta_i \equiv c\beta_{i-1} + dk_{1,i} + k_{3,i} \bmod 256.$$

*Proof.* We will prove our assertion using induction. When $i = 0$ we have that

$$C_0 \equiv aP_0 + bk_{1,0} + k_{2,0} = aP_0 + \alpha_0 \bmod 256,$$
$$T_0 \equiv cP_0 + dk_{1,0} + k_{3,0} = cP_0 + \beta_0 \bmod 256.$$

We assume that the assertion is true for $i$ and we prove it for $i+1$. Therefore, we have

$$\begin{aligned} C_{i+1} &\equiv aS_{i+1} + bk_{1,i+1} + k_{2,i+1} \\ &\equiv a(T_i + P_{i+1}) + bk_{1,i+1} + k_{2,i+1} \\ &\equiv ac\sum_{j=0}^{i} c^{i-j}P_j + aP_{i+1} + a\beta_i + bk_{1,i+1} + k_{2,i+1} \\ &\equiv a\sum_{j=0}^{i+1} c^{(i+1)-j}P_j + \alpha_{i+1} \bmod 256 \end{aligned}$$

and

$$\begin{aligned} T_{i+1} &\equiv cS_{i+1} + dk_{1,i+1} + k_{3,i+1} \\ &\equiv c(T_i + P_{i+1}) + dk_{1,i+1} + k_{2,i+1} \\ &\equiv c^2\sum_{j=0}^{i} c^{i-j}P_j + cP_{i+1} + c\beta_i + dk_{1,i+1} + k_{3,i+1} \\ &\equiv c\sum_{j=0}^{i+1} c^{(i+1)-j}P_j + \beta_{i+1} \bmod 256, \end{aligned}$$

as desired. □

According to Lemma 3.1, in order to encrypt an image using Essaid *et al.*'s scheme is enough to know the secret values $a$, $c$ and $\alpha_i$, for $i \in [0, HW)$. As a consequence, we can also decrypt using these values.

**Corollary 3.1.1.** *We can recover $P_i$ using*

$$P_i \equiv a^{-1}(C_i - a\sum_{j=0}^{i-1} c^{i-j}P_j - \alpha_i) \bmod 256.$$

A more efficient method for decrypting is given in the following lemma.

**Corollary 3.1.2.** *We can recover $P_i$ using*

$$P_i \equiv a^{-1}(C_i - \gamma_i - \alpha_i) \bmod 256,$$

*where* $\gamma_0 = 0$ *and*

$$\gamma_i \equiv acP_{i-1} + c\gamma_{i-1} \bmod 256.$$

# 4 CHOSEN PLAINTEXT ATTACK

A chosen plaintext attack (CPA) is a scenario in which the attacker $A$ briefly gains access to the encryption machine $O_{enc}$ and is permitted to query it with various inputs. In this way, $A$ generates specific plaintexts that can facilitate his attack and uses $O_{enc}$ to obtain the corresponding ciphertexts. We demonstrate in this paper that Essaid *et al.*'s image encryption scheme is vulnerable to such attacks.

Lets assume that we query $O_{enc}$ with two plaintexts $P$ and $P'$ and receive $C$ and $C'$, respectively. According to Lemma 3.1 we have

$$\begin{aligned} C_0 &\equiv aP_0 + \alpha_0 \bmod 256, \\ C'_0 &\equiv aP'_0 + \alpha_0 \bmod 256. \end{aligned}$$

Therefore, if $\gcd(P_0 - P'_0, 256) = 1$ then we can recover $a$ using

$$a \equiv (C_0 - C'_0)(P_0 - P'_0)^{-1} \bmod 256,$$

and $\alpha_0$ from

$$\alpha_0 \equiv C'_0 - aP'_0 \bmod 256. \quad (1)$$

Using Lemma 3.1 we also obtain

$$\begin{aligned} C_1 &\equiv aP_1 + acP_0 + \alpha_1 \bmod 256, \\ C'_1 &\equiv aP'_1 + acP'_0 + \alpha_1 \bmod 256, \end{aligned}$$

and since we already computed $a$ we can rewrite the equations as

$$\begin{aligned} C_1 - aP_1 &\equiv acP_0 + \alpha_1 \bmod 256, \\ C'_1 - aP'_1 &\equiv acP'_0 + \alpha_1 \bmod 256. \end{aligned}$$

Therefore, we can recover $c$ using

$$c \equiv (C_1 - aP_1 - C'_1 + aP'_1) \cdot a^{-1}(P_0 - P'_0)^{-1} \bmod 256,$$

since $\gcd(a, 256) = \gcd(P_0 - P'_0, 256) = 1$. Also, $\alpha_1$ is computed as follows

$$\alpha_1 \equiv C'_1 - aP'_1 - acP'_0 \bmod 256. \quad (2)$$

Once $a$ and $c$ are computed, the remaining $\alpha_i$ are computed from

$$\alpha_i \equiv C'_i - a\sum_{j=0}^{i} c^{i-j}P'_j \bmod 256. \quad (3)$$

In order to optimize the recovery of the secret values, we choose two plaintexts such that $P_0 = 1$ and $P_1 = \ldots = P_{HW-1} = P'_0 = \ldots = P'_{HW-1} = 0$. Therefore, we obtain the following relations

$$\begin{aligned} a &\equiv C_0 - C'_0 \bmod 256, \\ c &\equiv a^{-1}(C_1 - C'_1) \bmod 256, \\ \alpha_i &\equiv C'_i \bmod 256, \text{ for } i \in [0, HW). \end{aligned}$$

We can easily see that the complexity of our attack is constant and is dominated by computing an inverse and a multiplication modulo 256. Therefore, it is very efficient.

# 5 CHOSEN CIPHERTEXT ATTACK

In contrast to a chosen plaintext attack, a chosen ciphertext attack (CCA) assumes that the attacker $A$ briefly gains access to the decryption machine $O_{dec}$. $A$ then generates specific ciphertexts that can assist his attack and uses $O_{dec}$ to obtain the corresponding plaintexts. In this scenario, we describe an attack on Essaid *et al.*'s cryptosystem.

Lets assume that we query $O_{dec}$ with two ciphertexts $C$ and $C'$ and receive $P$ and $P'$, respectively. Using Corollary 3.1.1 we obtain

$$P_0 \equiv a^{-1}(C_0 - \alpha_0) \bmod 256,$$
$$P'_0 \equiv a^{-1}(C'_0 - \alpha_0) \bmod 256.$$

Therefore, if $\gcd(C_0 - C'_0, 256) = 1$ then we can recover $a^{-1}$ using

$$a^{-1} \equiv (P_0 - P'_0)(C_0 - C'_0)^{-1} \bmod 256.$$

Applying Corollary 3.1.1 to the second byte we obtain

$$P_1 \equiv a^{-1}(C_1 - acP_0 - \alpha_1) \bmod 256,$$
$$P'_1 \equiv a^{-1}(C'_1 - acP'_0 - \alpha_1) \bmod 256,$$

and since we already computed $a^{-1}$ we can rewrite the equations as

$$a^{-1}C_1 - P_1 \equiv cP_0 + a^{-1}\alpha_1 \bmod 256,$$
$$a^{-1}C'_1 - P'_1 \equiv cP'_0 + a^{-1}\alpha_1 \bmod 256.$$

Note that since $\gcd(a, 256) = \gcd(C_0 - C'_0, 256) = 1$, we obtain that $\gcd(P_0 - P'_0, 256) = 1$. Therefore, we can recover $c$ using

$$c \equiv (a^{-1}C_1 - P_1 - a^{-1}C'_1 + P'_1) \cdot (P_0 - P'_0)^{-1} \bmod 256.$$

Once $a$ and $c$ are computed, the $\alpha_i$ values are computed using Equations (1) to (3).

In order to optimize the recovery of the secret values, we choose two ciphertexts such that $C_0 = 1$ and $C_1 = \ldots = C_{HW-1} = C'_0 = \ldots = C'_{HW-1} = 0$. Therefore, we obtain the following relations

$$a \equiv (P_0 - P'_0)^{-1} \bmod 256,$$
$$c \equiv a(P'_1 - P_1) \bmod 256,$$
$$\alpha_i \equiv -a \sum_{j=0}^{i} c^{i-j} P'_j \bmod 256, \text{ for } i \in [0, HW). \quad (4)$$

Note that Equation (4) can be rewritten as

$$\alpha_0 \equiv -aP'_0 \bmod 256,$$
$$\alpha_i \equiv -aP'_i + c\alpha_{i-1} \bmod 256, \text{ for } i \in [1, HW).$$

The complexity of our attack dominated by two inverses and $2HW$ multiplications modulo 256. Using the fact that an inverse and a multiplication modulo 256 has constant complexity $O(1)$, we obtain that our attack has a complexity of $O(2HW)$. For example, if we encrypt 2 megapixels[1] images we obtain a complexity of $O(2^{21.87})$. In the case of 12 megapixels[2], we obtain $O(2^{24.51})$.

[1] $W \times H = 1600 \times 1200$

[2] $W \times H = 4000 \times 3000$

# 6 CONCLUSIONS

The authors of (Essaid et al., 2019b) presented an image encryption scheme that they claimed to have a security strength of 279 bits. However, our research in this paper demonstrated that the actual security strength of Essaid *et al.*'s scheme is essentially 0 bits. To establish our security bound, we designed a chosen plaintext attack that requires only 2 queries to the encryption oracle. Furthermore, we outline a chosen ciphertext attack that requires 2 queries to the decryption oracle and has a complexity of roughly $O(2^{24})$.

# REFERENCES

Alanazi, A. S., Munir, N., Khan, M., Asif, M., and Hussain, I. (2021). Cryptanalysis of Novel Image Encryption Scheme Based on Multiple Chaotic Substitution Boxes. *IEEE Access*, 9:93795–93802.

Arroyo, D., Diaz, J., and Rodriguez, F. (2013). Cryptanalysis of a One Round Chaos-Based Substitution Permutation Network. *Signal Processing*, 93(5):1358–1364.

Chen, J., Chen, L., and Zhou, Y. (2020). Cryptanalysis of a DNA-Based Image Encryption Scheme. *Information Sciences*, 520:130–141.

Chen, J.-x., Zhu, Z.-l., Fu, C., Zhang, L.-b., and Zhang, Y. (2015). An Efficient Image Encryption Scheme Using Lookup Table-Based Confusion and Diffusion. *Nonlinear Dynamics*, 81(3):1151–1166.

Essaid, M., Akharraz, I., Saaidi, A., and Mouhib, A. (2019a). A New Approach of Image Encryption Based on Dynamic Substitution and Diffusion Operations. In *SysCoBIoTS 2019*, pages 1–6. IEEE.

Essaid, M., Akharraz, I., Saaidi, A., and Mouhib, A. (2019b). Image Encryption Scheme Based on a New Secure Variant of Hill Cipher and 1D Chaotic Maps. *Journal of Information Security and Applications*, 47:173–187.

Fan, H., Zhang, C., Lu, H., Li, M., and Liu, Y. (2021). Cryptanalysis of a New Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps. *Entropy*, 23(12):1581.

Hosny, K. M. (2020). *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, volume 884. Springer.

Hu, G., Xiao, D., Wang, Y., and Li, X. (2017). Cryptanalysis of a Chaotic Image Cipher using Latin Square-Based Confusion and Diffusion. *Nonlinear Dynamics*, 88(2):1305–1316.

Hua, Z. and Zhou, Y. (2017). Design of Image Cipher Using Block-Based Scrambling and Image Filtering. *Information sciences*, 396:97–113.

Huang, X., Sun, T., Li, Y., and Liang, J. (2014). A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System. *Entropy*, 17(1):28–38.

Khan, M. (2015). A Novel Image Encryption Scheme Based on Multiple Chaotic S-Boxes. *Nonlinear Dynamics*, 82(1):527–533.

Khan, M. and Masood, F. (2019). A Novel Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps. *Multimedia Tools and Applications*, 78(18):26203–26222.

Li, M., Lu, D., Wen, W., Ren, H., and Zhang, Y. (2018). Cryptanalyzing a Color Image Encryption Scheme Based on Hybrid Hyper-Chaotic System and Cellular Automata. *IEEE access*, 6:47102–47111.

Li, M., Lu, D., Xiang, Y., Zhang, Y., and Ren, H. (2019a). Cryptanalysis and Improvement in a Chaotic Image Cipher Using Two-Round Permutation and Diffusion. *Nonlinear Dynamics*, 96(1):31–47.

Li, M., Wang, P., Liu, Y., and Fan, H. (2019b). Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. *IEEE Access*, 7:145798–145806.

Li, M., Wang, P., Yue, Y., and Liu, Y. (2021). Cryptanalysis of a Secure Image Encryption Scheme Based on a Novel 2D Sine–Cosine Cross-Chaotic Map. *Journal of Real-Time Image Processing*, 18(6):2135–2149.

Li, S. and Zheng, X. (2002). Cryptanalysis of a Chaotic Image Encryption Method. In *ISCAS 2002*, volume 2, pages 708–711. IEEE.

Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., and Miao, S. (2018). Image Block Encryption Algorithm Based on Chaotic Maps. *IET Signal Processing*, 12(1):22–30.

Liu, Y., Qin, Z., Liao, X., and Wu, J. (2020). Cryptanalysis and Enhancement of an Image Encryption Scheme Based on a 1-D Coupled Sine Map. *Nonlinear Dynamics*, 100(3):2917–2931.

Ma, Y., Li, C., and Ou, B. (2020). Cryptanalysis of an Image Block Encryption Algorithm Based on Chaotic Maps. *Journal of Information Security and Applications*, 54:102566.

Matoba, O. and Javidi, B. (2004). Secure Holographic Memory by Double-Random Polarization Encryption. *Applied Optics*, 43(14):2915–2919.

Mondal, B., Behera, P. K., and Gangopadhyay, S. (2021). A Secure Image Encryption Scheme Based on a Novel 2D Sine–Cosine Cross-Chaotic (SC3) Map. *Journal of Real-Time Image Processing*, 18(1):1–18.

Muthu, J. S. and Murali, P. (2021). Review of Chaos Detection Techniques Performed on Chaotic Maps and Systems in Image Encryption. *SN Computer Science*, 2(5):1–24.

Niyat, A. Y., Moattar, M. H., and Torshiz, M. N. (2017). Color Image Encryption Based on Hybrid Hyper-Chaotic System and Cellular Automata. *Optics and Lasers in Engineering*, 90:225–237.

Özkaynak, F. (2018). Brief Review on Application of Nonlinear Dynamics in Image Encryption. *Nonlinear Dynamics*, 92(2):305–313.

Pak, C., An, K., Jang, P., Kim, J., and Kim, S. (2019). A Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map. *Multimedia Tools and Applications*, 78(9):12027–12042.

Pak, C. and Huang, L. (2017). A New Color Image Encryption Using Combination of the 1D Chaotic Map. *Signal Processing*, 138:129–137.

Shafique, A. and Shahid, J. (2018). Novel Image Encryption Cryptosystem Based on Binary Bit Planes Extraction and Multiple Chaotic Maps. *The European Physical Journal Plus*, 133(8):1–16.

Sheela, S., Suresh, K., and Tandur, D. (2018). Image Encryption Based on Modified Henon Map Using Hybrid Chaotic Shift Transform. *Multimedia Tools and Applications*, 77(19):25223–25251.

Song, C. and Qiao, Y. (2015). A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. *Entropy*, 17(10):6954–6968.

Teşeleanu, G. (2023). Security Analysis of a Color Image Encryption Scheme Based on Dynamic Substitution and Diffusion Operations. In *ICISSP 2023*. SCITEPRESS.

Wang, H., Xiao, D., Chen, X., and Huang, H. (2018). Cryptanalysis and Enhancements of Image Encryption Using Combination of the 1D Chaotic Map. *Signal processing*, 144:444–452.

Wang, L., Wu, Q., and Situ, G. (2019). Chosen-Plaintext Attack on the Double Random Polarization Encryption. *Optics Express*, 27(22):32158–32167.

Wang, X., Teng, L., and Qin, X. (2012). A Novel Colour Image Encryption Algorithm Based on Chaos. *Signal Processing*, 92(4):1101–1108.

Wen, H. and Yu, S. (2019). Cryptanalysis of an Image Encryption Cryptosystem Based on Binary Bit Planes Extraction and Multiple Chaotic Maps. *The European Physical Journal Plus*, 134(7):1–16.

Wen, H., Yu, S., and Lü, J. (2019). Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. *Entropy*, 21(3):246.

Wen, H., Zhang, C., Huang, L., Ke, J., and Xiong, D. (2021). Security Analysis of a Color Image Encryption Algorithm Using a Fractional-Order Chaos. *Entropy*, 23(2):258.

Wu, J., Liao, X., and Yang, B. (2018). Image Encryption Using 2D Hénon-Sine Map and DNA Approach. *Signal processing*, 153:11–23.

Yen, J.-C. and Guo, J.-I. (2000). A New Chaotic Key-Based Design for Image Encryption and Decryption. In *ISCAS 2000*, volume 4, pages 49–52. IEEE.

Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M., and Jafari Barani, M. (2019). Digital Image Scrambling Based on a New One-Dimensional Coupled Sine Map. *Nonlinear Dynamics*, 97(4):2693–2721.

Yu, F., Gong, X., Li, H., and Wang, S. (2021). Differential Cryptanalysis of Image Cipher Using Block-Based Scrambling and Image Filtering. *Information Sciences*, 554:145–156.

Zhou, K., Xu, M., Luo, J., Fan, H., and Li, M. (2019). Cryptanalyzing an Image Encryption Based on a Modified Henon Map Using Hybrid Chaotic Shift Transform. *Digital Signal Processing*, 93:115–127.

Zolfaghari, B. and Koshiba, T. (2022). Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. *Applied System Innovation*, 5(3):57.