Mansoura Journal for Computer and Information Sciences (2024), Vol.**19**, No.**1**
doi:10.21608/mjcis.2024.286388.1003

Mansoura Journal for Computer and Information Sciences

ARTICLE

On Cryptanalysis Techniques in Chaos-based Cryptography

Wafaa Salaheldin,[*,1] Muhammad H. Zayyan,[1] and Ibrahim Mahmoud El-Henawy[2]

[1]Department of Computer Science, Faculty of Computers and Information Sciences, Mansoura University, Mansoura, Egypt
[2]Department of Computer Science, Faculty of Computers and Informatics, Zagazig University, Zagazig, Egypt

*Corresponding author: aawafaaj12@gmail.com

(Received: 6 May 2024; Accepted: 29 September 2024; Published: 5 October 2024)

Abstract

Since the 1990s, many chaos-based ciphers have been proposed and claimed to be secure by their designers. The designers of these ciphers usually use a set of statistical tests to manifest their security claims. It has been indicated that the commonly used statistical tests are insufficient to evaluate the security of these ciphers. Due to their inadequate cryptanalysis in the design stage, many of these ciphers reportedly have shown weaknesses in relatively simple attack scenarios and were broken in subsequent publications. This paper will investigate an evaluation methodology that appeared recently in chaos-based cryptography literature. The inadequacy of this methodology is demonstrated by presenting attacks on ciphers that pass this test. The attacks presented are of the same kind as those to which the suggested test is supposed to manifest a cipher's resistance. Hence, we concluded that the suggested test is unsuitable for showing a cipher's resistance to these attacks.

Keywords: Cryptanalysis; image encryption; chosen-plaintext attack; known-plaintext attack; chaos-based cryptography

1. Introduction

1.1 Security and cryptography

Security is a vital part of communication [1]. People want the messages they send to be secret and the messages they receive to be authenticated. Services such as digital banking and online trading were not feasible without security.

Cryptography is the main tool to provide security services such as confidentiality, integrity, and authentication in cyberspace [2]. To attain these services primitives such as ciphers, hash functions, message authentication codes, and digital signatures are deployed [2].

Before modern times, cryptography was mainly an interest of political and military sectors. However, with the rise of the internet and other digital services, the need for it has become part of everyday life.

1.2 Encryption

A fundamental problem in cryptography is to help two parties, usually named Alice and Bob, to communicate over an insecure channel without allowing a third party who eavesdrops on the channel, usually named Eve, to read their messages, as illustrated in Figure 1. Alice, Bob, and Eve are fictional characters originally invented to facilitate the communication of cryptographic concepts.

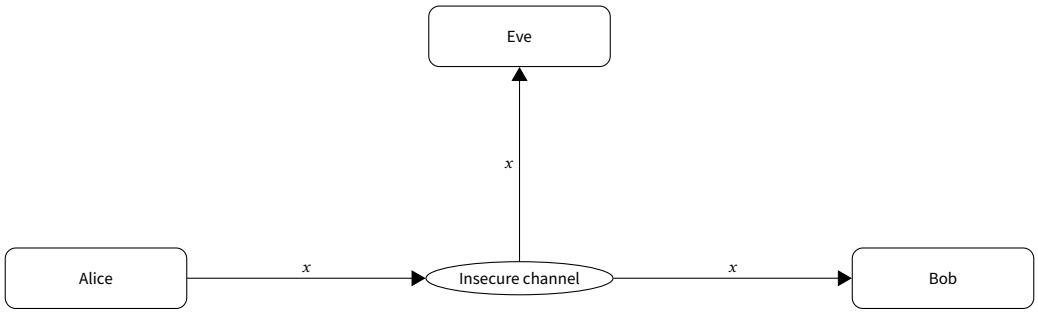

Figure 1. Communication over an insecure channel: Alice sends a message, x, to Bob while Eve is eavesdropping [3].

The eavesdropping problem is solved via encryption using a cipher/cryptosystem [3]. A secret key is selected from the cipher's keyspace (a large set of all possible keys for the cipher) and shared securely between Alice and Bob. At some later time, when Alice wants to send a message to Bob, they utilize the cipher via the following steps [3]:

1. Alice encrypts the message, named plaintext, using the cipher based on the secret key to get an unrecognizable message, named ciphertext, which is sent over the channel.
2. Upon receiving the ciphertext, Bob can invert it to the original message using the cipher and the possessed secret key.

For ciphers that provide the required security, the ciphertext cannot be inverted to the original message by parties that do not possess the secret key. Hence, Eve cannot extract the original message when she catches the ciphertext due to the lack of this key. This process is illustrated in Figure 2. We considered symmetric-key cryptosystems where the same key is used for encryption and decryption operations as opposed to asymmetric-key cryptosystems where different keys are used.

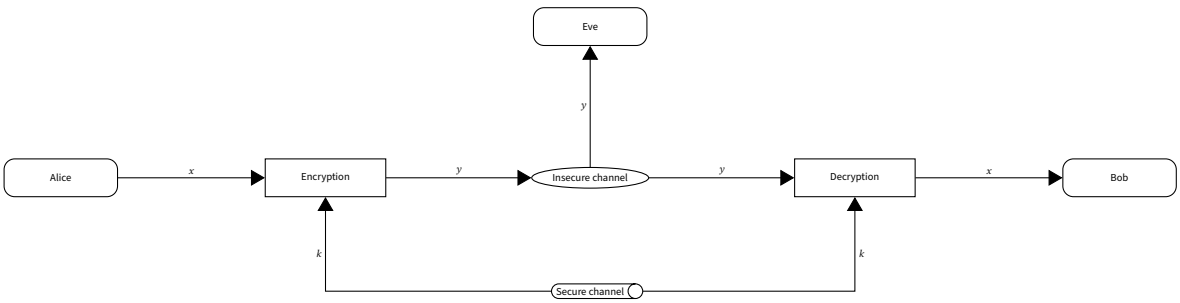

Figure 2. Symmetric-key encryption: Alice encrypts a plaintext, x, to a ciphertext, y, using a cipher and a secret key, k, before sending it to Bob who can reverse the process to get the plaintext [3].

1.3 Cryptanalysis

It is common to define cryptography to be the science of secure communications in the presence of an adversary. As adversaries are the main threat in cryptography, the need to estimate ciphers' ability to withstand their attacks is urgent.

Cryptanalysis is used to evaluate the security of cryptographic primitives [4]. It is used to break ciphers, find their weaknesses, or display their strength. Thus, cryptanalysis has a fundamental and continuous rule in the processes of designing cryptographic primitives. The more a cipher is analyzed and withstands attacks, the more credibility it gains. If the intention is to attack a cipher, then the goal could be to recover some plaintexts or even the key.

To have a cryptosystem analyzed as much as possible, it is recommended to publish its details. A fundamental assumption in cryptography is Kerckhoffs's principle [2, 1]. The origin of this principle is Kerckhoffs's 1883 essay "Cryptographie Militaire" in which he stated that [5]:

"The system must not require secrecy and
can be stolen by the enemy without causing trouble."

Lately, Shannon expressed this principle by saying: "The enemy knows the system." Consequently, it requires that the security of a cipher does not depend on the secrecy of its specifications, and only the key is required to be secret. Therefore, it should be assumed that the cipher is public when its security analysis is performed [6].

A straightforward attack on any cipher is to try the keys in its keyspace subsequently until the right key used for encryption is found; this attack is named the brute-force attack or exhaustive key search [3]. A large keyspace is essential to withstand this attack, however, this is a necessary, not sufficient, condition for security. A cipher would be considered weak if there is a feasible shortcut attack.

According to the data used in attacks, they are divided mainly into the following four models [2]:

1. **Ciphertext-only attack:** the attacker has a set of ciphertexts.
2. **Known-plaintext attack:** the attacker has a set of ciphertexts and their corresponding plaintexts.
3. **Chosen-plaintext attack:** the attacker has temporary access to the encryption machinery, then he obtains the set of ciphertexts corresponding to plaintexts of his choice.
4. **Chosen-ciphertext attack:** the attacker has temporary access to the decryption machinery, then he obtains the set of plaintexts corresponding to ciphertexts of his choice.

Attackers will try to break a cipher using the knowledge of its specifications and available data.

Ciphertext-only attacks are common in classical ciphers by exposing the statistical properties of ciphertexts. Examples of chosen-plaintext attacks and known-plaintext attacks are differential cryptanalysis and linear cryptanalysis, respectively. The chosen-ciphertext attack scenario has particular importance in asymmetric cryptography.

1.4 Chaos theory

Chaos theory is the study of deterministic dynamical systems that have special characteristics. These dynamical systems have a sensitive dependence on initial conditions and possess aperiodic and bounded orbits [7].

Examples of dynamical systems that exhibit chaotic behavior include the logistic map and the Henon map [7]. The logistic map is a 1D difference equation given by

$$x_{i+1} = rx_i(1 - x_i), \quad \text{for} \quad i = 0, 1, 2, \ldots, \tag{1}$$

where x_i, the ith element in the sequence, is between 0 and 1, x_0 is an initial condition, and $r \in [0, 4]$ is a parameter. As varying r, the system alternates between chaotic behavior and other more stable behaviors. An example of a point that leads to chaotic behavior is $r = 4$. Figure 3 depicts two orbits of the logistic map with $r = 4$ and slightly different initial conditions.

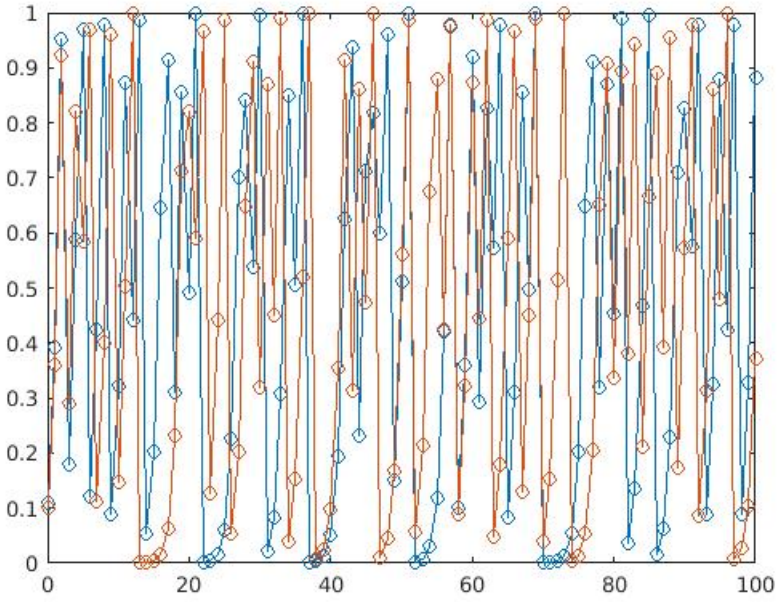

Figure 3. Two orbits of the logistic map with $r = 4$ and slightly different initial conditions.

Two things can be seen in Figure 3:

1. The orbits are scattered on the interval $[0, 1]$ with no noticed periodicity.
2. Although the initial conditions are nearby, they lead to completely different orbits.

It was noted that some properties of chaotic systems such as mixing and sensitivity resemble properties of cryptographic primitives [8]. This drew the attention of many researchers to the possibility of using chaotic systems for building cryptographic primitives [8].

1.5 Chaos-based image encryption

As a suggested way to build cryptographic primitives, applying chaos theory to cryptography emerged to the surface around 1990 [9, 10]. Cryptanalysis of some chaos-based ciphers was published just after their suggestion [11, 12]. Since then, chaos-based cryptography has attracted the attention of many physicists and engineers [13].

A popular suggested application of chaos theory to cryptography is chaos-based image encryption where chaos-based ciphers are dedicated to images [14, 15]. Chaos-based image encryption is mainly motivated by "the unsuitability of ciphers like the Advanced Encryption Standard (AES) for image encryption, and that images need special treatment due to their characteristics," however, this motivation was depreciated [16].

Due to designers' inadequate cryptanalysis [16, 17], many of these ciphers reportedly have been broken in subsequent publications [16]. This inadequacy is mainly embodied by the common prac-

tice of evaluating the security of a cipher by obtaining some statistical measures of ciphertexts [16]. These measures are solely dependent on the statistics of ciphertexts, and this does not reflect the attacker's possible use of knowing the cipher's details, due to Kerckhoffs's principle, to break it [16].

1.6 Organization

In this paper, we investigate a misinterpretation of the chosen-plaintext attack model, which adds to the inadequacy of chaos-based cryptanalysis. This misinterpretation appeared recently in some proposals in the literature of chaos-based image encryption. We are concerned only with digital, symmetric-key systems.

This paper is organized as follows. In Section 2, we will survey some related work. In Section 3, an interpretation of the chosen-plaintext attack model from chaos-based cryptography literature is presented. Then, as a demonstration, we will present attacks on ciphers in Sections 4 and 5. Finally, Section 6 concludes the paper.

2. Related work

2.1 Proposals and their cryptanalysis

Many proposals of chaos-based cryptographic primitives have appeared in the literature over the recent decades. These primitives include stream ciphers, block ciphers, hash functions, and some examples of public-key primitives [18, 19, 20]. Many cryptanalysis instances of these chaos-based proposals followed their publication [8, 21, 17].

Many proposed chaos-based ciphers are dedicated to image encryption [22, 14]. The interest in chaos-based ciphers dedicated to images is usually motivated by the claim that "images have special characteristics (e.g., redundancy and high correlation between adjacent pixels) and require special treatment" [16].

One of the most popular designs of chaos-based image encryption ciphers, which influenced many image encryption proposals [23], is due to J. Fridrich [24]. Reports of its cryptanalysis are provided in [25] and more recently in [26]. In addition, many proposals of chaos-based image encryption systems were suggested [27, 28, 29, 30], and reports of cryptanalysis and indications of flaws were published [31, 32, 33, 34, 8, 21]. Recently, more proposals were suggested [35, 36, 37, 38], and reports of cryptanalysis and indications of repeated flaws were published [39, 40, 41, 42, 43, 44, 45, 20, 16, 46]. Reported cryptanalysis and indications of weaknesses in two similar chaos-based image encryption cryptosystems were provided [47]. Chaos-based image encryption ciphers were reviewed in [22, 48, 49].

The criticism of weak designing (see Section 2.2.2), flawed designing (see Section 2.2.3), and insufficient evaluation (see Section 2.3) are not absent regarding the chaos-based proposals. Moreover, the common motivation behind chaos-based image encryption ciphers was depreciated [16].

2.2 Studies on chaos-based cryptography and image encryption

2.2.1 Studies

Many trials to provide "rigorous" studies on chaos-based cryptography in general, and on chaos-based image encryption in particular, have been published over the last three decades. These studies covered many aspects of applying chaos theory to cryptography. Examples of the covered aspects include:

1. The relationship between chaos theory and cryptography [50, 18, 8, 51].

2. The mathematical and numerical study of chaos theory as a basis for cryptographic applications [52, 18, 53, 54, 55, 56, 13, 57].
3. The cryptanalysis of chaos-based cryptosystems and the indication of their flaws (see Sections 2.2.2 and 2.2.3, respectively).
4. Guidelines and road maps to build chaos-based cryptosystems (see Section 2.2.4).

In the following, we will consider some of these aspects in more detail.

2.2.2 Cryptanalysis

It was repeatedly indicated that many chaos-based ciphers are very weak [17], and many of the chaos-based proposals were broken in subsequent publications by attacks that could be extended to similar proposals [16].

Surveys on the cryptanalysis of some chaos-based cryptosystems were provided in [17, 21, 8, 58]. The power of algebraic attacks on some chaos-based ciphers was investigated in [17] where the algebraic weaknesses of these ciphers were indicated. Furthermore, wider coverage of the cryptanalysis of chaos-based cryptosystems and review of reported instances was presented in [21, 8, 58] where some advice to build chaos-based encryption cryptosystems was provided based on these analyses.

In contrast to the analysis of individual ciphers, studies on the security of specific classes of cryptosystems and mechanisms were considered in [59, 44, 45], and the security of permutation-only cryptosystems was considered in [60, 61, 62].

Insufficient security evaluation of proposed chaos-based cryptosystems in the designing stage is a basic reason behind the cryptographic weaknesses of these systems (see Section 2.3).

2.2.3 Indication of flaws

In addition to cryptographic weaknesses (see Section 2.2.2), it is noted that some chaos-based cryptosystems are basically flawed [17], and indications of some flaws of these systems or their designing process are provided in [21, 8, 58, 20]. Here are some of the flaws summarized in [21, 8, 58, 20]:

1. Lack of details of the system.
2. The keyspace justification is flawed or absent.
3. Vagueness of the finite-precision specifications.
4. Highly complex or ad hoc designs.
5. The encryption procedure is non-invertible.
6. Low efficient cryptosystems or lack of efficiency analysis.
7. The cryptosystem's efficiency is dependent on the key's value.
8. Dynamical degradation of chaotic systems.
9. Dependency on statistical tests.

In the more recent investigation [20], the authors revisited flaws that were indicated more than a decade before and pointed out that recently published work still does not address these flaws.

2.2.4 Guidelines

The indicated flaws and cryptographic weaknesses encouraged some researchers to suggest guidelines to remedy them. In chaos-based cryptography literature, there were many trials to draw a road map or to provide guidelines for building chaos-based cryptosystems. These trials are basically driven by the indicated weaknesses and flaws in proposed chaos-based cryptosystems (see Sections 2.2.2 and 2.2.3).

Based on the cryptanalysis of many chaos-based proposals, a suggested list of basic requirements to build cryptosystems based on chaos theory was provided in [8]. Lessons and hints learned from

the cryptanalysis of chaos-based proposals are listed in [21, 58]. Here are some pieces of advice delivered in [21, 8, 58]:

1. The cryptosystem should be exhaustively and rigorously defined.
2. The key and the keyspace should be exhaustively and rigorously defined.
3. The cryptosystem's efficiency should not depend on the key's value.
4. The cryptosystem should have resistance to classical attacks.

Another list of guidelines and a suggested road map were provided in [63] and [22], respectively, and some advice is scattered in the literature [16, 47].

2.3 Depreciating of security evaluation of chaos-based cryptosystems

A major obstacle that hampers chaos-based cryptography's progress, recognition, and application is its inadequate security evaluation methodologies that are commonly utilized by chaos-based cryptographers. This basic point was indicated repeatedly over the last two decades [50, 51, 22, 20, 17, 13, 63, 16, 46, 64].

The negligence of algebraic properties of chaos-based ciphers in favor of statistical tests was criticized in [17], where the author indicated that the commonly used statistical tests used to manifest the strength of chaos-based cryptosystems are insufficient and that algebraic weaknesses inherent in a cipher cannot be hidden by statistics. Moreover, he emphasized how cryptanalysis plays a vital role in the ciphers' design process and how this is crucial for chaos-based cryptography to develop into "a mature field."

Some of the most striking comments on chaos-based cryptography are presented in [46, 16]. The authors indicated the insufficiency of common tests used in chaos-based image encryption proposals for "proving" the strength of a cipher. To validate their point, they experimentally showed that even deliberately chosen insecure ciphers can pass these tests. Moreover, the state of differential and linear cryptanalysis in some of these proposals was criticized [16].

The insufficiency of statistical tests is well known in cryptography [5]. This is clear from the abstract of the NIST's report on its test suite [65], which is popular in the literature of chaos-base cryptography. The abstract of [65] reads: "Statistical testing cannot serve as a substitute for cryptanalysis."

Some commentators indicated that insecure or inefficient ciphers based on chaos theory are due to the designers' insufficient knowledge of cryptography and state-of-the-art cryptanalysis techniques [64, 51]. It was noted recently that a perfect blend between chaos theory and cryptography has not been attained yet [47].

Usually, a chaos-based image encryption proposal is partitioned into three parts: motivation, specification, and evaluation. However, based on the above, these proposals commonly did not present a well-established case regarding these three aspects.

3. Chosen-plaintext attack model in some chaos-based proposals

Ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks mentioned above are general classifications. Attacks could be classified under one of these four attack models according to the type of data required to launch them. Even a brute-force attack could be classified as a known-plaintext attack [4].

Nowadays, resistance against chosen-plaintext attacks is a basic security requirement for a cipher [66]. Using a cipher that withstands these attacks is customary even if such attacks are not feasible in the targeted applications [2].

Many chaos-based ciphers are reportedly broken using a small number of plaintext-ciphertext pairs with a small number of operations [21, 8, 58, 17]. Some of these attacks need black plaintext images among the required data [67, 68]. Then it is used in further analysis to get the key or to crack other ciphertexts. The choice of a black image usually simplifies the analysis by reducing the number of variables.

Some authors considered the ability to withstand chosen-plaintext attacks to be the ability of a cipher to turn a black image and white image into an image of a noise-like appearance and take this as a test of the cipher's ability to withstand these attacks [69]. They may also add the ability to do the same to a gray image. The noise-like appearance is examined using either histograms or some other statistical tests [70]. For example, they consider that the cipher successfully passes the test if the ciphertexts of the three images have uniform histograms [69]. By passing this test, their ciphers are claimed to be able to withstand chosen-plaintext attacks.

The described methodology is an inadequate test. The chosen-plaintext attack model is a scenario in which an attacker can encrypt plaintexts of his choice for further analysis to undermine the cipher's security. Testing the robustness against this attack model cannot be manifested merely by checking the ability of a cipher to convert plaintexts into noise-like ciphertexts. Moreover, even a simple linear cipher could generate ciphertexts that have a noise-like appearance while being vulnerable to chosen-plaintext attacks.

As a simple illustration of the unsuitability of the suggested test, we consider the Linear Congruential Generator (LCG). It is known to be cryptographically insecure against chosen-plaintext attacks and not recommended for cryptographic applications [3, 16, 2, 5]. However, it can turn the three images into noise-like images with uniform histograms as shown in Figure 4.

In the remainder of this paper, we will illustrate how ciphers could pass the suggested test while still vulnerable to this attack model. Moreover, we will show that these ciphers are vulnerable to less demanding known-plaintext attacks because it is apparently tempting to use the suggested test for this attack model. The essence of these attack models should be clear from the presentation.

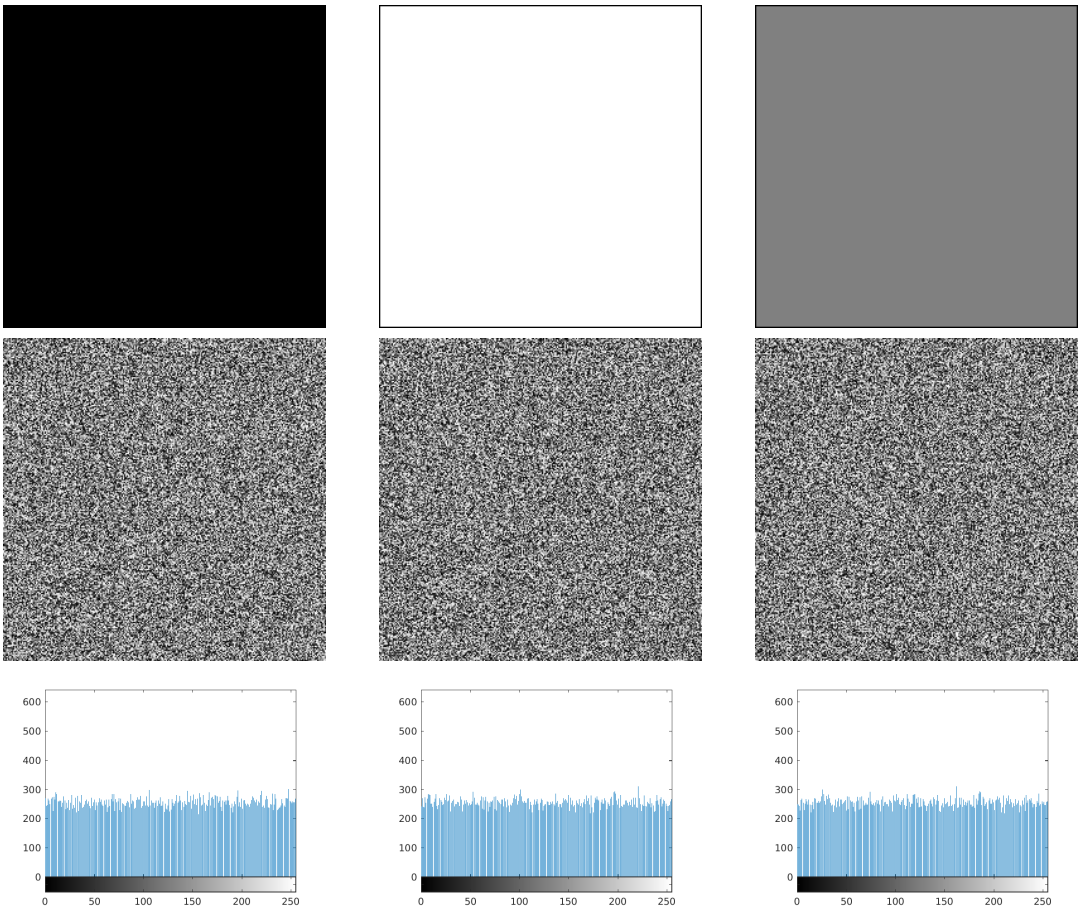

Figure 4. Applying the suggested test to an LCG cipher. For the LCG equation, $x_{i+1} = ax_i + b \mod m$, parameters a, b, and m are taken to be 294967291, 0, and 4294967291, respectively. The binary extension of each iteration is XORed with four pixels.

4. LFSR and the suggested test

In this section, we investigate a deliberately insecure cipher to show its ability to pass the suggested test besides its vulnerabilities.

4.1 LFSR description

A Linear Feedback Shift Register (LFSR) of degree m consists of a series of m flip-flops chained together as in Figure 5 [66, 3]. The flip-flops $F_{m-1}, \ldots, F_1, F_0$ save one bit either one or zero, and they are to be initially filled. An initial fill of the flip-flops and a set of feedback coefficients $p_{m-1}, \ldots, p_1, p_0$ are considered as a key [66]. Each feedback coefficient is set to either 0 or 1 to specify the contribution of the corresponding flip-flop to the feedback. We will consider feedback coefficients that give maximum periods. For the case of feedback coefficients that do not give maximum periods, a variant of the attack described below still applies [66]. Our presentation of LFSRs and the attacks on them adheres to [3].

In each step, the system in Figure 5 transfers from one state to the next as follows:

1. A collection of bits from the flip-flops, according to the feedback coefficient $p_{m-1}, \ldots, p_1, p_0$, are XORed together to compute a feedback bit.
2. The bit in F_0 is taken as an output, and the bits in $F_{m-1}, \ldots, F_1$ are shifted to $F_{m-2}, \ldots, F_0$, respectively, while the feedback bit is fed to F_{m-1}.

Let the flip-flops $F_{m-1}, \ldots, F_1, F_0$ are initially filled with $s_{m-1}, \ldots, s_1, s_0$, respectively. Then the feedback s_m is computed as

$$s_m = s_{m-1}p_{m-1} \oplus \cdots \oplus s_1 p_1 \oplus s_0 p_0,$$

where $\oplus$ stands for the bitwise XOR operation. Next, s_{m+1} is computed as

$$s_{m+1} = s_m p_{m-1} \oplus \cdots \oplus s_2 p_1 \oplus s_1 p_0.$$

In general, the feedback s_{i+m} is computed mathematically as

$$s_{i+m} = \bigoplus_{j=0}^{m-1} p_j s_{i+j}, \quad s_i, p_j \in \{0, 1\}, \ i = 0, 1, 2, \ldots.$$

The ith ciphertext bit y_i is computed by XORing the ith plaintext bit x_i with the ith keystream bit s_i.

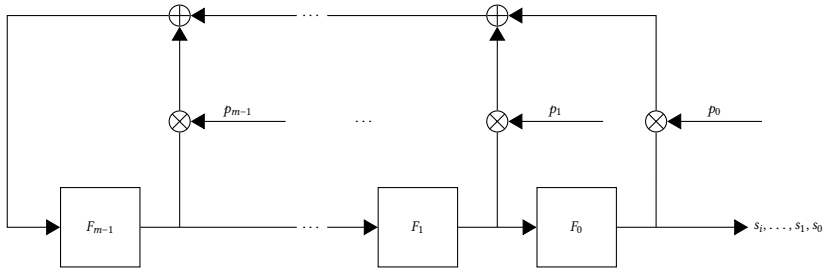

Figure 5. General linear feedback shift register [3].

4.2 Attacking LFSRs

LFSRs could produce streams with good statistical properties. However, a single LFSR cannot provide a strong stream cipher. A known-plaintext attack on LFSR could be launched as follows to get the key [66, 3]:

1. Let the attacker know the first 2m bits from the plaintext $x_0, x_1, \ldots, x_{2m-1}$. Hence, the attacker can compute the first $2m$ bits from the keystream by

$$s_i = x_i \oplus y_i, \quad i = 0, 1, 2, \ldots, 2m - 1.$$

2. Now, the attacker has the first $2m$ bits from the keystream. Using this information, the following linear system can be constructed:

$$\begin{aligned} s_m &= p_{m-1}s_{m-1} \oplus \cdots \oplus p_1 s_1 \oplus p_0 s_0, \\ s_{m+1} &= p_{m-1}s_m \oplus \cdots \oplus p_1 s_2 \oplus p_0 s_1, \\ &\vdots \\ s_{2m-1} &= p_{m-1}s_{2m-2} \oplus \cdots \oplus p_1 s_m \oplus p_0 s_{m-1}. \end{aligned} \tag{2}$$

3. The linear system in equation (2) can be solved efficiently for $p_{m-1}, \ldots, p_1, p_0$.

Hence, the cipher is vulnerable to a known-plaintext attack. This attack implies the cipher's vulnerability to chosen-plaintext attacks. In particular, we could get the required bits from the keystream by encrypting a string of $2m$ bits of zeros.

The initial fill may be considered as a public initialization vector (IV) and be discarded from keystreams. The inclusion of an IV resembles modern synchronous stream ciphers. This alters the generated bits with the same key for different IV values. However, essentially the same attacks described above still apply.

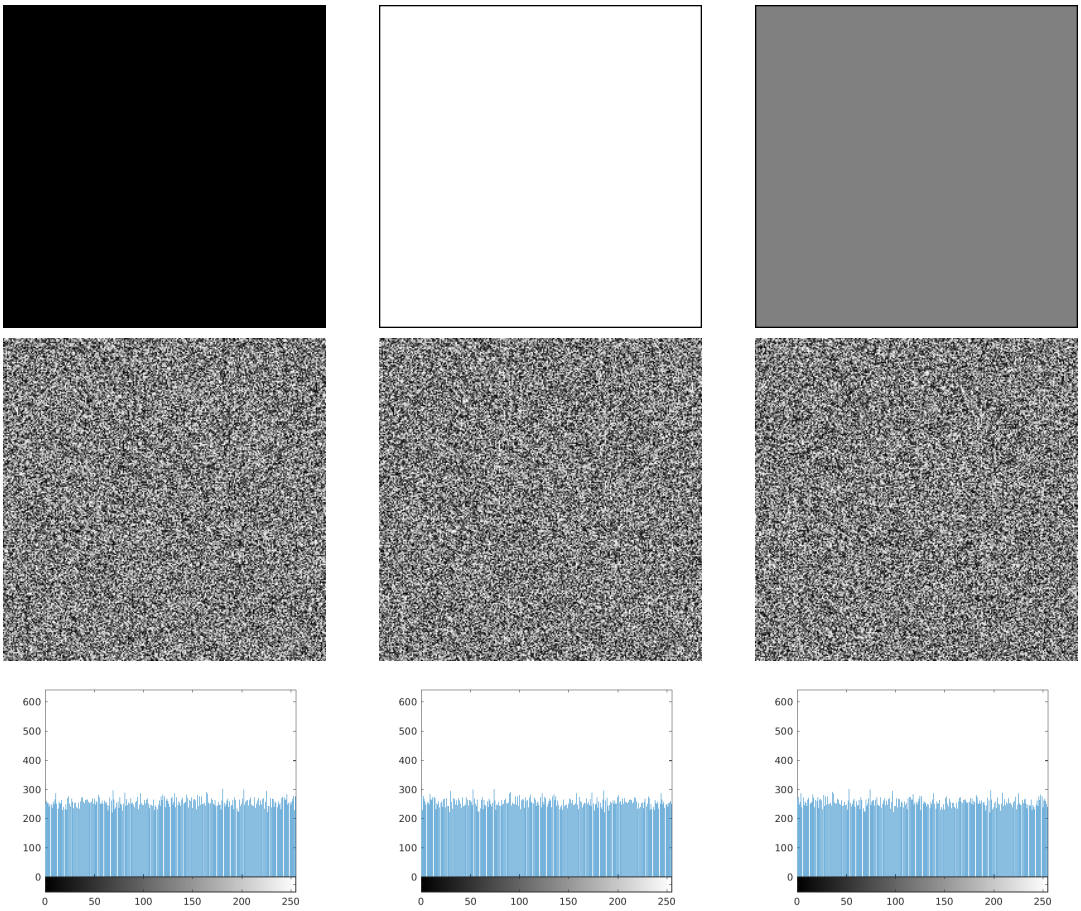

Figure 6. Applying the suggested test to a single LFSR cipher. The LFSR consisted of 21 flip-flops with p_{20}, p_3, and p_0 are set to 1, while $p_i = 0$ for the rest.

4.3 Passing the suggested test

As an illustration, we will use a specific LFSR to encrypt a white image, a gray image, and a black image. Then we will show that it can pass the suggested test, besides its weakness against chosen-plaintext attacks. Starting with three images, black, white, and gray, in the first row of Figure 6, we encrypt them using a single LFSR to get their ciphertexts in the second row, then the histograms of these ciphertexts are computed in the third row. As it is clear from Figure 6, the cipher turns the three images into noise-like images with uniform histograms. Thus, according to the suggested test, a single LFSR can withstand chosen-plaintext attacks. However, as indicated above, LFSRs are vulnerable to this attack model. Hence, the suggested test is not adequate to prove the ability of a

cipher to withstand this attack model. The same applies to the known-plaintext attack model.

5. A chaos-based image encryption cipher and the suggested test

In this section, we investigate a cipher from the literature of chaos-based cryptography to show its ability to pass the suggested test besides its vulnerabilities. However, due to the indicated flawed and vague formation [17, 13] (see Section 2), it could be problematic to consider these systems.

5.1 The cipher specifications

The cryptosystem proposed in [71] is based on the chaotic tent map defined by

$$x_{i+1} = \begin{cases} \mu x_i, & \text{for} \quad x_i < \frac{1}{2}, \\ \mu(1 - x_i), & \text{for} \quad x_i \geq \frac{1}{2}, \end{cases} \quad \text{for} \quad i = 0, 1, 2, \ldots, \tag{3}$$

where $x_i \in [0, 1]$ is the ith element in the sequence, x_0 is an initial condition, and $\mu \in [0, 2]$ is a control parameter. For confidence, we will consider applying the cipher to grayscale images, however, working with color images is a direct tripling of the work.

The encryption process in [71] is described by the following algorithm:

1. Read the plaintext image.
2. Input the secret key x_0. Iterate the tent map in equation (3) N times, where N is the number of the plaintext's pixels.
3. Encrypt each pixel of the original image using the corresponding tent map's iteration.
4. The resulting image in the previous step is the ciphertext.

The encryption step interpretation is similar to that in [72]: the pixels are XORed with the result of

$$\lfloor x_i \times 10^{12} \rfloor \mod 256, \quad \text{for} \quad i = 1, 2, \ldots, N.$$

Figure 7 shows a flowchart of the chaos-based cipher under study. We implemented this cipher in Matlab with double precision representation of floating-point numbers.

5.2 Passing the suggested test

As another illustration, we will apply the suggested test to the chaos-based cipher in [71]. Starting with three images, black, white, and gray, in the first row of Figure 8, we encrypt them using the chaos-based cipher to get their ciphertexts in the second row, then the histograms of these ciphertexts are computed in the third row. As it is clear from Figure 8, the cipher turns the three images into noise-like images with uniform histograms. Thus, according to the suggested test, the cipher in [71] can withstand chosen-plaintext attacks. However, in the following, we will show that the cipher is vulnerable to this attack model and to the known-plaintext attack model.

5.3 Attacking the chaos-based image encryption cipher

This section will apply attacks from two attack models to the chaos-based image encryption cipher. We will illustrate the vulnerability of this cipher against a chosen-plaintext attack and to a less demanding known-plaintext attack. A chosen-plaintext attack on the chaos-based cipher was performed in [72], and some general comments on its cryptanalysis were given in [73]. For the following attacks, we will name the key k and associate it with the array K, which is the whole stream of bits XORed with the plaintext. The goal of each attack is to obtain data equivalent to the key. This data could be used to decrypt other ciphertexts encrypted by the same key k, and the cipher is considered broken.

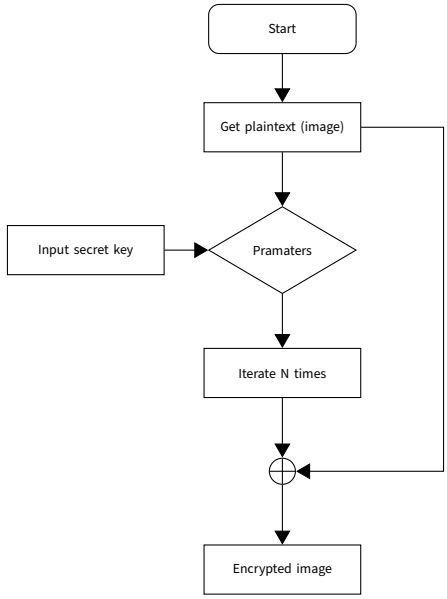

Figure 7. The encryption process of the chaos-based cipher [71].

5.3.1 Chosen-plaintext attack

As a first attack, we will present a chosen-plaintext attack. The attack presented here appeared in [72]. In this attack, we consider a black image B, i.e., an image of all zeros. After the plaintext is encrypted, we get

$$C = B \oplus K,$$

where C is the ciphertext of B. By canceling B, we get $K = C$, which can be used to decrypt other ciphertext C' to get its plaintext P' by

$$P' = C' \oplus K. \tag{4}$$

A simulation of this attack is summarized in Figure 9. The first row contains a plaintext (cameraman image), Figure 9 (a), and its encryption, Figure 9 (b). The second row contains a chosen plaintext (black image), Figure 9 (c), and its encryption, Figure 9 (d). The recovered image (cameraman image) is obtained in Figure 9 (e).

5.3.2 Known-plaintext attack

As a second attack, we will present a known-plaintext attack. The vulnerability of the chaos-based cipher to the known-plaintext attack model was indicated in [73]. In this attack, we use known plaintext-ciphertext pair P and C. The ciphertext is computed as

$$C = P \oplus K.$$

Then, because the plaintext P is known, the array K could be computed by bitwise XORing P with the two sides of the above equation to give $K = C \oplus P$, which can be used to decrypt other ciphertexts according to equation (4).

A simulation of this attack is summarized in Figure 10. The first row contains a plaintext (cameraman image), Figure 10 (a), and its encryption, Figure 10 (b). The second row contains a known plaintext (pepper image), Figure 10 (c), and its encryption, Figure 10 (d). The bitwise XORing of the two

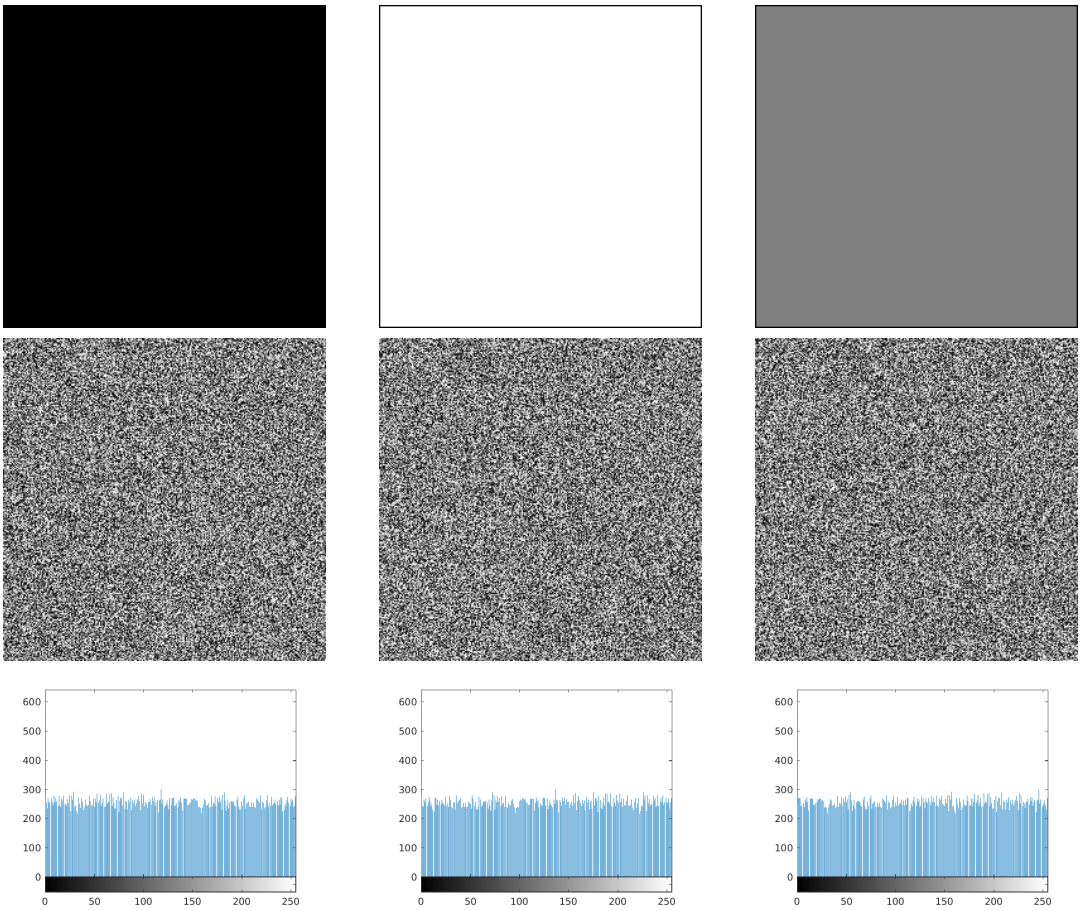

Figure 8. Applying the suggested test to the chaos-based cipher. μ is taken to be 1.999999.

ciphertexts is shown in Figure 10 (e), and the recovered image (cameraman image) is obtained in Figure 10 (f).

Therefore, the cipher in [71] is vulnerable to chosen-plaintext attacks and known-plaintext attacks while being able to pass the suggested test, which indicates the inadequacy of this test to evaluate the ability of a cipher to withstand these attack models.

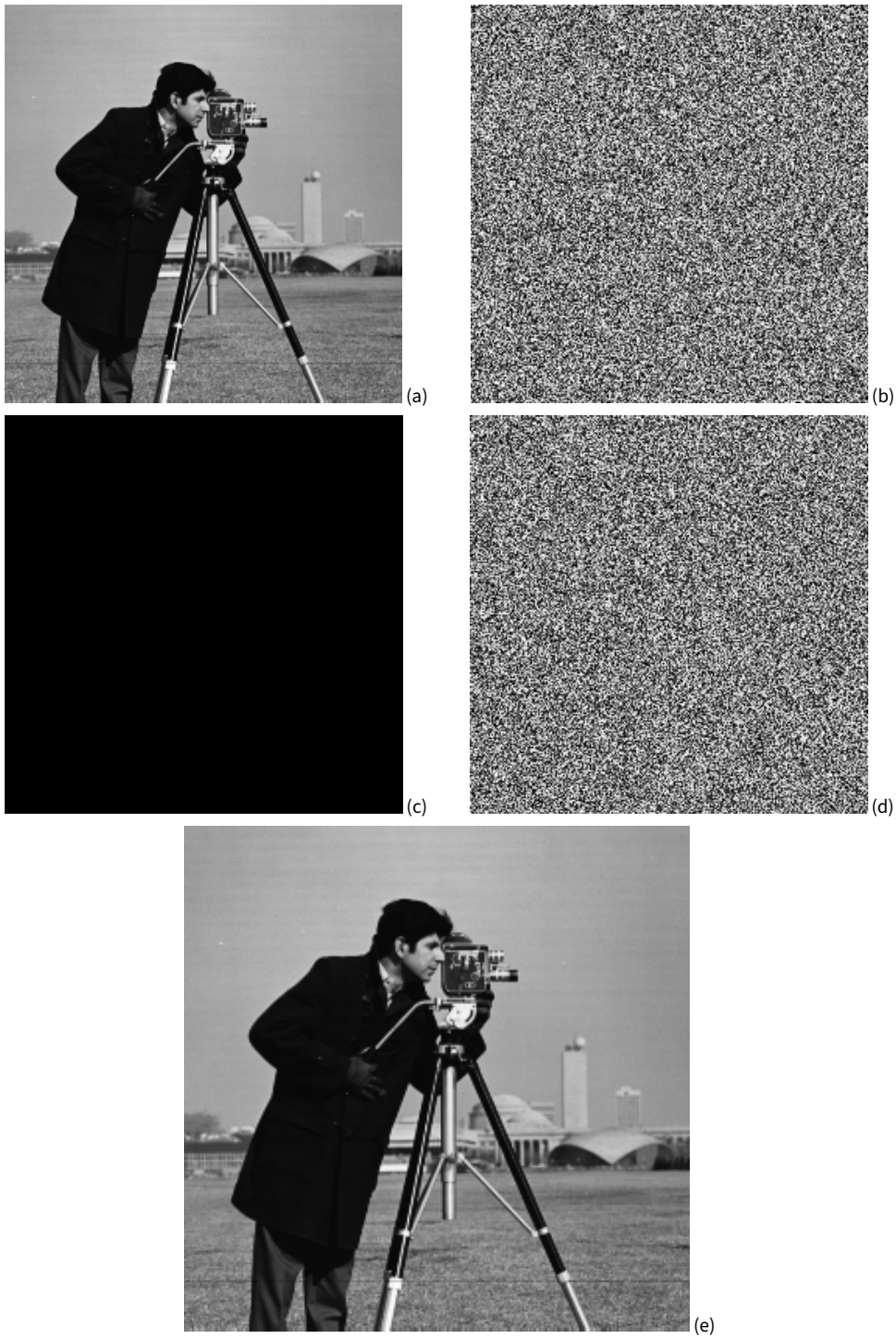

Figure 9. Chosen-plaintext attack on the chaos-based cipher.

Figure 10. Known-plaintext attack on the chaos-based cipher.

6. Conclusion

Cryptanalysis is an integrated and essential part of designing ciphers. In this paper, we investigated a newly suggested test in the literature of chaos-based cryptography. We pointed out the inaccuracies in the investigated test. Finally, we illustrated the inadequacy of this test for its intended measurements by showing ciphers that do not fulfill the measured attribute while passing this test.

Consequently, the designers are encouraged to stop using this test and deploy well-established cryptanalysis techniques.

Open data statement

To replicate the experiments, a black, white, and gray image could be created using Matlab, and the demo images in Matlab, which include the cameraman and pepper images, could be utilized.

References

[1] Henk C. A. van Tilborg and Sushil Jajodia, eds. *Encyclopedia of cryptography and security*. Springer, 2011.

[2] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press, 1997.

[3] Christof Paar, Jan Pelzl, and Tim Güneysu. *Understanding cryptography: a textbook for students and practitioners*. Springer, 2024.

[4] Christopher Swenson. *Modern cryptanalysis: techniques for advanced code breaking*. Wiley, 2008.

[5] Jean-Philippe Aumasson. *Serious cryptography: a practical introduction to modern encryption*. No Starch Press, 2018.

[6] Serge Vaudenay. *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media, 2006.

[7] David P Feldman. *Chaos and fractals: an elementary introduction*. Oxford University Press, 2012.

[8] Gonzalo Alvarez and Shujun Li. "Some basic cryptographic requirements for chaos-based cryptosystems". In: *International journal of bifurcation and chaos* 16.08 (2006), pp. 2129–2151.

[9] Toshiki Habutsu, Yoshifumi Nishio, Iwao Sasase, and Shinsaku Mori. "A secret key cryptosystem by iterating a chaotic map". In: *Advances in Cryptology — EUROCRYPT'91*. Ed. by Donald W. Davies. Springer Berlin Heidelberg, 1991, pp. 127–140.

[10] Robert Matthews. "On the derivation of a "chaotic" encryption algorithm". In: *Cryptologia* 13.1 (1989), pp. 29–42.

[11] Eli Biham. "Cryptanalysis of the chaotic-map cryptosystem suggested at EUROCRYPT'91". In: *Advances in Cryptology — EUROCRYPT'91*. Ed. by Donald W. Davies. Springer Berlin Heidelberg, 1991, pp. 532–534.

[12] Daniel D. Wheeler. "Problems with chaotic cryptosystems". In: *Cryptologia* 13.3 (1989), pp. 243–250.

[13] José María Amigó. "Chaos-based cryptography". In: *Intelligent computing based on chaos*. Ed. by Ljupco Kocarev, Zbigniew Galias, and Shiguo Lian. Springer, 2009, pp. 291–313.

[14] Yaobin Mao and Guanrong Chen. "Chaos-based image encryption". In: *Handbook of Geometric Computing*. Springer Berlin Heidelberg, 2005, pp. 231–265.

[15] Miguel Angel Murillo-Escobar, Manuel Omar Meranza-Castillón, Rosa Martha López-Gutiérrez, and César Cruz-Hernández. "Suggested integral analysis for chaos-based image cryptosystems". In: *Entropy* 21.8, 815 (2019).

[16] Mario Preishuber, Thomas Hütter, Stefan Katzenbeisser, and Andreas Uhl. "Depreciating motivation and empirical security analysis of chaos-based image and video encryption". In: *IEEE Transactions on Information Forensics and Security* 13.9 (2018), pp. 2137–2150.

[17] Ercan Solak. "Cryptanalysis of chaotic ciphers". In: *Chaos-Based Cryptography*. Ed. by Ljupco Kocarev and Shiguo Lian. Springer, 2011, pp. 227–256.

[18] Shujun Li. "Analyses and new designs of digital chaotic ciphers". PhD thesis. Xi'an Jiaotong University, 2003.

[19] Ljupco Kocarev and Shiguo Lian, eds. *Chaos-based cryptography: Theory, algorithms and applications*. Vol. 354. Studies in Computational Intelligence. Springer Science & Business Media, 2011.

[20] Je Sen Teh, Moatsum Alawida, and You Cheng Sii. "Implementation and practical problems of chaos-based cryptography revisited". In: *Journal of Information Security and Applications* 50, 102421 (Feb. 2020).

[21] Gonzalo Alvarez, José María Amigó, David Arroyo, and Shujun Li. "Lessons learnt from the cryptanalysis of chaos-based ciphers". In: *Chaos-Based Cryptography*. Ed. by Ljupco Kocarev and Shiguo Lian. Springer, 2011, pp. 257–295.

[22] Fatih Özkaynak. "Brief review on application of nonlinear dynamics in image encryption". In: *Nonlinear Dynamics* 92 (2018), pp. 305–313.

[23] Chengqing Li, Yun Zhang, and Eric Yong Xie. "When an attacker meets a cipher-image in 2018: A year in review". In: *Journal of Information Security and Applications* 48, 102361 (Oct. 2019).

[24] Jiri Fridrich. "Symmetric ciphers based on two-dimensional chaotic maps". In: *International Journal of Bifurcation and chaos* 8.06 (1998), pp. 1259–1284.

[25] Ercan Solak, Cahit Çokal, Olcay Taner Yildiz, and Türker Biyikoğlu. "Cryptanalysis of Fridrich's chaotic image encryption". In: *International Journal of Bifurcation and Chaos* 20.05 (2010), pp. 1405–1413.

[26] Eric Yong Xie, Chengqing Li, Simin Yu, and Jinhu Lü. "On the cryptanalysis of Fridrich's chaotic image encryption scheme". In: *Signal processing* 132 (2017), pp. 150–154.

[27] Hun-Chen Chen and Jui-Cheng Yen. "A new cryptography system and its VLSI realization". In: *Journal of Systems Architecture* 49.7-9 (2003), pp. 355–367.

[28] Zhi-Hong Guan, Fangjun Huang, and Wenjie Guan. "Chaos-based image encryption algorithm". In: *Physics letters A* 346.1-3 (2005), pp. 153–157.

[29] Xiaojun Tong and Minggen Cui. "Image encryption with compound chaotic sequence cipher shifting dynamically". In: *Image and Vision Computing* 26.6 (2008), pp. 843–850.

[30] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez. "Encryption and decryption of images with chaotic map lattices". In: *Chaos: An Interdisciplinary Journal of Nonlinear Science* 16.3, 033118 (2006).

[31] Shujun Li, Chengqing Li, Guanrong Chen, and Kwok-Tung Lo. "Cryptanalysis of the RCES/RSES image encryption scheme". In: *Journal of Systems and Software* 81.7 (2008), pp. 1130–1143.

[32] Cahit Çokal and Ercan Solak. "Cryptanalysis of a chaos-based image encryption algorithm". In: *Physics Letters A* 373.15 (2009), pp. 1357–1360.

[33] Chengqing Li, Shujun Li, Guanrong Chen, and Wolfgang A. Halang. "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence". In: *Image and Vision Computing* 27.8 (2009), pp. 1035–1039.

[34] Ercan Solak and Cahit Çokal. "Algebraic break of image ciphers based on discretized chaotic map lattices". In: *Information Sciences* 181.1 (2011), pp. 227–233.

[35] Vinod Patidar, NK Pareek, and KK Sud. "A new substitution-diffusion based image cipher using chaotic standard and logistic maps". In: *Communications in Nonlinear Science and Numerical Simulation* 14.7 (2009), pp. 3056–3075.

[36] I. Shatheesh Sam, P. Devaraj, and Raghuvel S. Bhuvaneswaran. "A novel image cipher based on mixed transformed logistic maps". In: *Multimedia tools and applications* 56 (2012), pp. 315–330.

[37] Guodong Ye, Chen Pan, Xiaoling Huang, Zhenyu Zhao, and Jianqing He. "A chaotic image encryption algorithm based on information entropy". In: *International Journal of Bifurcation and Chaos* 28.01, 1850010 (2018).

[38] Lingfeng Liu, Shidi Hao, Jun Lin, Ze Wang, Xinyi Hu, and Suoxia Miao. "Image block encryption algorithm based on chaotic maps". In: *IET Signal Processing* 12.1 (2018), pp. 22–30.

[39] Chengqing Li, Tao Xie, Qi Liu, and Ge Cheng. "Cryptanalyzing image encryption using chaotic logistic map". In: *Nonlinear dynamics* 78 (2014), pp. 1545–1551.

[40] Chengqing Li, Dongdong Lin, Bingbing Feng, Jinhu Lü, and Feng Hao. "Cryptanalysis of a chaotic image encryption algorithm based on information entropy". In: *IEEE Access* 6 (2018), pp. 75834–75842.

[41] Yunling Ma, Chengqing Li, and Bo Ou. "Cryptanalysis of an image block encryption algorithm based on chaotic maps". In: *Journal of Information Security and Applications* 54, 102566 (Oct. 2020).

[42] Yuansheng Liu, Hua Fan, Eric Yong Xie, Ge Cheng, and Chengqing Li. "Deciphering an image cipher based on mixed transformed logistic maps". In: *International Journal of Bifurcation and Chaos* 25.13, 1550188 (2015).

[43] Junxin Chen, Lei Chen, and Yicong Zhou. "Cryptanalysis of image ciphers with permutation-substitution network and chaos". In: *IEEE Transactions on Circuits and Systems for Video Technology* 31.6 (2021), pp. 2494–2508.

[44] Chengqing Li and Guanrong Chen. "On the security of a class of image encryption schemes". In: *2008 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE. 2008, pp. 3290–3293.

[45] Leo Yu Zhang, Yuansheng Liu, Fabio Pareschi, Yushu Zhang, Kwok-Wo Wong, Riccardo Rovatti, and Gianluca Setti. "On the security of a class of diffusion mechanisms for image encryption". In: *IEEE transactions on cybernetics* 48.4 (2018), pp. 1163–1175.

[46] Thomas Hütter, Mario Preishuber, Jutta Hämmerle-Uhl, and Andreas Uhl. "Weaknesses in security considerations related to chaos-based image encryption". In: *Information and Communications Security*. Ed. by Kwok-Yan Lam, Chi-Hung Chi, and Sihan Qing. Springer. 2016, pp. 278–291.

[47] J. Mohamedmoideen Kader Mastan and R. Pandian. "Cryptanalysis of two similar chaos-based image encryption schemes". In: *Cryptologia* 45.6 (2021), pp. 541–552.

[48] Bowen Zhang and Lingfeng Liu. "Chaos-based image encryption: Review, application, and challenges". In: *Mathematics* 11.11 (2023), p. 2585.

[49] Behrouz Zolfaghari and Takeshi Koshiba. "Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap". In: *Applied System Innovation* 5.3 (2022), p. 57.

[50] Ljupco Kocarev. "Chaos-based cryptography: a brief overview". In: *IEEE Circuits and Systems Magazine* 1.3 (2001), pp. 6–21.

[51] Pellicer-Lostao Carmen and López-Ruiz Ricardo. "Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem". In: *Applied Cryptography and Network Security*. Ed. by Jaydip Sen. IntechOpen, 2012. Chap. 12.

[52] David Arroyo. "TESIS DOCTORAL Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems". PhD thesis. Universidad Politécnica de Madrid, 2009.

[53] Shujun Li, Guanrong Chen, and Xuanqin Mou. "On the dynamical degradation of digital piecewise linear chaotic maps". In: *International journal of Bifurcation and Chaos* 15.10 (2005), pp. 3119–3151.

[54] Chengqing Li, Bingbing Feng, Shujun Li, Jüergen Kurths, and Guanrong Chen. "Dynamic analysis of digital chaotic maps via state-mapping networks". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 66.6 (2019), pp. 2322–2335.

[55] David Arroyo, José María Amigó Garcia, Shujun Li, and Gonzalo Alvarez. "On the inadequacy of unimodal maps for cryptographic applications". In: *RECSI 2010 : IX [i.e. XI] Reunión Española sobre Criptología y Seguridad de la Información, Tarragona 7 - 10 de septiembre 2010 ; coordinado por Josep Domingo Ferrer... Tarragona : Publicacions URV, 2010*. Ed. by Josep Domingo Ferrer. Publicacions URV, 2010, pp. 37–42.

[56] JM Amigó, Ljupco Kocarev, and Janus Szczepanski. "Theory and practice of chaotic cryptography". In: *Physics Letters A* 366.3 (2007), pp. 211–216.
[57] Daniel-Ioan Curiac, Daniel Iercan, Octavian Dranga, Florin Dragan, and Ovidiu Banias. "Chaos-based cryptography: end of the road?" In: *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*. IEEE. 2007, pp. 71–76.
[58] David Arroyo, Gonzalo Alvarez, and Shujun Li. "Some hints for the design of digital chaos-based cryptosystems: lessons learned from cryptanalysis". In: *IFAC Proceedings Volumes* 42.7 (2009), pp. 171–175.
[59] Ercan Solak. "On the security of a class of discrete-time chaotic cryptosystems". In: *Physics Letters A* 320.5 (2004), pp. 389–395.
[60] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G. Bourbakis, and Kwok-Tung Lo. "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks". In: *Signal Processing: Image Communication* 23.3 (2008), pp. 212–223.
[61] Chengqing Li and Kwok-Tung Lo. "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks". In: *Signal processing* 91.4 (2011), pp. 949–954.
[62] Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. "On the security of permutation-only image encryption schemes". In: *IEEE transactions on information forensics and security* 11.2 (2016), pp. 235–246.
[63] Arshad, Shahtaj Shaukat, Arshid Ali, Amna Eleyan, Syed Aziz Shah, and Jawad Ahmad. "Chaos theory and its application: an essential framework for image encryption". In: *Chaos Theory and Applications* 2.1 (2020), pp. 17–22.
[64] Christophe De Canniere, Joseph Lano, and Bart Preneel. "Cryptanalysis of the two-dimensional circulation encryption algorithm". In: *EURASIP Journal on Advances in Signal Processing* 2005, 968795 (2005).
[65] Andrew Rukhin et al. *SP 800-22 Rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2010.
[66] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2021.
[67] Rhouma Rhouma and Safya Belghith. "Cryptanalysis of a new image encryption algorithm based on hyper-chaos". In: *Physics Letters A* 372.38 (2008), pp. 5973–5978.
[68] Rhouma Rhouma, Ercan Solak, and Safya Belghith. "Cryptanalysis of a new substitution–diffusion based image cipher". In: *Communications in Nonlinear Science and Numerical Simulation* 15.7 (2010), pp. 1887–1892.
[69] Xudong Liu, Xiaojun Tong, Zhu Wang, and Miao Zhang. "Uniform non-degeneracy discrete chaotic system and its application in image encryption". In: *Nonlinear Dynamics* 108.1 (2022), pp. 653–682.
[70] Hongxiang Zhao, Shucui Xie, Jianzhong Zhang, and Tong Wu. "A dynamic block image encryption using variable-length secret key and modified Henon map". In: *Optik* 230, 166307 (Mar. 2021).
[71] Chunhu Li, Guangchun Luo, Ke Qin, and Chunbao Li. "An image encryption scheme based on chaotic tent map". In: *Nonlinear Dynamics* 87 (2017), pp. 127–133.
[72] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh. "Cryptanalysis of Image Encryption Scheme Based on Chaotic Tent Map". In: 2016.
[73] Alireza Jolfaei. "Comments on an image encryption scheme based on a chaotic Tent map". In: (2016). arXiv: 1611.00381. URL: http://arxiv.org/abs/1611.00381.