

Article

Statistical Analysis of the Negative–Positive Transformation in Image Encryption

Manuel Alejandro Cardona-López ¹, Juan Carlos Chimal-Eguía ^{1,*}, Víctor Manuel Silva-García ²
and Rolando Flores-Carapia ²

¹ Centro de Investigación en Computación, Instituto Politécnico Nacional, Mexico City 07738, Mexico; mcardonal2022@cic.ipn.mx

² Centro de Innovación y Desarrollo Tecnológico en Cómputo, Instituto Politécnico Nacional, Mexico City 07738, Mexico; vsilvag@ipn.mx (V.M.S.-G.); rfloresca@ipn.mx (R.F.-C.)

* Correspondence: jchimale@ipn.mx

Abstract: The negative–positive transformation (NPT) is a widely employed technique for encrypting images on pixel blocks, commonly integrated into cryptosystems compatible with compression algorithms. The existing literature on NPT analysis can be categorized into two types: theoretical analyses with results that apply to any image, primarily focused on compression compatibility, and numerical analyses that report empirical results from specific images, some without explaining the causes of the security results, while others are only related to the compression performance. Consequently, there is a significant gap in understanding the implications of applying the NPT for data protection. For that reason, this paper conducts a theoretical statistical analysis, presenting, demonstrating, and verifying six theorems to understand the security contributions of NPT. Two theorems examine the shape of the image histogram and the scatter plot of adjacent pixels after the NPT application. The subsequent four theorems explore the influence of NPT on the mean, variance, covariance, and correlation within each pixel block. The findings indicate that the NPT generates images with symmetrical histograms, the correlation of pixel blocks remains invariant, and distinct vertical and horizontal reflections manifest on the scatter plot. These theorems are verified by encrypting the Lena image with four pixel-block sizes. The histogram symmetry passed the goodness-of-fit test at a significance level of 5%, revealing consistent results. The correlation of pixel blocks remained unchanged, and the scatter plot exhibited an x-shaped pattern. Therefore, as the NPT alone does not achieve desirable encryption results, such as uniform histograms, scatter plots, and decreasing correlation, cryptosystems should complement it with additional techniques.

Keywords: encryption-then-compression; JPEG encryption; negative–positive transformation; statistical analysis

MSC: 68P25



Citation: Cardona-López, M.A.; Chimal-Eguía, J.C.; Silva-García, V.M.; Flores-Carapia, R. Statistical Analysis of the Negative–Positive Transformation in Image Encryption. *Mathematics* **2024**, *12*, 908. <https://doi.org/10.3390/math12060908>

Academic Editor: Alla Levina

Received: 26 February 2024

Revised: 12 March 2024

Accepted: 14 March 2024

Published: 20 March 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The negative–positive transformation (NPT) is a commonly utilized encryption operation for securing images, particularly in compatible cryptosystems with compression techniques [1,2]. Notably, the NPT is employed in the encryption scheme of JPEG images, featuring prominently in various proposals [3–7]. In all of these instances, the NPT operates at the pixel block level [8] and applies to both color and grayscale images [9,10]. Moreover, the NPT finds applications beyond JPEG image encryption, extending its utility to hybrid methods like compressed sensing. In such applications, the NPT plays a role in achieving effective results for compressing encrypted images, as it can mask the original image before compression [11]. In addition, the versatility of the NPT is established in video encryption, particularly in MJPEG files [12]. In this context, it can replace video blocks within the original frames.

In its essence, the NPT finds application in the realm of data protection [13]. For instance, it is utilized to generate learnable transformed images, subsequently employed in convolutional neural network models. The objective is to control access to trained models [14]. Furthermore, various adaptations and versions based on the NPT have been developed. These proposals often strike a balance between security levels and the efficiency of compression savings [15]. One example is the injected negative–positive transformation (NINPT) [16] designed for compressed sensing. It is integrated into the encoding process to resist known plain-text attacks. Another variant is the double negative–positive transformation (DNPT) [17], which applies the NPT twice to encrypt images from a pixel matrix.

On the other hand, evaluating the security of algorithms designed to protect data is of paramount importance [18]. For image encryption algorithms, various measures and analyses are employed. One crucial aspect involves statistical analysis, often incorporating tools such as histograms, correlation assessments, and scatter plots [19,20]. The histogram illustrates the distribution of intensity levels among encrypted pixels in an image. Additionally, the histogram of the encrypted image is ideally uniform [21,22]. In cryptography, the goal is to introduce disparities between the original pixel values and the encrypted ones. The more evenly distributed the pixel values are, the more resilient the algorithm is against statistical attacks [23]. The correlation coefficient measures the relation between pixel values. Frequently, plain digital images tend to exhibit high correlation among adjacent pixels, capturing image features in specific regions [24]. In this way, the scatter plot is part of correlation analysis, plotting pairs of adjacent pixels to visualize the distribution of correlation in a specific direction [25].

However, the scope of analyses related to the NPT is limited, classifiable into theoretical and numerical works, where the former yields results applicable to any image, and the latter provides outcomes specific to certain images. The existing theoretical analyses primarily explore the relationship between pixels after NPT encryption. For instance, one study focuses on the Euclidean distance and the inner product of pixel vectors [26], aiming to assess image compatibility with machine learning models. In contrast, our work evaluates the NPT effects on the image histogram to analyze its statistical security. Other theoretical analyses in the EtC domain concentrate on preserving image properties for an effective compression process [27]. Differing from these theoretical analyses focused on preserving compatibility, ours is grounded in security considerations.

In the realm of numerical analysis, studies address security concerns related to encryption quality, using statistical parameters such as the correlation coefficient. However, these analyses are numerical and specifically reported from certain images [28], in contrast to the theorems presented in this study, which have applicability to any image. While other works mention that each pixel block in images encrypted with EtC exhibits almost the same correlation as the original images [29,30], they lack a demonstration of the underlying causes, a gap addressed in our work. Moreover, a comprehensive statistical analysis is often absent in this genre of research, which typically focuses solely on compression results [31]. Hence, our proposed study emphasizes a security analysis. Understanding the security implications of the NPT is crucial, particularly as it serves as the final step in some cryptosystems [32], and its outcomes can directly impact the encrypted information.

Therefore, it is necessary to explore the contribution of the NPT to the cryptosystem's security. This paper theoretically analyzes the NPT through one of the most essential studies: statistical analysis. Within this analysis, six theorems are presented, each accompanied by its respective demonstration and subsequently validated through computer simulations.

1.1. Motivation

Given the regular application of the NPT in encryption schemes compatible with compression, there is a need to explore its individual security performance. Existing security analyses are limited, and other studies primarily concentrate on compression performance. To understand the limitations of the technique, it is crucial to move beyond a mere numerical

study and conduct a theoretical analysis. An individual analysis of the NPT can offer insights into its specific contribution to security. This knowledge is essential for the design of new encryption techniques aimed at enhancing results in encryption and compression schemes and complementing the application of the NPT with other procedures.

1.2. Contribution

The primary contribution of this work lies in the security study of using the NPT for image encryption through a theoretical statistical analysis. Six theorems are presented to elucidate various statistical outcomes after the application of the NPT. Two theorems examine the shape of the image histogram and the scatter plot of adjacent pixels. The remaining four theorems delve into the impact of NPT on the mean, variance, covariance, and correlation within each pixel block. In addition to the theoretical demonstration of these theorems, their computational verification is carried out by encrypting the Lena image using NPT. The results obtained can be leveraged in the development of future encryption techniques and implementations of NPT in cryptosystems to enhance security considerations.

The paper's organization is as follows. Section 2 presents the main concepts of this work, the NPT, correlation coefficient, binomial distribution, and the goodness of fit test. Section 3 contains the theoretical statistical analysis of the NPT encryption, presenting the six theorems and their proofs. Section 4 consists of the encrypted images, graphs, and tables that verify the theorems. Sections 5 and 6 are the discussion and conclusions sections.

2. Materials and Methods

The encryption-then-compression (EtC) systems, which incorporate block scrambling, encrypt an image with dimensions $W = M \times N$ pixels in blocks of size $w = m \times n$ pixels, where M indicates the number of pixel rows in the image, N denotes the number of pixel columns, and W represents the total number of pixels in the image. Similarly, in the pixel block, m indicates the number of pixel rows, n denotes the number of pixel columns, and w denotes the number of pixels in the block. This scheme incorporates the NPT as one of the techniques within the EtC systems, as depicted in Figure 1. The NPT is applied to pixel blocks and all color components of the pixels.

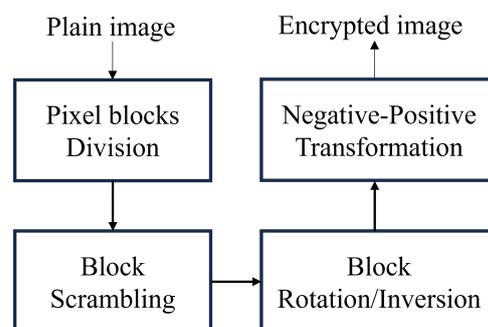


Figure 1. The negative–positive transformation (NPT) as a component of the EtC system for image encryption [33].

2.1. The Negative–Positive Transformation

The negative–positive transformation (NPT) is an encryption technique applied per pixel block, selectively transforming some pixel color values while leaving others unaltered. The NPT randomly employs the XOR binary operation between the pixel color value $px(i)$ and the number 255. The number 255 corresponds to the case where the number of intensity levels of a pixel color value is equal to 256. The decision to change the pixel color value, $px(i)$, to $px'(i) = px(i) \oplus 255$ or retain its original value, $px'(i) = px(i)$, is determined by a discrete random variable, X . In summary, the NPT application is defined by Equation (1). It is necessary to note that this transformation is applied to each pixel block, a , of the

image, affecting all pixel color values $px(i)$ within the block, a , where $1 \leq a \leq W/w$ and $1 \leq i \leq w$.

$$px'(i) = \begin{cases} px(i) \oplus 255, & \text{if } X = 1 \\ px(i), & \text{if } X = 0 \end{cases} \tag{1}$$

It is important to note that the variable X is a Bernoulli discrete random variable (BDRV), as defined in Equation (2). The probability mass function for X is presented in Table 1.

$$X = \begin{cases} 1, & \text{if the pixel block } a \text{ is selected} \\ 0, & \text{if the pixel block } a \text{ is not selected} \end{cases} \tag{2}$$

Table 1. Probability mass function of X in tabular form.

x	0	1
$p(x)$	0.5	0.5

Additionally, it is noteworthy that Equation (1) can be expressed as Equation (3), as the XOR operation can be interpreted as the two’s complement of an 8-bit number, which represents values between 0 and 255.

$$px'(i) = \begin{cases} 255 - px(i), & \text{if } X = 1 \\ px(i), & \text{if } X = 0 \end{cases} \tag{3}$$

In summary, an initial random number, $X = x$, is generated for each pixel block encryption. Subsequently, the computation of $px'(i)$ takes place for all pixels within the same pixel block according to the generated number. The process applies to each color channel, c , in the case of a color image. Below are two examples illustrating the implementation of the NPT for a color image, where each pixel, i , has three color components, $px(i) = \{R_i, G_i, B_i\}$. Table 2 corresponds to the example when the random number is $X = 1$, and Table 3 corresponds to the case when the generated number is $X = 0$. In both scenarios, the number of pixels, w , in the block is equal to 3. The original pixel values for Example 1 are $px(1) = \{120, 254, 31\}$, $px(2) = \{123, 252, 37\}$, and $px(3) = \{118, 249, 34\}$, while for Example 2, the values are $px(1) = \{10, 41, 55\}$, $px(2) = \{19, 42, 53\}$, and $px(3) = \{11, 37, 54\}$.

Table 2. The Negative-Positive Transformation (NPT) application over a color-pixel block of $w = 3$ pixels and $X = 1$.

Value	First Pixel			Second Pixel			Third Pixel		
	R ₁	G ₁	B ₁	R ₂	G ₂	B ₂	R ₃	G ₃	B ₃
$px(i)$	120	254	31	123	252	37	118	249	34
$px'(i)$	135	1	224	132	3	218	137	6	221

Table 3. The NPT application over a color-pixel block of $w = 3$ pixels and $X = 0$.

Value	First Pixel			Second Pixel			Third Pixel		
	R ₁	G ₁	B ₁	R ₂	G ₂	B ₂	R ₃	G ₃	B ₃
$px(i)$	10	41	55	19	42	53	11	37	54
$px'(i)$	10	41	55	19	42	53	11	37	54

2.2. Correlation Coefficient

The correlation coefficient (ρ) assesses the confusion and diffusion effects in an encrypted image by considering pairs of pixels [34]. It is defined by Equation (4). In this context, let K represent the discrete random variable for the pixel color value in the original image, and Q denote the adjacent pixel color value in the original image. Throughout this

work, the samples consist of w pixels as elements, where the total number of pixels in an image is W , and $w \leq W$.

$$\rho(K, Q) = \frac{\text{Cov}(K, Q)}{\sqrt{\text{Var}(K)}\sqrt{\text{Var}(Q)}} \tag{4}$$

where the covariance $\text{Cov}(K, Q)$, applicable to image encryption [35,36], is shown in Equation (5). It serves as a measure to evaluate the strength of the relationship between two random variables, K and Q .

$$\text{Cov}(K, Q) = \frac{1}{w} \sum_{i=1}^w (k_i - \bar{k})(q_i - \bar{q}) \tag{5}$$

Also, variance s_k^2 or $\text{Var}(K)$ of a sample is defined in Equation (6).

$$\text{Var}(K) = \frac{1}{w} \sum_{i=1}^w (k_i - \bar{k})^2 \tag{6}$$

Finally, the mean \bar{k} of a sample with w elements is defined in Equation (7).

$$\bar{k} = \frac{1}{w} \sum_{i=1}^w k_i \tag{7}$$

2.3. Binomial Distribution

If a distribution is binomial, the following conditions must be satisfied [37]:

1. It has a fixed number of trials n .
2. In each trial, there are two possible outcomes.
3. One outcome is termed as a success with a fixed probability, p , for all the trials.
4. The trials are independent of each other.
5. The random variable Y denotes the number of successes observed after the n -executed trials.

If all the aforementioned conditions are met, the probability mass function for the variable Y is given by Equation (8). In addition, if Y follows a binomial distribution, it can be denoted as $Y \sim B(n, p)$.

$$f_Y(n, p) = \binom{n}{y} p^y (1 - p)^{n-y} \tag{8}$$

where $y = 0, 1, 2, 3, \dots, n$, its expected value is $E[Y] = np$, and the variance is $\text{Var}(Y) = np(1 - p)$.

2.4. Goodness-of-Fit Test

It is a statistical hypothesis test used to compare if the observed data from a sample of d elements has an expected distribution. In other words, it assesses the fit of the theoretical distribution with the collected information [38]. The test is based on proving the null hypothesis, H_0 : The data follow the theoretical distribution. Although not rejecting H_0 should not be interpreted as accepting it as verified. The traditional goodness-of-fit test follows the chi-square test. It works with the χ^2 statistic, computed as Equation (9) defines it. It sums the squared deviations between the observed registers, O_i , and the expected values, E_i .

$$\chi^2 = \sum_{i=1}^d \frac{(O_i - E_i)^2}{E_i} \tag{9}$$

The χ^2 has $d - 1$ degrees of freedom, where d indicates the number of categories (cells) into which the data are divided [39]. Additionally, the statistical test has an associated p -value. Specifically, a histogram of 256 classes follows a theoretical distribution if $\chi^2 < 291$

with a significance level of 0.05 [40]. The preceding information is relevant since the color images in this work have 256 different intensity levels.

3. Statistical Analysis

In this section, the statistical analysis is conducted through the presentation and proof of six theorems. Section 3.1 contains the theorem on the histogram. Section 3.2 provides the theorem on the mean, Section 3.3 presents the theorem on variance, and Section 3.4 addresses the theorem on covariance. Section 3.5 explores the theorem on correlation. Finally, Section 3.6 delves into the theorem on the scatter plot. The theorems on the histogram and scatter plot encompass the results of the entire image, while the remaining theorems focus specifically on the outcomes of pixel blocks. Furthermore, Sections 3.3–3.5 include two distinct proofs each.

The analysis is based on the following assumptions. Firstly, considering that the NPT in EtC systems is implemented in the RGB space, the analysis focuses specifically on this color space. Furthermore, NPT operates by pixel block; hence, the results derived from the analysis apply to pixel-block encryption. Also, it is assumed that the image width is a multiple of the block width, and the image height is a multiple of the block height. While the current examination is conducted on a single color component, it is important to note that the findings can be extrapolated to any of the three colors in the RGB space. Subsequently, the upcoming section will perform computer verification for each color, aligning with the outcomes of this theoretical analysis.

3.1. Histogram

Histograms applied to images serve to depict the frequency distribution of each color intensity across all pixels. In other words, it quantifies the number of pixels with a specific intensity value throughout the entire image. This process is replicated for each color channel, providing statistical insights into its distribution [41]. In the present study, the number of intensity levels is 256, ranging from 0 to 255, and there are three colors: red, green, and blue. However, it does not capture information about the spatial position of individual pixels. Following the application of the NPT procedure, the new pixel color values, $px'(i)$, lead to a redistribution of the original intensity levels within the image histogram. In this context, the resulting frequencies of the histogram are analyzed in Theorem 1.

Theorem 1. *The intensity level distribution of any image, after applying the NPT, conforms to a symmetric histogram.*

Proof. The proof involves two probabilistic experiments to examine the modified distribution.

1. Observe the new pixel color value, $px'(i)$, after the NPT, of a pixel with an original color value equal to h . This analysis applies to all instances of $px(i) = h$.
2. Observe the new pixel color value, $px'(i)$, after the NPT, of a pixel with an original color value equal to $h \oplus 255$. It is repeated for all instances of $px(i) = h \oplus 255$.

Therefore, the observation in experiment number 1 has two possibilities: retaining its value as $px'(i) = h$ or modifying it to $px'(i) = h \oplus 255$. In this context, the BDRV, S_i , is defined in Equation (10) to represent this scenario. Additionally, in experiment two, there are two possibilities, and to signify them, the BDRV, T_i , is defined in Equation (11).

$$S_i = \begin{cases} 1, & \text{if } px'(i) = h \\ 0, & \text{if } px'(i) = h \oplus 255 \end{cases} \quad (10)$$

$$T_i = \begin{cases} 1, & \text{if } px'(i) = h \\ 0, & \text{if } px'(i) = h \oplus 255 \end{cases} \quad (11)$$

It is important to note that in Equation (11), value h is obtained when $px(i) = h \oplus 255$ changes its value to $px'(i) = (h \oplus 255) \oplus 255 = h$. Additionally, considering the NPT composition in Equation (1), the probabilities for both S_i and T_i variables are $p(0) = p(1) = 0.5$.

Another point to consider is that experiment number 1 can only be executed over the $l_h \leq W$ pixel color values, such that $px(i) = h$, and similarly, the second experiment can be performed $l_{h \oplus 255}$ times. Consequently, two new discrete random variables are defined, S_{tot} and T_{tot} , corresponding to the sum of the variables, S_i and T_i , respectively. Both are presented in Equations (12) and (13).

Additionally, considering that the sum of BDRV converges to a binomial distribution [42], it follows that $S_{tot} \sim B(l_h, 0.5)$, where the number of trials is l_h , and the probability of success is equal to 0.5. Similarly, $T_{tot} \sim B(l_{h \oplus 255}, 0.5)$, with $l_{h \oplus 255}$ trials and a success probability of 0.5.

$$S_{tot} = \sum_{i=1}^{l_h} S_i \tag{12}$$

$$T_{tot} = \sum_{i=1}^{l_{(h \oplus 255)}} T_i \tag{13}$$

In other words, the variable S_{tot} corresponds to the number of transformed pixels $px'(i) = h$, such that the pixel color component was previously $px(i) = h$. Similarly, the variable T_{tot} represents the number of $px'(i) = h$ occurrences, which was previously $px(i) = h \oplus 255$.

Furthermore, it can be verified that both variables satisfy the conditions for a binomial distribution. For example, the verification for the variable S_{tot} is provided below.

1. It has a fixed number of trials l_h , which is the original number of pixels that satisfy $px(i) = h$.
2. There are only two possible outcomes: $px'(i) = h$ and $px'(i) = h \oplus 255$.
3. The success is $px'(i) = h$ with a probability of $p = 0.5$.
4. The trials are independent because, within a pixel block, there are similar pixel color values, though not necessarily the same. Then, the NPT is applied independently to each pixel $px(i) = h$.

On the other hand, a final discrete random variable is proposed, denoted as F , representing the number of color pixels with a value equal to h after the NPT. It is defined in Equation (14) and can be replicated for each color c .

$$F = S_{tot} + T_{tot} \tag{14}$$

With this in mind, the expected value of F is given in Equation (15).

$$E(F) = E(S_{tot} + T_{tot}) = E(S_{tot}) + E(T_{tot}) \tag{15}$$

Since S_{tot} and T_{tot} follow a binomial distribution, their expected value is computed as $n \times p$, resulting in Equation (16). This represents the number of pixel color values equal to h after the NPT.

$$E(F) = l_h \times 0.5 + l_{h \oplus 255} \times 0.5 = \frac{(l_h + l_{h \oplus 255})}{2} \tag{16}$$

Now, to estimate the number of pixel color values equal to $h \oplus 255$ after the NPT, the variables S'_{tot} and T'_{tot} are defined in Equations (17) and (18), respectively. Here, S'_{tot} represents the number of transformed pixels $px'(i) = h \oplus 255$ that were originally $px(i) = h$. Meanwhile, T'_{tot} considers the number of transformed pixels $px'(i) = h \oplus 255$ with the original color values $px(i) = h \oplus 255$.

$$S'_{tot} = l_h - S_{tot} \tag{17}$$

$$T'_{tot} = l_{h \oplus 255} - T_{tot} \tag{18}$$

Thus, the variable F' , as defined in Equation (19), represents the frequency of the $h \oplus 255$ level after the NPT.

$$F' = S'_{\text{tot}} + T'_{\text{tot}} \tag{19}$$

Now, the expected value of F' , indicating the expected frequency of pixel color values equal to the $h \oplus 255$ level, is shown in Equation (20).

$$E(F') = E(S'_{\text{tot}} + T'_{\text{tot}}) = E(l_h - S_{\text{tot}} + l_{h \oplus 255} - T_{\text{tot}}) \tag{20}$$

The expected value can also be expressed as Equation (21) by rearranging and utilizing the definition of F in Equation (14).

$$E(F') = E(l_h + l_{h \oplus 255} - (S_{\text{tot}} + T_{\text{tot}})) = E(l_h + l_{h \oplus 255} - F) \tag{21}$$

Finally, the resultant $E(F)$ from Equation (16) leads to Equation (22).

$$E(F') = l_h + l_{h \oplus 255} - E(F) = l_h + l_{h \oplus 255} - \frac{(l_h + l_{h \oplus 255})}{2} \tag{22}$$

Simplifying the expected value of F' , it is presented in Equation (23). This result is equivalent to the $E(F)$ obtained in Equation (16). In other words, the expected value of the number of frequencies for the color level h is the same as the color level $h \oplus 255$. This is anticipated for all the intensity levels of the histograms after applying the NPT.

$$E(F') = \frac{(l_h + l_{h \oplus 255})}{2} = E(F) \tag{23}$$

□

3.2. Arithmetic Mean

The mean \bar{k}' calculates the average of the new pixel color values $px'(i)$ after the NPT application to the w pixels within a pixel block. This is illustrated in Equation (24).

$$\bar{k}' = \frac{1}{w} \sum_{i=1}^w px'(i) \tag{24}$$

Theorem 2. *The mean of the pixels in a block after the NPT is equal to the NPT of its original mean.*

Proof. The demonstration considers two cases: when the BDRV $X = 1$, and $X = 0$. In the former, the value $px(i) = k_i$ changes to $px'(i) = k_i \oplus 255$, while Equation (25) illustrates its mean \bar{k}' .

$$\bar{k}' = \frac{1}{w} \sum_{i=1}^w (255 - k_i) \tag{25}$$

Equation (25) is split into two sums, resulting in Equation (26).

$$\bar{k}' = \frac{1}{w} \left(\sum_{i=1}^w 255 - \sum_{i=1}^w k_i \right) \tag{26}$$

The first term is a constant sum, and the second one corresponds to Equation (7). The simplified result is in Equation (27).

$$\bar{k}' = 255 - \bar{k} \tag{27}$$

Which is equivalent to Equation (28).

$$\bar{k}' = \bar{k} \oplus 255 \tag{28}$$

In the case of $X = 0$, the pixel value remains unchanged, i.e., $px'(i) = px(i)$. Consequently, the mean also remains the same, $\bar{k}' = \bar{k}$.

In conclusion, in both cases, the mean of pixels in a block after the NPT is equal to the NPT of its original mean, as shown in Equation (29).

$$\bar{k}' = \begin{cases} \bar{k} \oplus 255, & \text{if } X = 1 \\ \bar{k}, & \text{if } X = 0 \end{cases} \tag{29}$$

□

3.3. Variance

Similarly to the mean, the variance of $px'(i)$ in a pixel block after applying the NPT is analyzed with Equation (6). Since the pixels might change their values, the mean \bar{k}' also needs to be considered (obtained in Equation (29)). Consequently, the variance $s_k'^2$, which includes these considerations, is shown in Equation (30).

$$s_k'^2 = \frac{1}{w} \sum_{i=1}^w (px'(i) - \bar{k}')^2 \tag{30}$$

The variance quantifies the degree of dispersion among the elements within a set [41]. It considers the squared distance between a specific value of the set and the mean of the set. It computes all the distances in this manner for all the elements of the set. Subsequently, their average is calculated to derive the variance. In this context, the set is the pixel block, and the elements are the pixel color values. Since the mean can change after the NPT application, the variance must consider this modification along with the encryption of the pixel color values. In this way, the Theorem 3 is presented.

Theorem 3. *The variance of pixels in a block remains invariant after the NPT.*

Proof. The demonstration considers the two following NPT cases: $X = 1$ and $X = 0$. When $X = 1$, then $px'(i) = 255 - k_i$, and the resulting variance $s_k'^2$ is expressed in Equation (31), taking into account the mean from Equation (27).

$$s_k'^2 = \frac{1}{w} \sum_{i=1}^w (255 - k_i - (255 - \bar{k}))^2 \tag{31}$$

The simplified form of Equation (31) is presented in Equation (32).

$$s_k'^2 = \frac{1}{w} \sum_{i=1}^w (-k_i + \bar{k})^2 \tag{32}$$

Finally, it can be observed that Equations (6) and (32) are equivalent, both representing the same quadratic term.

$$s_k'^2 = s_k^2 \tag{33}$$

In the case of $X = 0$, where the pixel values remain unchanged ($px'(i) = px(i)$), the variance remains the same, i.e., $s_k'^2 = s_k^2$. In conclusion, the NPT does not alter the variance of any pixel block in either case. □

Proof. Another method to derive the variance result is through the proposition in Equation (34), which applies to linear functions of the form $aK + b$ [43].

$$\text{Var}(aK + b) = a^2 \sigma_K^2 \tag{34}$$

Let the discrete random variable K' represent the pixel color value in the block after the NPT. When $X = 1$, K' takes the value $255 - K$. Therefore, applying the proposition, its resulting variance is given by Equation (35). In this case, $a = -1$ and $b = 0$.

$$\text{Var}(K') = \text{Var}(-K + 255) = (-1)^2 s_k^2 = s_k^2 \tag{35}$$

Consequently, the variance after the NPT application, whether $X = 1$ or $X = 0$, remains unchanged. \square

3.4. Covariance

In a similar manner, the covariance is examined after the NPT by employing two discrete random variables. One is the variable K' introduced earlier in the variance section, and another random variable is defined as Q' : The adjacent pixel color value in the block after the NPT. The covariance of both variables is computed using Equation (5), resulting in Equation (36).

$$\text{Cov}(K', Q') = \frac{1}{w} \sum_{i=1}^w (k_i - \bar{k})(q_i - \bar{q}) \tag{36}$$

The covariance measures the degree of the relationship between a pair of variables, denoted as K' and Q' , within the same sample [41]. In this case, the sample is the pixel block, and the pairs of variables are defined by the values of adjacent pixels. Similar to the variance, the covariance assesses the distance of each variable value from its respective mean, and subsequently multiplies them. Consequently, the sign of the covariance depends on the variability of one variable relative to the other. A positive covariance indicates a change in the same direction, while a negative sign suggests an opposite change. Now, the relationship between these variables is assessed after the NPT application. In this context, the Theorem 4 is presented.

Theorem 4. *The covariance within a pixel block remains invariant after the NPT.*

Proof. The NPT, in the case of $X = 0$, preserves the initial covariance $\text{Cov}(K', Q') = \text{Cov}(K, Q)$, similar to the mean and variance. Conversely, when the NPT takes the value $X = 1$, the alternative definition of the NPT in Equation (3) for k'_i and q'_i , along with the sample mean value result of Equation (27), modifies Equation (36) to Equation (37).

$$\text{Cov}(K', Q') = \frac{1}{w} \sum_{i=1}^w ((255 - k_i) - (255 - \bar{k}))((255 - q_i) - (255 - \bar{q})) \tag{37}$$

Simplifying, the result is presented in Equation (38).

$$\text{Cov}(K', Q') = \frac{1}{w} \sum_{i=1}^w (-k_i + \bar{k})(-q_i + \bar{q}) \tag{38}$$

Consequently, the product can be expressed as shown in Equation (39).

$$\text{Cov}(K', Q') = \frac{1}{w} \sum_{i=1}^w (-1)(k_i - \bar{k})(-1)(q_i - \bar{q}) \tag{39}$$

Therefore, the final result is shown in Equation (40).

$$\text{Cov}(K', Q') = \frac{1}{w} \sum_{i=1}^w (k_i - \bar{k})(q_i - \bar{q}) \tag{40}$$

In conclusion, the NPT does not modify the covariance value in a pixel block.

$$\text{Cov}(K', Q') = \text{Cov}(K, Q) \tag{41}$$

□

Proof. Another approach to validate the covariance result is through the use of the proposition in Equation (42) [43].

$$\text{Cov}(aK + c, Q) = a\text{Cov}(K, Q) \tag{42}$$

In the NPT, when $X = 1$, the discrete random variables K' and Q' change to $255 - K$ and $255 - Q$, respectively, as illustrated in Equation (43).

$$\text{Cov}(K', Q') = \text{Cov}(-K + 255, -Q + 255) \tag{43}$$

Therefore, we apply the proposition of Equation (42) to Equation (43) with $a = -1$ and $b = 255$.

$$\text{Cov}(K', Q') = (-1)\text{Cov}(K, -Q + 255) \tag{44}$$

Since $\text{Cov}(K, Q) = \text{Cov}(Q, K)$, applying Equation (42) once more yields Equation (45).

$$\text{Cov}(K', Q') = (-1)(-1)\text{Cov}(Q, K) \tag{45}$$

Consequently,

$$\text{Cov}(K', Q') = \text{Cov}(K, Q) \tag{46}$$

□

3.5. Pearson Correlation

The correlation of Equation (4) is rewritten as Equation (47) to denote the NPT application.

$$\rho(K', Q') = \frac{\text{Cov}(K', Q')}{\sqrt{\text{Var}(K')} \sqrt{\text{Var}(Q')}} \tag{47}$$

Theorem 5. *The Pearson correlation in a pixel block remains invariant under the NPT.*

Proof. Combining the results obtained for variance in Equation (33) and covariance in Equation (41), the overall result is presented in Equation (48).

$$\rho(K', Q') = \frac{\text{Cov}(K, Q)}{\sqrt{\text{Var}(K)} \sqrt{\text{Var}(Q)}} \tag{48}$$

In conclusion, the correlation remains unaltered, i.e., $\rho(K', Q') = \rho(K, Q)$. □

3.6. Scatter Plot

Given two pixel values denoted as r and s , where one is adjacent to the other, their representation on a scatter plot can be with the point (r, s) . The NPT application shifts this point in horizontal and vertical directions, as depicted in Figure 2. It is important to highlight that reflections occur concerning the center at $(127, 127)$.

Below, each of the reflections presented in Figure 2 are described as follows:

1. Vertical reflection. In Figure 2b, the pixel value r remains unchanged after the application of the NPT, indicating that it was applied in this block with $X = 0$. On the other hand, the adjacent pixel with an original value, s , changes its value to $255 - s$, signifying that it belongs to another (but adjacent) pixel block where the NPT has been applied with $X = 1$.
2. Horizontal reflection. In Figure 2d, the pixel value r transforms to $255 - r$ after the application of the NPT with $X = 1$ in its block. Meanwhile, the adjacent pixel with value s belongs to another pixel block (though adjacent), and in that block, the NPT is applied with $X = 0$, resulting in an unchanged value.

3. Simultaneous vertical and horizontal reflection. This is illustrated in Figure 2c. In contrast to the other two cases, this type of reflection arises from two possibilities. Firstly, both adjacent pixels with values r and s are in the same pixel block, and the NPT is applied with $X = 1$ in that pixel block. The second possibility is that both pixel values are in different pixel blocks, but in both blocks, the NPT is applied with $X = 1$.

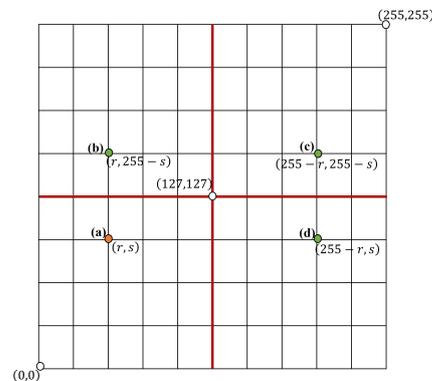


Figure 2. Possible reflections of a pixel value pair (r, s) after NPT. (a) Original position. (b) Vertical reflection across the abscissa axis. (c) Reflection over both axes. (d) Horizontal reflection across the ordinate axis.

Theorem 6. *The NPT results in reflections in a scatter plot, occurring over either the horizontal, vertical, or both axes, with the point of origin set at $(127, 127)$.*

Proof. The demonstration evaluates the distance of the new point to the origin $(127, 127)$ in various directions after applying the NPT compared to the original distances.

In the horizontal direction, let $d = |127 - r|$ represent the distance to the center before the NPT. If the NPT, applied to its corresponding pixel, has $X = 1$, then $d = |127 - (255 - r)| = |-128 + r| = |128 - r|$. Otherwise, it does not alter its value, and the distance remains unchanged.

Similarly, the distance to the center in the vertical direction is $d = |127 - s|$. If it modifies its value, the distance becomes $d = |127 - (255 - s)| = |-128 + s| = |128 - s|$. □

4. Computer Verification

In this section, we validate the six theorems by implementing the NPT and applying it to encrypt the Lena image (Figure 3). Furthermore, the original histograms and scatter plots are displayed in Figure 4. As the NPT operates on pixel blocks, and although the theorems are demonstrated for any size, we present the results of four different block sizes. The encryption results in sizes of 2×2 , 4×4 , 8×8 , and 16×16 are shown in Figure 5.

Concerning the execution time for encrypting the Lena color image of 512×512 pixels, it is 120.03 ms for a pixel block size of 2×2 , 82.05 ms for a size of 4×4 , 78.80 ms for a block size of 8×8 , and finally, 78.64 ms for a size of 16×16 .

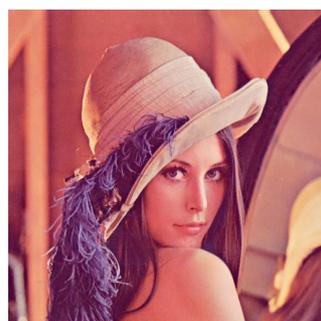


Figure 3. The Lena image, measuring 512×512 pixels, is utilized in this section for encryption, using the NPT to validate the presented theorems.

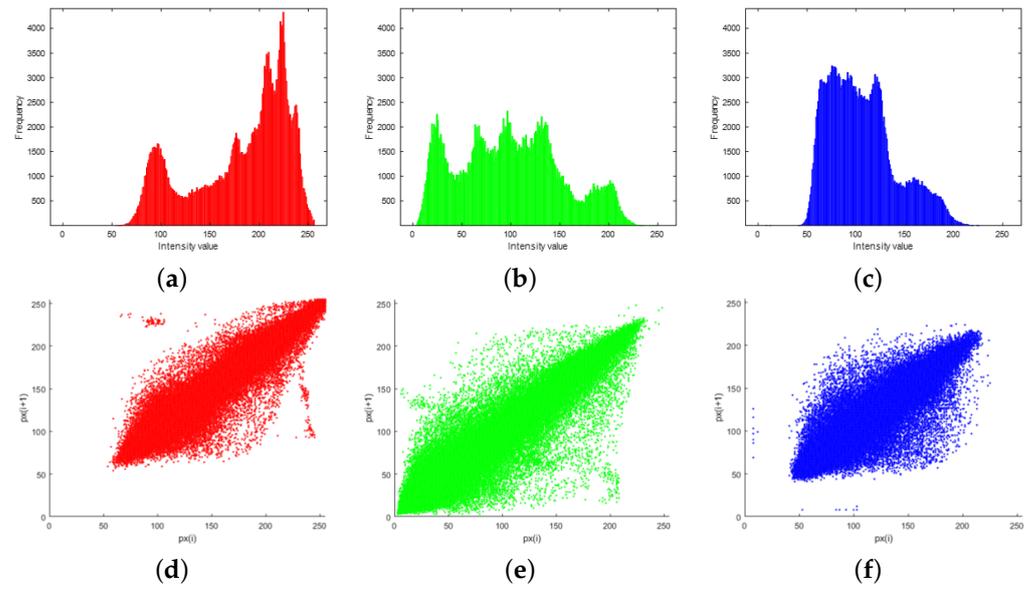


Figure 4. Lena’s original histograms and scatter plots. (a) Histogram of the red channel. (b) Histogram of the green channel. (c) Histogram of the blue channel. (d) Scatter plot of the red channel. (e) Scatter plot of the green channel. (f) Scatter plot of the blue channel.

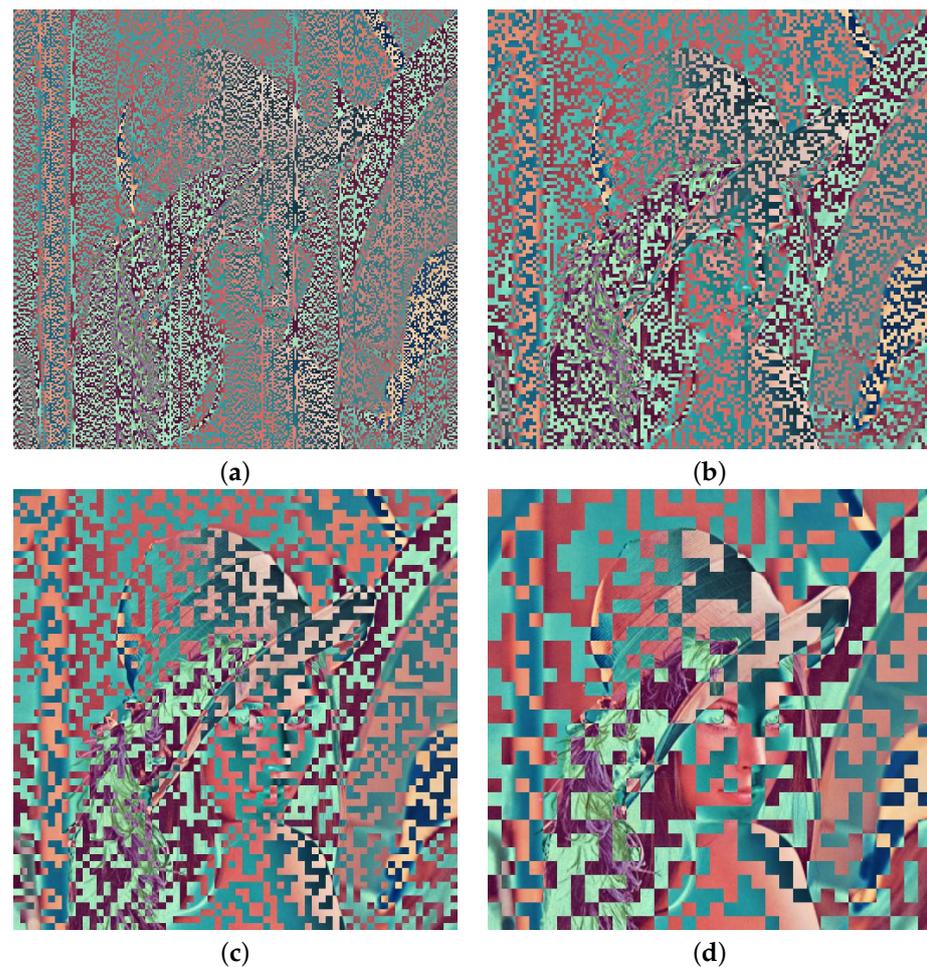


Figure 5. Encryption results of the Lena image using the NPT for various block sizes. (a) Pixel block size of 2×2 . (b) Pixel block size of 4×4 . (c) Pixel block size of 8×8 . (d) Pixel block size of 16×16 .

4.1. Histogram

The histograms in Figure 5 display a symmetric shape, with the center around intensity levels of 127–128. Additionally, each color histogram is presented for the four different pixel block sizes. The red color histogram is depicted in Figure 6, while Figures 7 and 8 showcase the green and blue color histograms, respectively. By comparing the observed values from the histograms with the expected frequencies obtained in Equation (23), a goodness-of-fit test is conducted. The degree of resemblance between the experimental and theoretical values is quantified and summarized in Table 4. Notably, the pixel blocks of size 2×2 and 4×4 successfully pass the test for their 256 intensity levels in each color.

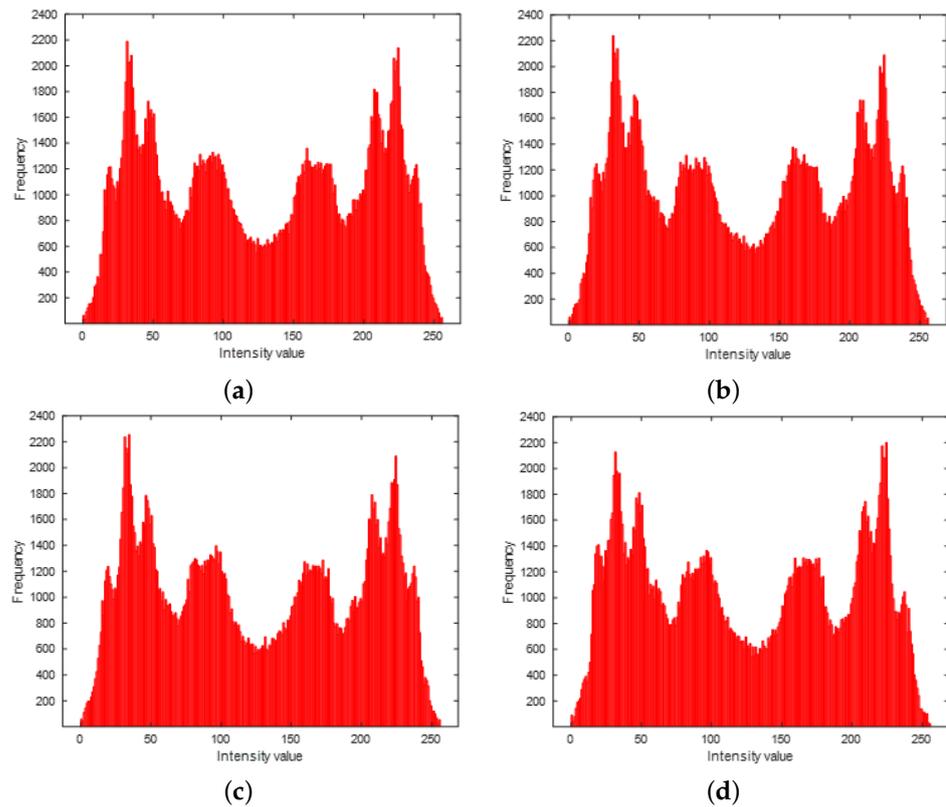


Figure 6. Resultant histograms of the red channel from Figure 5. (a) Red channel histogram from Figure 5a. (b) Red channel histogram from Figure 5b. (c) Red channel histogram from Figure 5c. (d) Red channel histogram from Figure 5d.

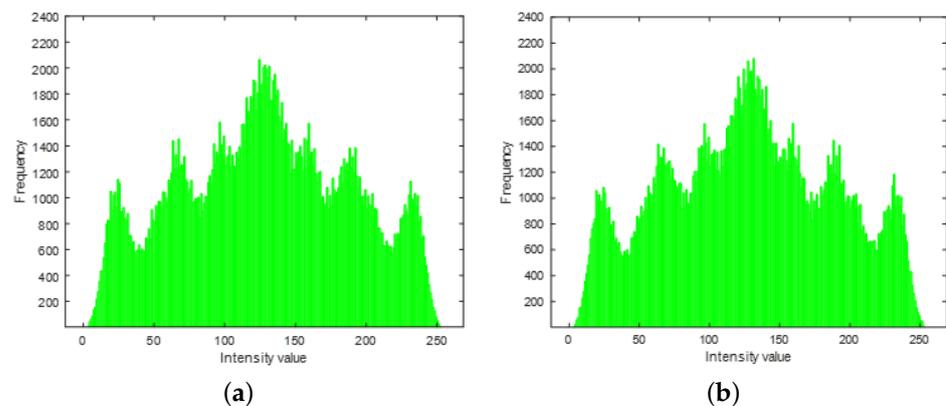


Figure 7. Cont.

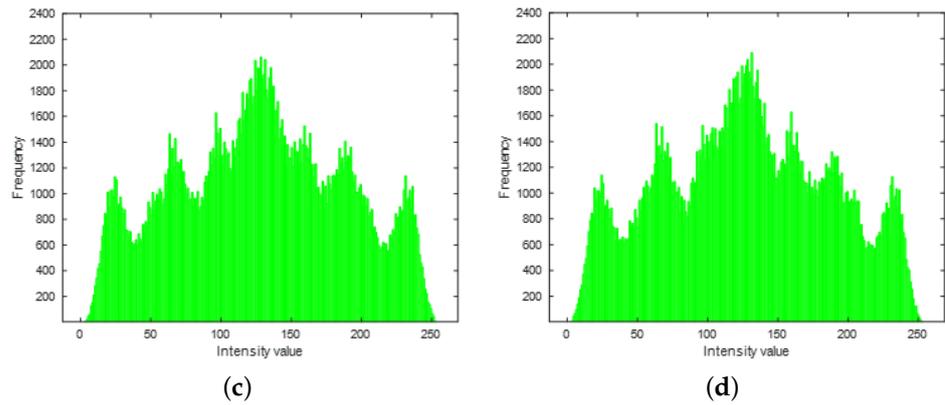


Figure 7. Resultant histograms of the green channel from Figure 5. (a) Green channel histogram from Figure 5a. (b) Green channel histogram from Figure 5b. (c) Green channel histogram from Figure 5c. (d) Green channel histogram from Figure 5d.

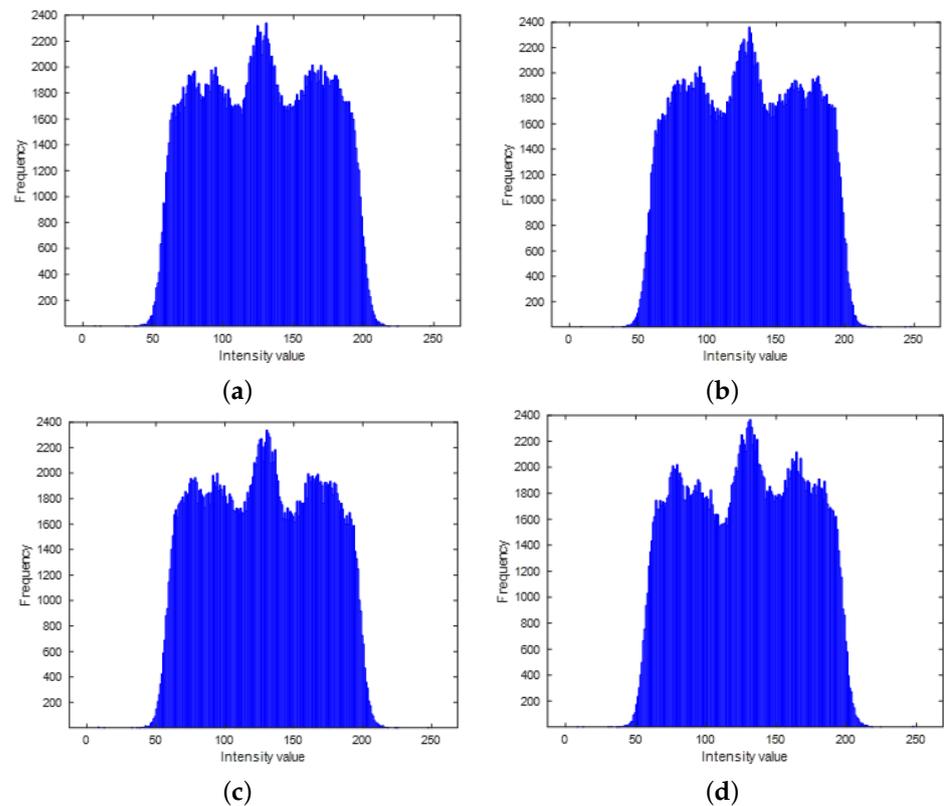


Figure 8. Resultant histograms of the blue channel from Figure 5. (a) Blue channel histogram from Figure 5a. (b) Blue channel histogram from Figure 5b. (c) Blue channel histogram from Figure 5c. (d) Blue channel histogram from Figure 5d.

Table 4. Results of the goodness-of-fit test (✓ Accept, × Reject), with $\alpha = 0.01$.

Color	2×2	4×4	8×8	16×16
Red	213.8/✓	284.5/✓	597.8/x	1824.5/x
Green	215.0/✓	238.5/✓	370.8/x	1702.7/x
Blue	222.3/✓	240.8/✓	459.2/x	1456.8/x

4.2. Correlation Coefficient

Calculating the correlation coefficient involves considering the mean, variance, and covariance, all of which were addressed in the preceding section through various theorems.

Now, the empirical values are presented to validate each of these properties for four different block sizes, mirroring the approach taken in the histogram section. Tables 5–8 provide the statistical outcomes both before and after encrypting two pixel blocks for each size. The first pixel block is encrypted by NPT with $X = 1$, and the second with $X = 0$. The results are detailed in the following points.

1. In the first pixel block, the original mean, \bar{k} , changes to its complement to 255, whereas, in the second one, it remains unaltered, i.e., $\bar{k} = \bar{k}'$. This outcome aligns with Theorem 2, asserting that the arithmetic mean of a pixel block after the NPT corresponds to the NPT of the original mean.
2. The variance (Var), covariance (Cov), and correlation coefficient (ρ) of each pixel block remain unaltered in both NPT cases, thereby affirming the validity of Theorems 3–5. Here, for Tables 5–8, S_K and S_Q represent the original variances in the pixel block, while $S_{K'}$ and $S_{Q'}$ denote the resultant variances after the NPT application. A similar notation is maintained for the covariance, transitioning from $\text{Cov}(K, Q)$ to $\text{Cov}(K', Q')$, and the correlation, progressing from $\rho(K, Q)$ to $\rho(K', Q')$.
3. The second pixel block in Table 5 exhibits a variance equal to zero since all its pixels share the same value for the blue color. Consequently, computing the correlation is not feasible.

Table 5. Results for two pixel blocks of 2×2 , before and after the NPT in its two cases.

	First Pixel Block			Second Pixel Block		
	Red _{X=1}	Green _{X=1}	Blue _{X=1}	Red _{X=0}	Green _{X=0}	Blue _{X=0}
\bar{k}	210.5	114.5	100.0	183.0	72.5	81.0
\bar{k}'	44.5	140.5	155.0	183.0	72.5	81.0
s_k^2	110.25	240.25	100.0	4.0	2.25	0.0
$s_k'^2$	110.25	240.25	100.0	4.0	2.25	0.0
s_Q^2	110.25	240.25	100.0	4.0	2.25	0.0
$s_Q'^2$	110.25	240.25	100.0	4.0	2.25	0.0
$\text{Cov}(K, Q)$	−110.25	−240.25	−100.0	−4.0	−2.25	0.0
$\text{Cov}(K', Q')$	−110.25	−240.25	−100.0	−4.0	−2.25	0.0
$\rho(K, Q)$	−1.0	−1.0	−1.0	−1.0	−1.0	—
$\rho(K', Q')$	−1.0	−1.0	−1.0	−1.0	−1.0	—

Table 6. Results for two pixel blocks of 4×4 , before and after the NPT in its two cases.

	First Pixel Block			Second Pixel Block		
	Red _{X=1}	Green _{X=1}	Blue _{X=1}	Red _{X=0}	Green _{X=0}	Blue _{X=0}
\bar{k}	224.5	136.75	127.75	88.313	24.438	59.688
\bar{k}'	30.5	118.25	127.25	88.313	24.438	59.688
s_k^2	2.25	0.188	10.688	26.215	17.371	6.465
$s_k'^2$	2.25	0.188	10.688	26.215	17.371	6.465
s_Q^2	2.25	0.188	15.688	28.426	21.879	6.848
$s_Q'^2$	2.25	0.188	15.688	28.426	21.879	6.848
$\text{Cov}(K, Q)$	1.125	−0.063	−1.063	11.102	6.031	−0.375
$\text{Cov}(K', Q')$	1.125	−0.063	−1.063	11.102	6.031	−0.375
$\rho(K, Q)$	0.5	−0.333	−0.082	0.407	0.309	−0.056
$\rho(K', Q')$	0.5	−0.333	−0.082	0.407	0.309	−0.056

Table 7. Results for two pixel blocks of 8×8 , before and after the NPT in its two cases.

	First Pixel Block			Second Pixel Block		
	Red _{X=1}	Green _{X=1}	Blue _{X=1}	Red _{X=0}	Green _{X=0}	Blue _{X=0}
\bar{k}	225.844	134.828	121.109	199.234	109.594	104.906
\bar{k}'	29.156	120.172	133.890	199.234	109.594	104.906
s_k^2	3.788	10.580	41.347	1641.992	1499.334	420.054
$s_k'^2$	3.788	10.580	41.347	1641.992	1499.334	420.054
s_Q^2	4.086	11.297	42.042	1933.309	1729.037	457.635
$s_Q'^2$	4.086	11.297	42.042	1933.309	1729.037	457.635
Cov(K, Q)	1.507	0.321	22.953	1683.994	1451.319	357.024
Cov(K', Q')	1.507	0.321	22.953	1683.994	1451.319	357.024
$\rho(K, Q)$	0.383	0.029	0.551	0.945	0.901	0.814
$\rho(K', Q')$	0.383	0.029	0.551	0.945	0.901	0.814

Table 8. Results for two pixel blocks of 16×16 , before and after the NPT in its two cases.

	First Pixel Block			Second Pixel Block		
	Red _{X=1}	Green _{X=1}	Blue _{X=1}	Red _{X=0}	Green _{X=0}	Blue _{X=0}
\bar{k}	105.922	41.102	74.863	117.160	38.113	65.895
\bar{k}'	149.078	213.898	180.137	117.160	38.113	65.895
s_k^2	330.931	461.927	324.845	553.291	216.515	84.087
$s_k'^2$	330.931	461.927	324.845	553.291	216.515	84.087
s_Q^2	374.225	545.479	380.137	619.509	232.891	86.422
$s_Q'^2$	374.225	545.479	380.137	619.509	232.891	86.422
Cov(K, Q)	298.760	422.537	299.807	563.409	200.191	53.260
Cov(K', Q')	298.760	422.537	299.807	563.409	200.191	53.260
$\rho(K, Q)$	0.849	0.842	0.853	0.962	0.892	0.625
$\rho(K', Q')$	0.849	0.842	0.853	0.962	0.892	0.625

4.3. Scatter Plot

In this section, Figures 9–11 show the scatter plots for red, green, and blue pixel colors after the application of the NPT in four distinct block sizes. The horizontal axis represents the current pixel value at position i , while the vertical axis indicates the adjacent pixel value one place to the right. The adjacent pixels are extracted from the first column to the last pixel column. Additionally, the various reflections over the vertical and horizontal axes can be observed, confirming Theorem 6. The three reflection combinations, along with the original positions, create an “x” figure, which is more prevalent in small pixel block sizes such as 2×2 and 4×4 .

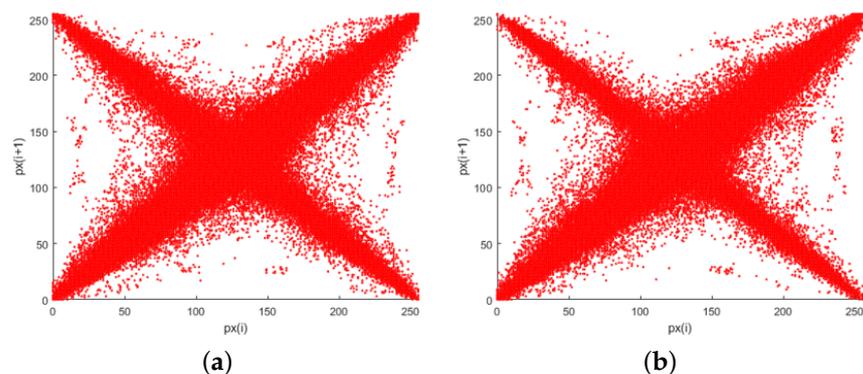


Figure 9. Cont.

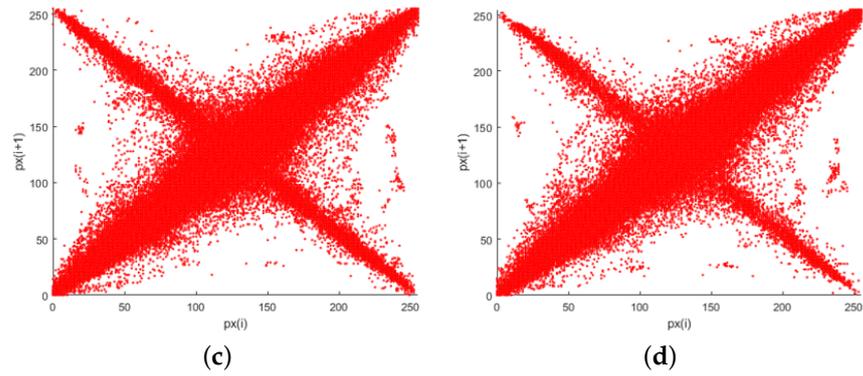


Figure 9. Resultant scatter plots of the red channel from Figure 5. (a) Red channel scatter plot from Figure 5a. (b) Red channel scatter plot from Figure 5b. (c) Red channel scatter plot from Figure 5c. (d) Red channel scatter plot from Figure 5d.

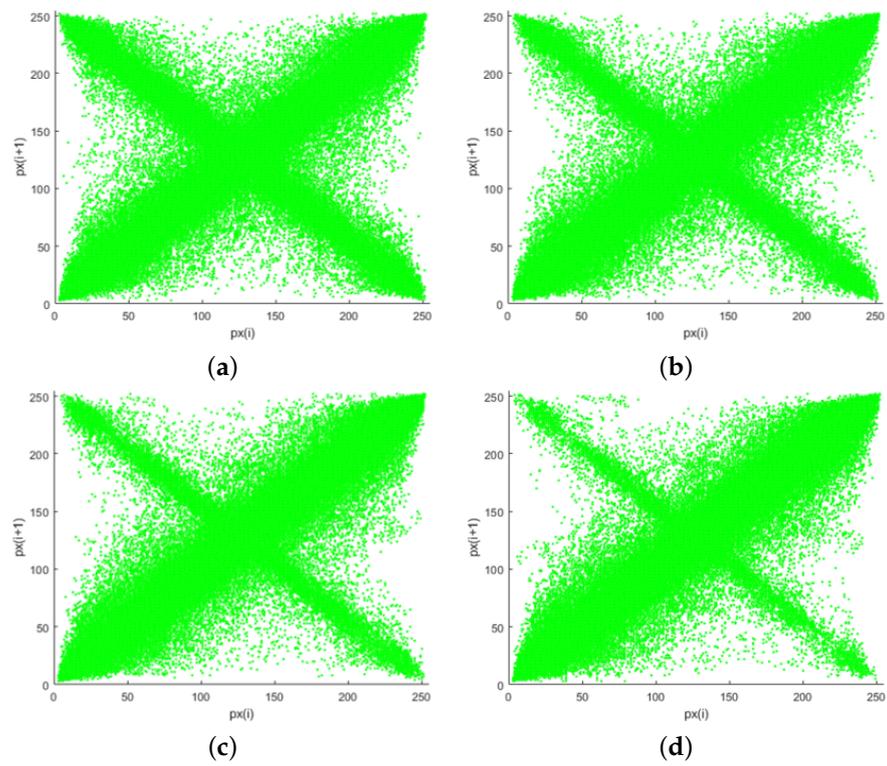


Figure 10. Resultant scatter plots of the green channel from Figure 5. (a) Green channel scatter plot from Figure 5a. (b) Green channel scatter plot from Figure 5b. (c) Green channel scatter plot from Figure 5c. (d) Green channel scatter plot from Figure 5d.

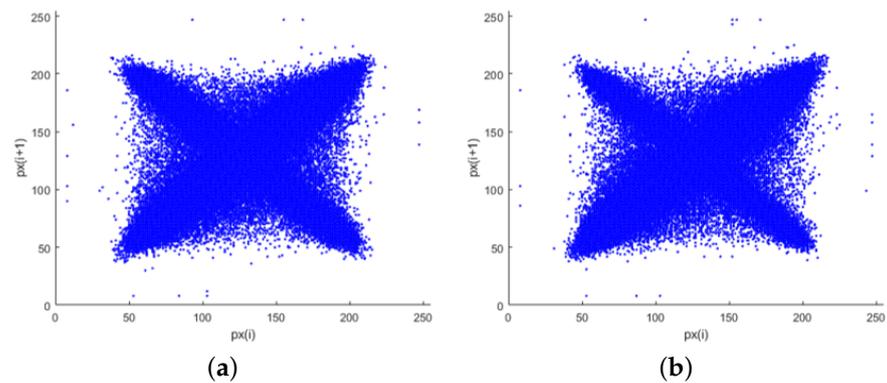


Figure 11. Cont.

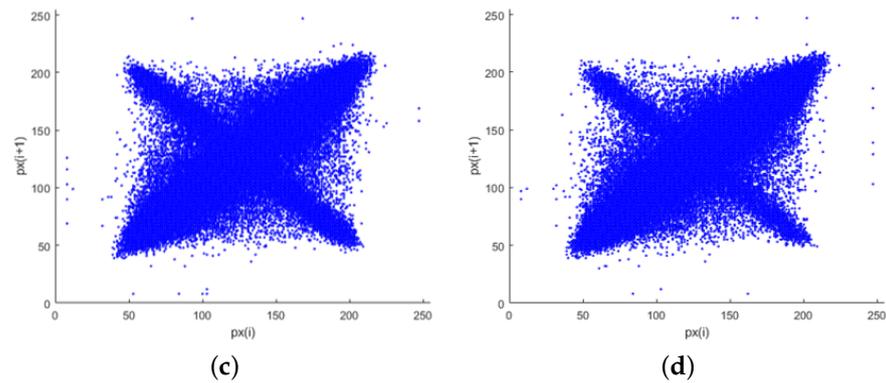


Figure 11. Resultant scatter plots of the blue channel from Figure 5. (a) Blue channel scatter plot from Figure 5a. (b) Blue channel scatter plot from Figure 5b. (c) Blue channel scatter plot from Figure 5c. (d) Blue channel scatter plot from Figure 5d.

5. Discussion

Following the results obtained from NPT encryption, a discussion of the findings is presented below.

- The histogram graph of an image after the NPT application displays a symmetric shape, centered around the intensity levels of 127–128. This symmetry arises because, for each pair of symmetric intensity levels (e.g., intensities 0 and 255), the expected values of their frequencies are identical. Furthermore, the expected value is equal to the average of the original frequencies of the two intensity levels before the NPT application.
- The theorem of the symmetric histogram assumes that the NPT is independently applied. However, in larger pixel block sizes, particularly those of 8×8 and greater, this independence is not rigorously maintained. The increased occurrence of pixels with the same intensity value in larger blocks may influence the independent application of the NPT. In such cases, multiple pixels sharing the same intensity level simultaneously are subject to the same single NPT application, resulting in a diminished symmetric appearance.
- The arithmetic mean of an encrypted pixel block using the NPT corresponds to the NPT of the original mean. Specifically, when $X = 1$, the new value becomes the complement of 255, considering both the integer and decimal parts of the mean. Conversely, if $X = 0$, the average remains unchanged.
- The variance, covariance, and correlation of a pixel block remain invariant under the NPT for any block size and magnitude measure. This was theoretically demonstrated and experimentally verified.
- Reflections are observed by plotting points of adjacent pixel values on a scatter plot after the NPT application. These reflections appear along one or two axes, specifically delimited by $x = 127$ and $y = 127$, with the origin point being $(127, 127)$. The double reflection occurs when the NPT is applied with $X = 1$ to both adjacent pixels. A single reflection occurs when the NPT operates with $X = 1$ over only one of the two adjacent pixels, and they belong to different pixel blocks.
- Given that plain images exhibit a high linear correlation, the pairs of adjacent pixels are similar to a line $y = x$ on the scatter plot. After the NPT application, a graph in the form of “x” emerges on the scatter plot, resulting from vertical and/or horizontal reflections. Points on the line $y = -x$ indicate a single reflection, and this occurs only in pixel pairs from different blocks. As the number of blocks decreases (and the block size increases), the number of pixels over this line also decreases.
- The single application of NPT preserves the initial correlation within each pixel block, even though NPT can alter pixel values. As a technique for image encryption by pixel blocks, it proves insufficient for safeguarding data when there is initially high correlation. Additional encryption procedures must be applied afterward to modify pixel values and concurrently reduce correlation.

- Conversely, the NPT does not affect the efficacy of image compression algorithms such as JPEG, where a high correlation is desirable in pixel blocks. Therefore, this encryption technique can be incorporated into cryptosystems that are compatible with compression.

Limitations and Future Directions

Conducting a theoretical analysis of the individual security of an encryption technique encounters limitations in deriving results that can apply to any image. The study of these limitations allows for a more informed understanding of the technique's applicability and the expected outcomes. The present work specifically examined the NPT within EtC systems, providing results on the histogram, mean, variance, covariance, and correlation that apply to any image, contrary to numerical analysis that reports results for specific images. However, it is crucial to acknowledge these limitations in future research works. Below, we describe some of them.

1. Entropy. The conclusion regarding a symmetric histogram in the image after the NPT may prompt further research into other measures based on the histogram, such as entropy. However, this obtained result alone cannot provide a complete theoretical analysis of entropy after the NPT application. Since information entropy considers the probability, $p(I = h)$, that a pixel color value, I , has a specific intensity level h , this work has demonstrated that the frequencies of intensity level, h , are the same as the intensity level $l \oplus h$, and are equal to the average of these two. Therefore, the probability would tend to $p(I = h) = p(I = h \oplus 255) = (l_h + l_{h \oplus 255}) / (2 \times W \times H)$. Consequently, the Shannon entropy would transition from $E(I) = -\sum_{i=0}^{255} p(I = i) \log_2 p(I = i)$ to approximately $E(I) = -2 \sum_{i=0}^{127} p(I = i) \log_2 p(I = i)$. This result does not offer clear information to conclude a reduction or increase in entropy.
2. Image correlation. The correlation result obtained in this work applies to pixel blocks, as the NPT operates at the pixel block level. Extending this procedure to obtain the pixel correlation of the entire image presents a challenge. While the correlation of pixel blocks remains consistent before and after encryption, it does not necessarily imply this behavior for the correlation of the entire image. If pixel-block values change post-encryption, even with invariant individual correlations, the correlation of the entire image considers all the image pixels. The difficulty is located in the neighborhood pixels across different pixel blocks. Particularly, when a pixel block is encrypted with $X = 1$ and an adjacent block with $X = 0$, the correlation between pixel blocks may change, as their values do not necessarily change in the same direction. This dynamic interaction between pixel blocks makes it challenging to compute the theoretical correlation of the entire image.
3. New encryption techniques. In the field of encryption schemes compatible with compression, there are two primary considerations: the security outcomes of the employed techniques and the impact of altering pixel values on compression performance. In the case of JPEG compression, it operates at the pixel block level. Preserving the correlation of the original image within pixel blocks is advantageous for its compression algorithm. This is why the NPT is employed for JPEG encryption, as it maintains pixel block correlations while altering the original values. However, it is noteworthy that the resulting distribution of pixel values does not approximate a uniform histogram. Producing new encryption techniques has the challenge of improving security and maintaining compression compatibility.

6. Conclusions

This paper presents a statistical analysis of encrypted images using the NPT technique, highlighting six theorems. These theorems were demonstrated and verified computationally to comprehend the security implications of applying the NPT. The resulting histogram of the image exhibits a symmetric shape because the expected frequencies of each pair of symmetric intensity levels are equal. Therefore, to achieve a uniform distribution, it is

required that the sum of frequencies for each pair of symmetric intensities be the same. Additionally, horizontal and vertical reflections occur for couples of adjacent pixels on the scatter plot. Furthermore, the NPT preserves the initial correlation within each pixel block. This observation is significant, given that the primary objective of cryptography is to disassociate information. Consequently, it is imperative to incorporate operations, either before or after the NPT application, which reduces correlation, as the NPT itself does not alter it. However, this weakness makes it compatible with EtC algorithms, as they operate effectively when the correlation remains high. In conclusion, the NPT exhibits security vulnerabilities when employed for image encryption at the pixel block level. It is necessary to incorporate additional encryption techniques alongside the NPT that not only modify pixel values but also decrease correlation and generate uniform histograms. The challenge lies in ensuring that these techniques are also compatible with compression.

Author Contributions: Conceptualization, methodology, formal analysis, investigation, visualization, writing—review and editing, data curation, software, validation, writing—original draft preparation M.A.C.-L., J.C.C.-E., V.M.S.-G. and R.F.-C.; resources, supervision, project administration, funding acquisition, J.C.C.-E. and V.M.S.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded in part by the economic support program of Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCyT), and the Secretaría de Investigación y Posgrado (SIP) of the Instituto Politécnico Nacional under grants no. SIP-20242497 and no. SIP-20241356.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon request.

Acknowledgments: The authors would like to thank the Instituto Politécnico Nacional of México (Secretaría Académica, SIP, COFAA, CIC, and CIDETEC), and the CONAHCyT for their support in the development of this work.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

NPT	negative–positive transformation
BDRV	Bernoulli discrete random variable
EtC	encryption-then-compression
DNPT	double negative positive transformation

References

1. El Saj, R.; Sedgh Gooya, E.; Alfalou, A.; Khalil, M. Privacy-Preserving Deep Neural Network Methods: Computational and Perceptual Methods—An Overview. *Electronics* **2021**, *10*, 1367. [[CrossRef](#)]
2. Singh, K.N.; Singh, A.K. Towards integrating image encryption with compression: A survey. *ACM Trans. Multimed. Comput. Commun. Appl.* **2022**, *18*, 89. [[CrossRef](#)]
3. Aryal, A.; Imaizumi, S.; Horiuchi, T.; Kiya, H. Integrated algorithm for block-permutation-based encryption with reversible data hiding. In Proceedings of the 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Kuala Lumpur, Malaysia, 12–15 December 2017; pp. 203–208. [[CrossRef](#)]
4. Imaizumi, S.; Kiya, H. A block-permutation-based encryption scheme with independent processing of RGB components. *IEICE Trans. Inf. Syst.* **2018**, *101*, 3150–3157. [[CrossRef](#)]
5. Aryal, A.; Imaizumi, S.; Horiuchi, T.; Kiya, H. Integrated Model of Image Protection Techniques. *J. Imaging* **2018**, *4*, 1. [[CrossRef](#)]
6. Imaizumi, S.; Ogasawara, T.; Kiya, H. Block-Permutation-Based Encryption Scheme with Enhanced Color Scrambling. In Proceedings of the Image Analysis: 20th Scandinavian Conference, SCIA 2017, Tromsø, Norway, 12–14 June 2017; Sharma, P., Bianchi, F.M., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 562–573.
7. Motomura, R.; Imaizumi, S.; Kiya, H. Reversible Data Hiding in Compressible Encrypted Images with Capacity Enhancement. *APSIPA Trans. Signal Inf. Proc.* **2023**, *12*, e31. [[CrossRef](#)]
8. Sirichotedumrong, W.; Kinoshita, Y.; Kiya, H. Pixel-Based Image Encryption without Key Management for Privacy-Preserving Deep Neural Networks. *IEEE Access* **2019**, *7*, 177844–177855. [[CrossRef](#)]

9. Ahmad, I.; Shin, S. Perceptual Encryption-based Privacy-Preserving Deep Learning for Medical Image Analysis. In Proceedings of the 2023 International Conference on Information Networking (ICOIN), Bangkok, Thailand, 11–14 January 2023; pp. 224–229. [\[CrossRef\]](#)
10. Kenta, K.; Masanori, K.; Shoko, I.; Sayaka, S.; Hitoshi, K. An Encryption-then-Compression System for JPEG/Motion JPEG Standard. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2015**, *E98.A*, 2238–2245. [\[CrossRef\]](#)
11. Zhang, B.; Xiao, D.; Xiang, Y. Robust Coding of Encrypted Images via 2D Compressed Sensing. *IEEE Trans. Multimed.* **2021**, *23*, 2656–2671. [\[CrossRef\]](#)
12. Shimizu, K.; Suzuki, T.; Kameyama, K. Cube-Based Encryption-then-Compression System for Video Sequences. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2018**, *E101.A*, 1815–1822. [\[CrossRef\]](#)
13. Li, P.; Lo, K.T. Survey on JPEG compatible joint image compression and encryption algorithms. *IET Signal Process.* **2020**, *14*, 475–488. [\[CrossRef\]](#)
14. Maungmaung, A.; Kiya, H. A protection method of trained CNN model with a secret key from unauthorized access. *APSIPA Trans. Signal Inf. Process.* **2021**, *10*, e10. [\[CrossRef\]](#)
15. Ahmad, I.; Choi, W.; Shin, S. Comprehensive Analysis of Compressible Perceptual Encryption Methods—Compression and Encryption Perspectives. *Sensors* **2023**, *23*, 4057. [\[CrossRef\]](#) [\[PubMed\]](#)
16. Zhang, B.; Xiao, D.; Wang, M.; Liang, J. Privacy-Preserving Compressed Sensing for Image Simultaneous Compression-Encryption Applications. In Proceedings of the 2021 Data Compression Conference (DCC), Snowbird, UT, USA, 23–26 March 2021; pp. 283–292. [\[CrossRef\]](#)
17. Zhang, C.; Fan, H.; Zhang, M.; Lu, H.; Li, M.; Liu, Y. Plaintext-related image encryption scheme without additional plaintext based on 2DCS. *Optik* **2023**, *272*, 170312. [\[CrossRef\]](#)
18. SaberiKamarposhti, M.; Ghorbani, A.; Yadollahi, M. A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. *Chaos Solitons Fractals* **2024**, *178*, 114361. [\[CrossRef\]](#)
19. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. [\[CrossRef\]](#)
20. Murillo-Escobar, M.A.; Meranza-Castillón, M.O.; López-Gutiérrez, R.M.; Cruz-Hernández, C. Suggested Integral Analysis for Chaos-Based Image Cryptosystems. *Entropy* **2019**, *21*, 815. [\[CrossRef\]](#)
21. Biban, G.; Chugh, R.; Panwar, A. Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix. *Chaos Solitons Fractals* **2023**, *170*, 113396. [\[CrossRef\]](#)
22. Moya-Albor, E.; Romero-Arellano, A.; Brieva, J.; Gomez-Coronel, S.L. Color Image Encryption Algorithm Based on a Chaotic Model Using the Modular Discrete Derivative and Langton's Ant. *Mathematics* **2023**, *11*, 2396. [\[CrossRef\]](#)
23. Sun, J.; Ma, Y.; Wang, Z.; Wang, Y. Dynamic analysis and cryptographic application of a 5D hyperbolic memristor-coupled neuron. *Nonlinear Dyn.* **2023**, *111*, 8751–8769. [\[CrossRef\]](#)
24. Lai, Q.; Zhang, H. A new image encryption method based on memristive hyperchaos. *Opt. Laser Technol.* **2023**, *166*, 109626. [\[CrossRef\]](#)
25. Lidong, L.; Jiang, D.; Wang, X.; Zhang, L.; Rong, X. A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing. *IEEE Access* **2020**, *8*, 210382–210399. [\[CrossRef\]](#)
26. Kiya, H.; Maung, A.P.M.; Kinoshita, Y.; Imaizumi, S.; Shiota, S. An overview of compressible and learnable image transformation with secret key and its applications. *APSIPA Trans. Signal Inf. Proc.* **2022**, *11*, e11. [\[CrossRef\]](#)
27. Puchala, D.; Stokfiszewski, K.; Yatsymirskyy, M. Image Statistics Preserving Encrypt-then-Compress Scheme Dedicated for JPEG Compression Standard. *Entropy* **2021**, *23*, 421. [\[CrossRef\]](#)
28. Ahmad, I.; Shin, S. A Perceptual Encryption-Based Image Communication System for Deep Learning-Based Tuberculosis Diagnosis Using Healthcare Cloud Services. *Electronics* **2022**, *11*, 2514. [\[CrossRef\]](#)
29. Chuman, T.; Kurihara, K.; Kiya, H. On the security of block scrambling-based ETC systems against jigsaw puzzle solver attacks. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017; pp. 2157–2161. [\[CrossRef\]](#)
30. Chuman, T.; Kurihara, K.; Kiya, H. Security evaluation for block scrambling-based ETC systems against extended jigsaw puzzle solver attacks. In Proceedings of the 2017 IEEE International Conference on Multimedia and Expo (ICME), Hong Kong, China, 10–14 July 2017; pp. 229–234. [\[CrossRef\]](#)
31. Iida, K.; Kiya, H. Privacy-Preserving Content-Based Image Retrieval Using Compressible Encrypted Images. *IEEE Access* **2020**, *8*, 200038–200050. [\[CrossRef\]](#)
32. Chuman, T.; Sirichotedumrong, W.; Kiya, H. Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images. *IEEE Trans. Inf. Forensic Secur.* **2019**, *14*, 1515–1525. [\[CrossRef\]](#)
33. Sirichotedumrong, W.; Kiya, H. Grayscale-based block scrambling image encryption using ycbcr color space for encryption-then-compression systems. *APSIPA Trans. Signal Inf. Process.* **2019**, *8*, e7. [\[CrossRef\]](#)
34. Hosny, K.M.; Zaki, M.A.; Lashin, N.A.; Fouda, M.M.; Hamza, H.M. Multimedia Security Using Encryption: A Survey. *IEEE Access* **2023**, *11*, 63027–63056. [\[CrossRef\]](#)
35. Kumar, A.; Dua, M. A GRU and chaos-based novel image encryption approach for transport images. *Multimed. Tools Appl.* **2023**, *82*, 18381–18408. [\[CrossRef\]](#)
36. Mamia, S.B.; Puteaux, P.; Puech, W.; Bouallegue, K. From Diffusion to Confusion of RGB Pixels Using a New Chaotic System for Color Image Encryption. *IEEE Access* **2023**, *11*, 49350–49366. [\[CrossRef\]](#)

37. Wroughton, J.; Cole, T. Distinguishing between binomial, hypergeometric and negative binomial distributions. *J. Stat. Educ.* **2013**, *21*, 1. [[CrossRef](#)]
38. Seong, J.H.; Seo, D.H. Wi-Fi fingerprint using radio map model based on MDLP and euclidean distance based on the Chi squared test. *Wirel. Netw.* **2019**, *25*, 3019–3027. [[CrossRef](#)]
39. Sei, Y.; Ohsuga, A. Privacy-preserving chi-squared test of independence for small samples. *BioData Min.* **2021**, *14*, 6. [[CrossRef](#)]
40. Musanna, F.; Dangwal, D.; Kumar, S. Novel image encryption algorithm using fractional chaos and cellular neural network. *J. Ambient. Intell. Humaniz. Comput.* **2022**, *8*, 2205–2226. [[CrossRef](#)]
41. Burger, W.; Burge, M.J. Histograms and Image Statistics. In *Digital Image Processing: An Algorithmic Introduction*, 3rd ed.; Springer International Publishing: Cham, Switzerland, 2022; pp. 29–48. [[CrossRef](#)]
42. Kammoo, P.; Neammanee, K.; Laipaporn, K. The local limit theorem for general weighted sums of Bernoulli random variables. *Commun. Stat. Theory Methods* **2023**, *0*, 1–9. [[CrossRef](#)]
43. Evans, M.J.; Rosenthal, J.S. *Probability and Statistics: The Science of Uncertainty*, 2nd ed.; W.H. Freeman: New York, NY, USA, 2009; pp. 159–166.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.