

A New Hybrid Image Encryption Model Based on Custom Logic Functions and Dynamic Chaotic Keys

Adil Ibrahim Khalil^{1*} , Adel A. Abed Al Wahaab Al Imam² 

^{1,2} College of Education for Pure Science, University of Diyala, Diyala 32001, Iraq, <https://ror.org/01eb5yv70>

Corresponding author: Adil Ibrahim Khalil,
College of Education for Pure Science,
University of Diyala, Diyala, Iraq
dr.adil.khali@uodiyala.edu.iq



Article History:
Received: 23.07.2025
Revised: 25.10.2025
Accepted: 27.10.2025
Published Online: 11.12.2025

ABSTRACT

Any secure image encryption system needs to distort the statistical and visual structure of the image to prevent unauthorized access. Unlike traditional chaos-XOR methods, this paper presents a new hybrid image encryption model based on dynamic chaotic key generation, combined with two novel dedicated bit-level logic functions. The proposed model includes image pre-processing steps, such as flattening color channels and pixel shuffling, to break down the spatial structure. Bit-level nonlinear transformations are then applied using dedicated bit-level logic functions (FLF and FOF). The Bogdanov scheme was used as the chaotic key generator. The image encryption quality was evaluated against four state-of-the-art models using Entropy, NPCR, UACI, PSNR, and SSIM, along with visual analysis of histograms and correlation indices. The experimental results reported an average Entropy value of 7.95. NPCR rate and UACI values were 99.61% and 33.2% respectively. The correlation coefficient was 0.0046. The SSIM remained at 1.0, while the average encryption execution was 0.47 seconds. These results demonstrate that the proposed system can achieve a high level of visual security. This study represents a qualitative and quantitative contribution to the development of secure digital image processing methods.

Keywords: Image processing, Bogdanov scheme, FLF, FOF, Chaotic key

1. Introduction

Medicine, security, and communications are examples of fields that can be developed using image processing techniques [1]–[3]. Some image processing applications are vulnerable to unauthorized access. Therefore, image processing stages may require an internal data encryption model to provide protection against unauthorized access. Any secure image encryption mode is designed to convert images into an encrypted format that is difficult for unauthorized individuals to understand. Multiple methods have been proposed for image encryption, including traditional methods such as symmetric and asymmetric encryption, as well as more advanced methods like chaos-based encryption. Therefore, image encryption technology has become an important part of information security to protect sensitive data [4], [5]. In certain special cases, such as resource-limited environments, the challenge becomes more complex. As a result of such reasons, the available algorithms may not be able to operate efficiently [6]. Several encryption algorithms have been proposed. However, many of them are not suitable for image data due to the optical integrity of the image data [7]. Furthermore, various chaotic algorithms show insufficient diffusion and confusion when using XOR operations [8], [9]. Additionally, the process of retrieving the original image after encryption may be affected by noise during transmission [10].

It is worth mentioning that efforts have been made to address the use of chaotic models for image encryption [11]–[13]. These contributions often relied on simple classical maps and XOR operations. In contrast, several previous studies investigated the mathematical structure of encryption without focusing on the structural analysis of the image or texture patterns [14]–[16]. For instance, a symmetric key encryption algorithm based on the logistic map has been presented by Wang et al. [17]. Their algorithm did not provide sufficient resistance against differential attacks (NPCR/UACI less than 99%). Zhou et al. [12] proposed a combination of Henon and Tent maps for key generation. The encryption result of this study remained linear through XOR only, without support for nonlinear operations or Feistel-based architecture.

In addition, a chaotic key from a logistic map has been utilized by Patel and Veeramalai [18] in their study to encrypt medical images. This study does not address partial corruption, such as noise. Furthermore, metrics such as PSNR or SSIM were not used to evaluate image encryption performance. The study of Hanif et al. [19] used a chaotic algorithm based on permutation and substitution. This study also investigates the static key structures. Yuan et al. [20] developed an XOR-based system with a Tent map for practical random number generation. The model generates a random key without incorporating any Boolean functions or multiple encryption layers, making it reproducible. Pourasad et al. presented a digital image encryption method based on chaos theory [21]. This work generates random chaotic sequences and discrete wavelet transform (DWT) structures.

It is worth noting that the use of DWT may introduce computational complexity for large images. Therefore, the algorithm may not be suitable for real-time applications or low-resource devices. A chaotic iteration of dragon fractal shapes (ChDrFr) for encryption, with filters to enhance image quality, was the objective of another study [22]. The results of this study enhanced random dispersion in pixel distribution and increased resistance to statistical attacks. However, this study did not provide results regarding the quality of the optical properties. In addition, other researchers presented a model that combines a chaotic Bogdanov map with the anti-asynchronous property of the Chain dynamical system [23]. The study aimed to generate encryption keys with high randomness and advanced mathematical complexity. This study also demonstrated Bogdanov's algorithm's ability to generate strong keys. However, the study did not include tests in non-ideal environments, such as the presence of noise or partial image loss.

Algorithms such as KASUMI are used widely in 3G cellular networks. These algorithms are based on the Feistel structure. Such a structure consists of binary-level implementations of subfunctions, including FL, FO, and FI, as presented in [24]. In contrast, the KASUMI algorithm is not compatible with dynamic, chaotic keys. It was designed to investigate textual data rather than visual data. Furthermore, certain chaotic algorithms that rely only on XOR operations have poor diffusion and confusion, particularly when the same seed values are used repeatedly [8], [25]. From another perspective, sensitive applications such as those involving military or medical images are vulnerable to image corruption due to errors or noise in the encrypted image transmission.

The research gap in the field of digital image encryption is related to the lack of algorithms that combine two essential elements. On one hand, the use of complex chaotic schemes, such as the Bogdanov map. The Bogdanov map provides more diverse dynamic behavior and a larger key space. This way may enhance encryption strength compared to traditional maps. On the other hand, the integration of bit-level logic functions is inspired by cryptographic algorithms such as KASUMI. It generates large-scale internal randomness within the image. Such an idea may outperform the capabilities of simple linear operations such as XOR. Additionally, traditional algorithms often overlook the structural properties of digital images. As a result, this can lead to data distortion or loss of information during the decryption process. Furthermore, traditional encryption techniques typically do not consider the resistance to noise or partial image damage [26]. Thus, it is essential to have encryption models that can retrieve images in unexpected situations.

To address these challenges, this paper presents a novel hybrid digital image encryption model that leverages the visual and statistical properties of the image. This model combines the generation of chaotic keys using the Bogdanov scheme and the application of dedicated bit-level logical functions. These functions are referred to as Feistel-Like Function (FLF) and Feistel-Oriented Function (FOF). The structure of FLF and FOF functions is similar to image processing filters. These functions could be used to enhance internal blurring and introduce large-scale nonlinear randomness within encrypted image data. The proposed model addresses the weakness in many conventional systems by reshaping the spectral and spatial structure of the image before and during encryption. Thus, the proposed model could be considered as an extension of *secure image processing* concepts, rather than a standalone encryption system. Another objective of this paper is to evaluate the proposed model's ability to process noisy images. To do that, the simulation of real-world environments was investigated when images are subject to partial loss or distortion. Our proposed model aims to preserve the basic optical properties of the decrypted image, even in the presence of salt-and-pepper noise in unreliable networks.

In summary, this study contributes to the field of digital image processing by introducing a novel hybrid model that integrates a chaotic key scheme with two specialized bit-level logic functions (FLF and FOF). The propagation and confusion characteristics of the encryption process will be enhanced due to such integration. Therefore, the proposed model's result may provide a high level of optical security and robustness against noise and partial data corruption.

2. Material and Theoretical Background

The structure of the digital image, pixel distribution, and image statistical properties are the fundamental concepts of our proposed encryption model. The methodology and theoretical steps to build the proposed image encryption model are given in the next sections.

2.1 Image Visual Properties and Processing Objectives

In this study, PNG color images were evaluated, as it is a lossless compression format. This format preserves the original pixel values, allowing for the accurate evaluation of statistical metrics. The image contains three color channels (R, G, and B). Each channel has a different statistical distribution. Images are characterized by spatial redundancy between pixels and correlation between channels. Considering these properties, encryption increases the robustness of the proposed algorithm against statistical analysis attacks. Therefore, techniques similar to "pre-transformations" have been adopted, such as flattening the color matrix to a 2D shape, reordering pixels to break the spectral and spatial structure, and encryption is performed at each pixel (not only at the block level). Pre-encoding phases are designed to be similar to image processing steps.

2.2 Proposed Model Structure

Fig. 1 presents a flowchart of the proposed model. The model is based on a hybrid architecture of three main components: 1) A dynamic chaotic key generated using the Bogdanov map. 2) Linear and nonlinear processing operations, including pixel shifting and XOR operations.

3) Custom logic functions (FLF and FOF) are implemented at the bit level to enhance diffusion and blurring. The algorithm is applied to three-channel color (RGB) images after converting them to a flat matrix. Each color element is encoded separately.

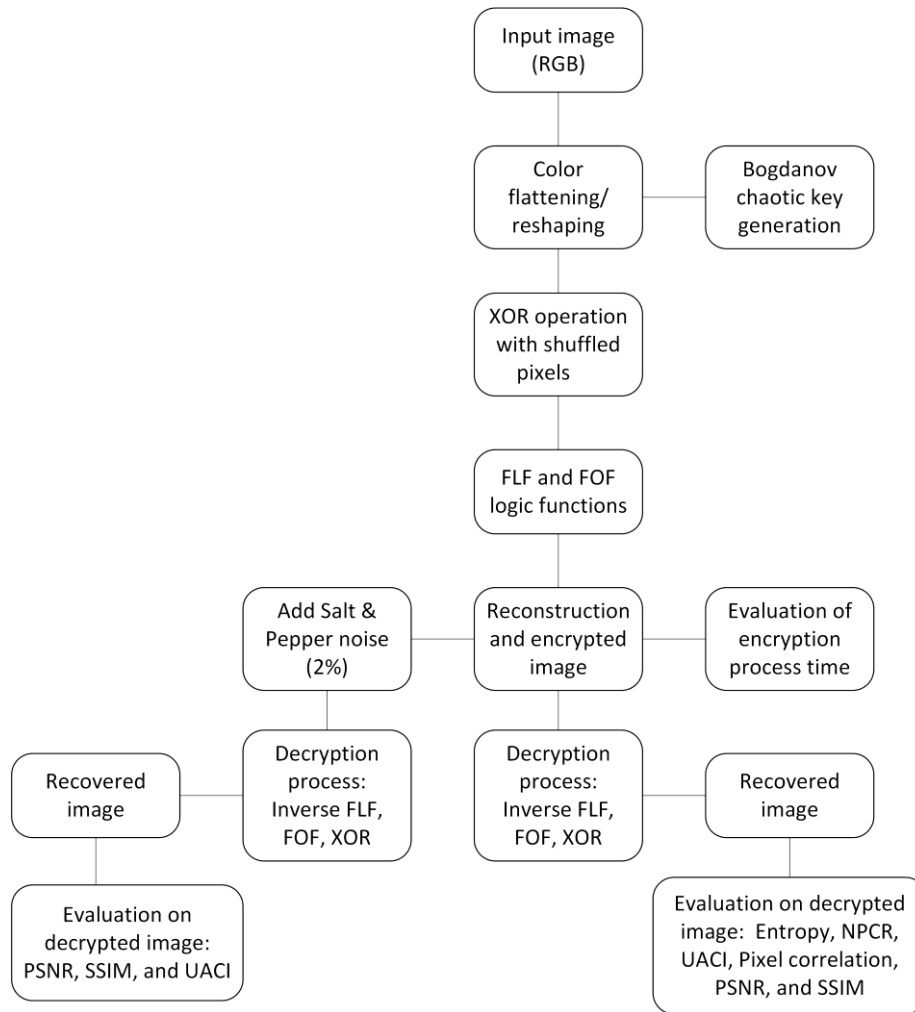


Figure 1. Flowchart of the proposed hybrid image encryption model.

2.3 Key Generation Using the Bogdanov Scheme

Cryptography and mathematical coding techniques play an important role in enhancing information security. Therefore, efforts have been made to use mathematical models to achieve high levels of security [27]. In contrast, this study proposes a chaotic approach based on Bogdanov's dynamic key generation map and dedicated bit-level logic functions to achieve high diffusion and confusion in the digital image. Thus, the proposed model offers a complementary approach to these mathematical methods, focusing on processing digital images rather than textual or numerical data. The Bogdanov method produces a chaotic key. The key generation method is based on two iterative equations, as shown below:

$$x_{n+1} = x_n + y_n \quad (1)$$

$$y_{n+1} = y_n + e \cdot y_n + k \cdot x_n \cdot (x_n - 1) + m \cdot x_n \cdot y_n \quad (2)$$

where $e=0.01$, $m=0.1$, and $k=0.295$ are three constants. Furthermore, $x_0 = 0.5$ and $y_0 = 0.9$ are two initial values. The result values are then converted to numerical values between 0 and 255 using quantization to obtain 8-bit key as shown in Equation 3:

$$K_i = \text{round}(255 \times |x_i \bmod 1|) \quad (3)$$

These values are then divided into subkeys that are used inside the FLF and FOF functions. The results demonstrated that the keys provide strong randomness properties and a large key space (NIST SP800-22 test).

The chaotic Bogdanov key was chosen due to its high suitability for image encryption applications. This property yields a large effective key space under finite-precision quantization and good stability when quantified to 8 bits. Unlike traditional logistic/tent maps, the Bogdanov scheme provides high variance across iterations. In the proposed model, the key is dynamically updated to avoid reuse. Such a step enhances randomness and reduces correlation between image pixels.

2.4 Design of FLF and FOF Functions

FOF operates on three consecutive rounds of nonlinear encryption using keys that are dynamically created using the Bogdanov algorithm. For each round, a series of logical operations is performed. These operations include calls to dedicated binary substitution tables (S7 and S9), as well as extension, truncation, and XOR gate interlocking. The FLF function has been developed in a Feistel-like microstructure. It performs logical operations (AND, OR, XOR and ROL) on the two halves of a binary block alternately to generate dynamically changing internal noise. This function is similar to a logical filter that is applied to a binary block level before merging the final output. This implementation achieves high levels of randomness, thereby enhancing the algorithm's resistance to statistical analysis and attacks. Such properties distinguish our proposed model from traditional systems that rely only on XOR.

2.4.1 The FLF function

FLF function is built in a manner that simulates the work of edge detection filters (such as Sobel and Laplacian). Logical operations are performed at the bit level to create a "logical blur" in the image that helps break visual patterns. FLF is a bidirectional logic encryption function that splits the input block into two halves (32 bits per half) and performs logical operations, as shown in Algorithm 1.

Algorithm 1. FLF algorithm

1	Dividing the binary string into Bin11 and Bin12 (32 bits each)
2	BKa = Bin11 AND KL1, where KL1 refers to key left part 1
3	BKa = ROL (BKa, 1), where ROL means rotate left
4	Bin12 = Bin12 XOR BKa
5	Tmp = Bin12 OR KL2 where KL2 refers to key left part 2
6	Tmp = ROL(tmp, 1)
7	Bin11 = bin11 XOR Tmp
8	Buf = Bin11 + Bin12

Both keys, KL1 and KL2, are internal subkeys derived from the main chaotic key, generated using the Bogdanov scheme. It is worth noting that the structure of FLF is similar to the FL functions in the KASUMI algorithm; however, it has been optimized for operation in a chaotic environment and with image data.

2.4.2 The FOF function

FOF is applied to a series of adjacent blocks and interacts with their values. It is similar to a non-linear convolution process. FOF relies on three internal rounds involving the keys KO(i), KI(i), and implementation of custom nonlinear functions S-Boxes (S7: a 128-element substitution table and S9: A 512-element substitution table). The S7 and S9 functions were chosen to be equivalent to complex activation functions in image processing networks. Operations are performed by alternating between half-blocks and using directed XOR operations to generate a final, unpredictable output.

2.5 Encryption Algorithm

The steps shown in Algorithm 2 below are not typical digital encryption operations but rather serve as image processing procedures at the optical level. These steps rearrange image components in a way that breaks repetitive patterns and weakens the original image structure. Dedicated logical filters are used, performing functions similar to those used in spectral transforms such as DCT or Wavelet, but implemented at the bit level. Thus, each encryption step performs a dual role: encryption on the one hand, and optical structural processing on the other, to achieve a higher level of optical security.

Algorithm 2. Steps of the proposed Encryption model

1	Reading the image and converting it to a three-dimensional (RGB) matrix.
2	Flattening the matrix to a two-dimensional $N \times 3$ matrix.
3	Generate a chaotic key using the Bogdanov scheme
4	Using a permutation function to generate a shuffled pixel from chaotic strings generated by a Bogdanov map.
5	Applying the XOR operation between the resulting chaotic keys and the rearranged pixels.
6	Applying the FLF and FOF functions to each 32-bit data block.
7	Resampling the image and storing it in PNG format.

2.6 Decryption Steps

The decryption process relies on recovering the original pixel order, as shown below:

- 1) The FLF and FOF functions are applied to the encrypted image in reverse order.

- 2) Applying the XOR operation using the same chaotic keys.
- 3) The original image is restored using reverse permutation.

2.7 Evaluation Methodology

To compute the performance of the proposed model, several statistical metrics were used for this purpose. These tools are an effective way to measure the effectiveness of the proposed model in distorting the visual and statistical properties of the original image. Furthermore, some of these indicators demonstrate the proposed model's ability to preserve the quality of the decrypted image.

Entropy Index (H): Entropy measures the degree of uncertainty. In cryptography, Entropy measures the uncertainty in the distribution of color values within the encrypted image. An entropy value close to 8 indicates an unpredictable distribution [28]. The value of Entropy is calculated as follows:

$$H = - \sum_{i=0}^{255} p_i \log_2 p_i, \quad (4)$$

where p_i is the probability of the gray value.

Number of Pixel Change Rate (NPCR): NPCR is used in image processing to measure the sensitivity of an encryption method to any alterations in the original image. An NPCR value close to the ideal value of 100% reflects the algorithm's robustness in propagating changes and then higher resistance to differential attacks. The value of NPCR is calculated as shown in Equation 5.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \quad (5)$$

where M and N represent the image dimensions.

Unified Average Changing Intensity (UACI): Measures the spectral differences between two similar images after encryption. This metric shows how effectively the algorithm changes the overall appearance of the image.

$$UACI = \frac{1}{M \times N} \sum \frac{|img_1 - img_2|}{255} \times 100, \quad (6)$$

where img_1 and img_2 are two encrypted images. The total number of pixels is represented by $M \times N$. The absolute difference for each pixel is represented by $|img_1 - img_2|$.

Correlation Coefficient (r): It measures the statistical relationship between neighboring pixels in an image. Values close to zero indicate that the algorithm is successful in breaking the structural correlations of the image. Given two images or two sets of pixel values $X = \{x_1, x_2, \dots, x_n\}$ and $Y = \{y_1, y_2, \dots, y_n\}$, the correlation coefficient is computed as follows:

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \cdot \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}, \quad (7)$$

where \bar{x} is the mean value of X and \bar{y} represents the mean value of Y .

Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM): These metrics assess the quality of the decoded image in comparison to the original. PSNR measures the numerical loss in the signal, while SSIM measures the structural similarity between the two images. PSNR is computed as shown in Equations 8 and 9, while SSIM is calculated as provided by Equation 10.

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right) \quad (8)$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I(i,j) - K(i,j)]^2 \quad (9)$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \quad (10)$$

where μ_x, μ_y are the mean of images x and y . σ_x^2, σ_y^2 are the variance of images x and y . C_1, C_2 are two small constants.

Additionally, a simulation of noise or data loss that may occur during image transmission over unreliable channels was conducted. This was done by adding Salt and Pepper noise to the encrypted image. The decrypted image was evaluated using PSNR, SSIM, and UACI. Therefore, the proposed model performs the encryption process and provides an additional feature for processing damaged images.

2.8 Algorithmic Summary of the Proposed Model

The basic steps of the proposed image encryption and decryption model are summarized as shown in Algorithm 3.

2.9 Statistical and Experimental Setup

A paired t-test was conducted to compute a performance comparison between the results of the proposed model and the results of the reference algorithms. The average performance metrics (Entropy, NPCR, UACI, PSNR, and SSIM) of twenty

independent experiments for each model were evaluated. For each statistical analysis, a p-value less than 0.05 was considered statistically significant. The statistical properties of the keys generated by the proposed model were evaluated using the NIST SP800-22 standard randomness test. Additionally, all experiments were conducted on a system equipped with an Intel Core i7-2600 CPU at 2.60 GHz, 16 GB of RAM, and Windows 10 (64-bit), utilizing **Python 3.10**. To ensure fair comparison, the proposed model and all reference algorithms were implemented using the same parameter settings and operating conditions. The average time reported in this study represents only the computation time required for the encryption algorithm. It is the duration between the start and end of the encryption function. This function does not include key generation, image loading, or file I/O operations.

Algorithm 3. Summary of the proposed model

1	Generate initial values using a chaotic Bogdanov map and a secret key.
2	Produce an eight-bit key stream after executing several cycles to remove transitions.
3	Flatten the RGB channels and reorder the pixels according to a chaotic sequence.
4	Perform an XOR operation followed by nonlinear logic transformations (FLF and FOF) to increase diffusion and confusion.
5	Introduce salt-and-pepper noise to test the robustness of the proposed system.
6	Perform the inverse operations in the same order to restore the original image.
7	Calculate statistical and visual performance indicators to estimate the quality of the proposed Model: Entropy, NPCR, UACI, PSNR, and SSIM.

3. Results and Discussion

Figure 2 shows the application of the proposed encryption model to an example image. It is clear from this Figure that the algorithm successfully destroyed all visual and color patterns of the original image. One can notice that there are no visually distinguishable features or details. This result confirms the effectiveness of the nonlinear encryption steps. Furthermore, the application of FLF and FOF functions demonstrates their ability to reduce the spatial and spectral correlations of image data.

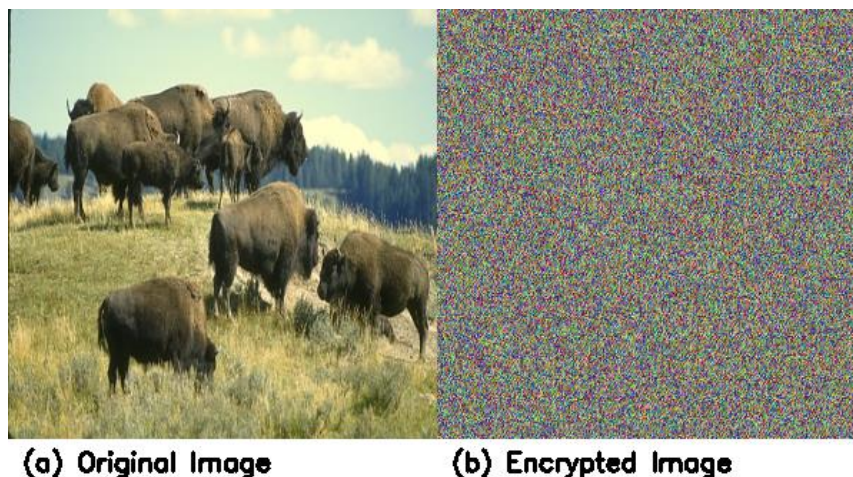


Figure 2. Example of applying the proposed model to a test image. (a) Original image, and (b) the encrypted image

Figure 3 demonstrates the correlation map between the adjacent pixels of the original image and the encrypted image. From this Figure, it is evident that the scattered points are predominantly located along a diagonal line, as shown in Figure 3(a). Such a distribution indicates a strong correlation between the neighboring pixels. This is a natural behavior in unencrypted images due to the spatial symmetry. In Figure 3 (b), the points appear to be distributed randomly across the various regions of the graph. Thus, this finding means a loss of regular pattern. Therefore, a clear breakdown in the statistical correlation between neighboring pixels could be noticed due to the encryption process. This result reflects the effectiveness of our proposed model in distorting the visual structure of the image by breaking up local patterns and reducing predictability. This is due to the effectiveness of FLF and FOF logic functions in producing strong nonlinear distortion at the bit level.

Figure 4 demonstrates the visual analysis of the histogram related to three color channels (red, green, and blue) in an RGB image before and after encoding. The original histogram in Figure 4(a) displays clear peaks for each color channel. This reveals the presence of a distinct color pattern and the dominance of specific colors in the scene. This type of distribution is an easy target for statistical analysis attacks. It can be exploited to infer the content of the image or some of its components. The histogram related to the encrypted image is presented in Figure 4 (b). One can see from this Figure a random distribution

across all levels, without clear peaks for any color. The histogram appeared randomly balanced in all color channels (R, G, B), indicating the decomposition of the original spectral structure. This helps prevent the recovery of the original patterns. The homogeneous distribution indicates that the proposed algorithm enhances the randomness of the image, making it difficult to infer its content through statistical analysis. The absence of a symmetric distribution after the encryption process demonstrates the ability of our proposed model to remove the distinctive spectral structure of the original image. Therefore, the proposed model of this study reduces the possibility of retrieving visual information from the encrypted image, thereby increasing visual security.

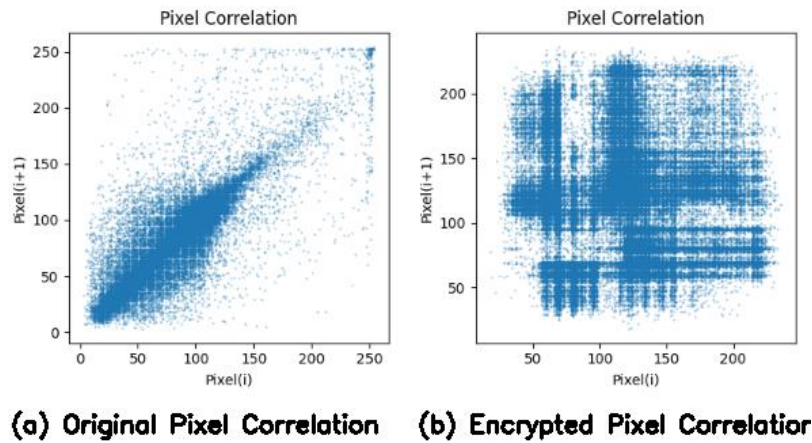


Figure 3. Neighboring pixels correlation. (a) Original image and (b) the encrypted image.

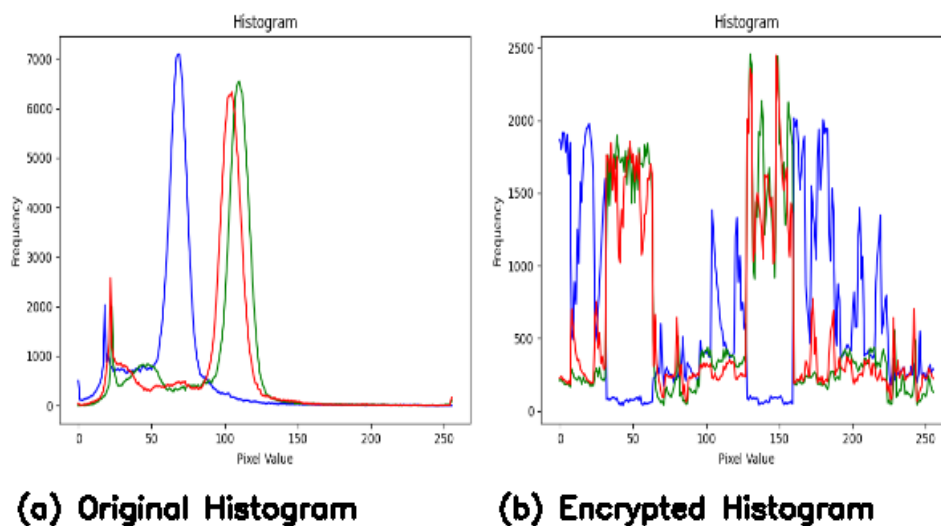


Figure 4. Histogram representation. (a) Original image. (b) Encrypted image.

The proposed model was evaluated using a set of statistical metrics to approve the secure image processing. The results presented in this paper include encryption using both our proposed model (Bogdanov + FLF/FOF) and four state-of-the-art algorithms, such as Henon, Tent, Hyperchaotic Lorenz, and LogisticXOR. The proposed and the reference models were applied to a set of 20 different images. Table 1 shows the average results of our model and these reference models using a set of statistical metrics. According to this Table, the average NPCR of our proposed model was 99.6%, indicating that the algorithm responds to minor changes in the original image. This behavior enhances the diffusion property, making it difficult to reconstruct the original image from the encrypted one. According to the study of Wang et al. [17], any algorithm with an NPCR value exceeding 99% is considered to have high security performance. In contrast, the average value of UACI exceeded 33%. Therefore, the results that are shown in Table 1 indicate that the encrypted image differs significantly in color intensity from the original one.

It is obvious from Table 1 that the application of our proposed Bogdanov+FLF/FOF model to encrypt an image achieved an average entropy value of **7.9561**. This value indicates a high degree of randomness in the pixel distribution. It has been reported that a high entropy value contributes to the production of an unpredictable pattern [8]. This result indicates that the encryption successfully hides the original structure of the image. In addition, the reference algorithms achieved a slightly higher entropy value than our proposed model. However, this may not reflect a security advantage, because some algorithms rely on linear XOR operations, such as LogisticXOR. Studies such as Li et al. [8] have demonstrated that it is vulnerable to cracking in some scenarios due to poor diffusion and confusion. Furthermore, the average correlation coefficient was

approximately 0.0046. This result confirms that the proposed model successfully broke down the correlation between neighboring pixels. In contrast, the average SSIM was constant at 1.0. This result reveals that the decoded images were similar to the original images. This reflects an efficient lossless decryption model. Finally, the average execution time for a 256×256 image was only 0.476 seconds. Such an execution time makes the proposed model suitable for real-time applications.

From another perspective, our proposed model combines nonlinear logical operations (FLF and FOF) with a Bogdanov chaotic key. Therefore, the result of the cryptographic pattern was more resistant to statistical analysis. FLF is responsible for enhancing diffusion within bits via simple logical operations such as XOR, AND, OR, and Rotation to distribute the change from one bit to multiple bits [29]. In addition, FOF adds a layer of nonlinearity (confusion) that prevents statistical and differential analysis [30]. Furthermore, the close performance of our proposed model to the reference methods demonstrates greater efficiency in preserving visual properties after encryption and decryption. Furthermore, a paired t-test was performed to compare the proposed model's results with those of each baseline method. All obtained p-values were higher than 0.05. These results confirm that there are no significant differences between the performance of the proposed model and the reference models in terms of quantitative metrics. In addition, the unique hybrid architecture of the proposed model provides flexibility and effectiveness in changing and noisy environments. Therefore, it can be concluded that the integration of Bogdanov chaotic dynamics with the customized bitwise logic layers (FLF/FOF) provides encryption quality comparable to established chaotic and classical standards models, while maintaining structural novelty and computational efficiency.

Table 1. The proposed Model's performance results against four state-of-the-art methods

Model	Entropy Encrypted	NPCR	UACI	Correlation Encrypted	PSNR Decrypted	SSIM Decrypted	Encrypted time (s)
Henon	8.0229	99.6112	33.0838	-0.0007	∞ (lossless)	1.0000	0.4809
Tent	8.0228	99.6017	33.0765	-0.0006	∞ (lossless)	1.0000	0.4665
HyperLorenz	8.0229	99.6120	33.1134	0.0004	∞ (lossless)	1.0000	0.4617
LogisticXOR	8.0229	99.6033	33.0904	0.0002	∞ (lossless)	1.0000	0.4666
Our Model	7.9561	99.6136	33.2851	0.0046	∞ (lossless)	1.0000	0.4769

The algorithm's resilience against partial corruption was tested by applying 2% salt-and-pepper noise to the encrypted image. Figure 5 presents the result of the decrypted image after applying noise compared to the original decrypted one. Consequently, our model demonstrated high tolerance in noisy conditions.

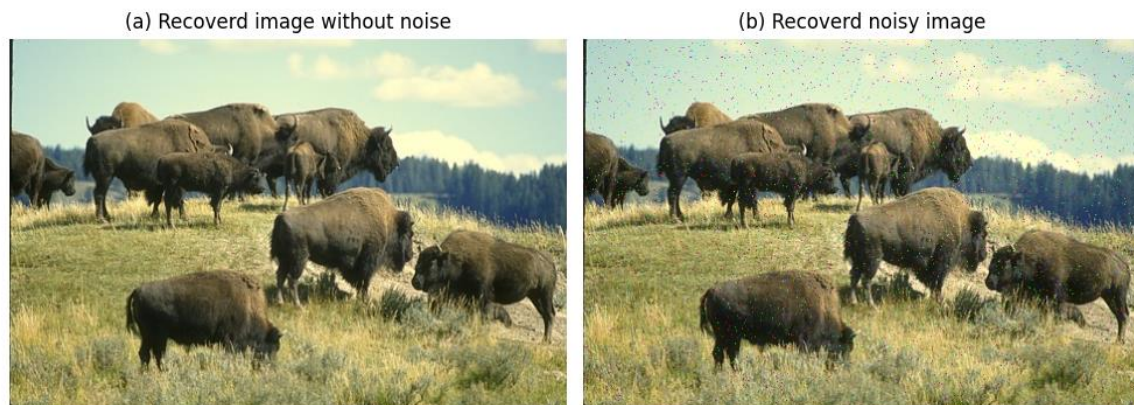


Figure 5. The results of the recovered image without noise are compared to the recovered noisy image by applying the proposed model.

Additionally, the statistical indicators of the noisy decrypted image with a 2% salt-and-pepper noise are presented in Table 2. It is clear from this table that a low UACI indicates that the noise effect is limited compared to the encryption. By testing the encrypted image with salt-and-pepper noise, we found that the proposed model can recover the image with satisfactory quality (PSNR \approx 24.5 dB, SSIM \approx 0.80). Such results were not achieved by most conventional algorithms based on XOR or simple chaotic maps. This demonstrates that our proposed model is not just an encryption system, but also a cryptographic image processing system. In addition, the proposed model has demonstrated its ability to handle data loss in unreliable transmission environments. These properties offer significant advantages in applications like medicine, surveillance, and wireless sensor networks. For instance, noise and partial distortion resistance in any cryptography model are important criteria in medical applications [10].

The model demonstrates that it is not only robust against attacks but also maintains high resilience against partial corruption during transmission. This confirms the importance of our proposed model in image processing applications, such as those in

wireless networks. Many previous studies, such as the one by [18], did not address the processing of damaged images. This study addressed the issue by introducing Salt and Pepper noise and verifying the ability of our system to recover images with acceptable quality. Compared to the results of previous studies [12], [17], our algorithm achieves similar or better NPCR and Entropy values. However, the FLF and FOF structures provided results that are more resistant to statistical analysis. Traditional XOR algorithms fail under corruption. The two logical functions, FLF and FOF, constitute a qualitative contribution to the architectural structure of the proposed model. These functions introduce bit-level logical randomness, similar to the effect of edge detection filters (such as Sobel and Laplacian), but in a way that achieves encryption in addition to visual processing. This combination of processing and encryption principles creates what is known as "structural encryption," which not only alters values but also reconfigures the spectral structure of the image. This approach is rarely discussed in the current literature. For example, it has been reported that the importance of integrating advanced chaotic maps, such as Bogdanov, with dynamic properties to ensure key diversity, as shown in [18]. However, the combination with structural logical operations was not investigated.

Table 2. The statistical indicators of the decrypted noisy image

Decrypted noisy image	PSNR	SSIM	UACI
38092_noisy.png	24.51 dB	0.8006	0.77%

4. Conclusion

To the best of our knowledge, this study is considered the first one conducted to integrate security concepts with image processing techniques. The manual implementation of FLF and FOF functions proved its ability to combine complex logical operations with the use of nonlinear substitution tables. Thus, the proposed model is enhanced to analyze visual and statistical patterns of images. The applications of the proposed model to image datasets demonstrate high performance in security and randomness metrics. Furthermore, this study provided image processing properties, including noise response, spatial disorder, and post-decryption optical stability. These results are promising for a wide use in sensitive and visual application environments. In addition, the structure of FLF and FOF contributes to efficient noise and bit-level diffusion. Therefore, the proposed model is comparable to traditional XOR-based models and resistant to analytical attacks. The use of the Bogdanov scheme as a key generator enhances the security compared to traditional chaotic maps. Furthermore, the proposed model takes into account the structural properties of the image, including spatial and spectral redundancy. This enhances the model's resistance to attacks, making it suitable for applications such as medical, surveillance, and remote sensing.

Several future ideas can be developed from this work. First, the encryption algorithm could be extended to include multi-layer chaotic systems, thereby increasing the key space and enhancing the level of randomness. Second, it would be beneficial to integrate artificial intelligence and deep learning techniques to automatically assess the quality of encryption and determine the optimal parameters for various image types. Furthermore, the proposed model could be implemented in real hardware environments or on low-power embedded devices used in IoT and smart surveillance applications. Additionally, it is proposed to test the proposed model against various types of analytical attacks, including statistical attacks, chosen plaintext attacks, and differential attacks, to verify its robustness in real-world applications.

It may now be beneficial to propose supporting multi-layer encryption by incorporating more than one chaotic map, such as the Tent or Piecewise Linear map. Additionally, it may be of interest to integrate a machine learning model to analyze the security levels of encrypted images or evaluate the quality of the decrypted images. Finally, this study is a qualitative and quantitative contribution to the field of secure digital image processing. It represents a practical step toward developing image encryption algorithms.

References

- [1] D. Altunkaya, F. Y. Okay, and S. Özdemir, "Encoding IoT Data: A Comprehensive Review of Image Transformation Techniques," *Sakarya University Journal of Computer and Information Sciences*, vol. 8, no. 2, pp. 358–381, 2025. doi: 10.35377/saucis.1639203.
- [2] M. Rafiei, J. Raitoharju, and A. Iosifidis, "Computer Vision on X-Ray Data in Industrial Production and Security Applications: A Comprehensive Survey," *IEEE Access*, vol. 11, Institute of Electrical and Electronics Engineers Inc., pp. 2445–2477, Jan. 02, 2023. doi: 10.1109/ACCESS.2023.3234187.
- [3] A. Khalil, A. Humeau-Heurtier, P. Abraham, and G. Mahé, "Microvascular blood flow with laser speckle contrast imaging: Analysis of static scatterers effect through modelling and simulation," *Proceedings - UKSim-AMSS 8th European Modelling Symposium on Computer Modelling and Simulation, EMS 2014*, no. October, pp. 82–86, 2014, doi: 10.1109/EMS.2014.53.
- [4] X. Liao, Y. Yu, B. Li, Z. Li, and Z. Qin, "A New Payload Partition Strategy in Color Image Steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 3, pp. 685–696, 2020, doi: 10.1109/TCSVT.2019.2896270.
- [5] X. Liao, Z. Qin, and L. Ding, "Data embedding in digital images using critical functions," *Signal Processing: Image*

- Communication*, vol. 58, pp. 146–156, 2017, doi: 10.1016/j.image.2017.07.006.
- [6] Ü. ÇAVUŞOĞLU and H. AL-SANABANİ, “The Performance Comparison of Lightweight Encryption Algorithms,” *Sakarya University Journal of Computer and Information Sciences*, vol. 2, no. 3, pp. 158–169, 2019, doi: 10.35377/saucis.02.03.648493.
- [7] Y. Alghamdi and A. Munir, “Image Encryption Algorithms: A Survey of Design and Evaluation Metrics,” *Journal of Cybersecurity and Privacy*, vol. 4, no. 1. Multidisciplinary Digital Publishing Institute, pp. 126–152, Feb. 23, 2024. doi: 10.3390/jcp4010007.
- [8] C. Li, S. Li, G. Alvarez, G. Chen, and K. T. Lo, “Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 369, no. 1–2, pp. 23–30, 2007, doi: 10.1016/j.physleta.2007.04.023.
- [9] C. Li, Y. Liu, L. Y. Zhang, and M. Z. Q. Chen, “Breaking a chaotic image encryption algorithm based on modulo addition and xor operation,” *International Journal of Bifurcation and Chaos*, vol. 23, no. 4, p. 48, 2013, doi: 10.1142/S0218127413500752.
- [10] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, “Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain,” *IEEE Access*, vol. 9, pp. 59108–59130, 2021, doi: 10.1109/ACCESS.2021.3071535.
- [11] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. P. Samal, “A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication,” *Scientific Reports 2025 15:1*, vol. 15, no. 1, pp. 1–16, Apr. 2025, doi: 10.1038/s41598-025-95995-8.
- [12] W. Zhou, Y. Lu, R. Wang, Q. Wang, and J. Zheng, “A Novel Image Encryption Based on Style Transfer,” in *ISKE 2023 - 18th International Conference on Intelligent Systems and Knowledge Engineering*, 2023, pp. 119–127. doi: 10.1109/ISKE60036.2023.10481503.
- [13] M. Kumar, A. Aggarwal, and A. Garg, “A Review on Various Digital Image Encryption Techniques and Security Criteria,” *International Journal of Computer Applications*, vol. 96, no. 13, pp. 975–8887, 2014.
- [14] U. Zia *et al.*, “Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains,” *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.
- [15] O. F. Mohammad, M. Shafry, M. Rahim, S. Rafeeq, M. Zeebaree, and F. Y. H. Ahmed, “A Survey and Analysis of the Image Encryption Methods,” 2017. Accessed: Jul. 20, 2025. [Online]. Available: https://www.academia.edu/download/57642736/Dec2017ijaerv12n23_35.pdf
- [16] S. Tunçer and C. Karakuzu, “Performance Analysis of Chaotic Neural Network and Chaotic Cat Map Based Image Encryption,” *Sakarya University Journal of Computer and Information Sciences*, vol. 5, no. 1, pp. 37–47, Apr. 2022, doi: 10.35377/saucis...1002582.
- [17] J. Wang, X. Song, H. Wang, and A. A. Abd El-Latif, “Applicable image security based on new hyperchaotic system,” *Symmetry*, vol. 13, no. 12, 2021, doi: 10.3390/sym13122290.
- [18] S. Patel and T. Veeramalai, “Image Encryption Using a Spectrally Efficient Halton Logistics Tent (HaLT) Map and DNA Encoding for Secured Image Communication,” *Entropy*, vol. 24, no. 6, 2022, doi: 10.3390/e24060803.
- [19] M. Hanif *et al.*, “A Novel Grayscale Image Encryption Scheme Based on the Block-Level Swapping of Pixels and the Chaotic System,” *Sensors*, vol. 22, no. 16, 2022, doi: 10.3390/s22166243.
- [20] Z. Yuan, H. Li, Y. Miao, W. Hu, and X. Zhu, “Digital-Analog Hybrid Scheme and Its Application to Chaotic Random Number Generators,” *International Journal of Bifurcation and Chaos*, vol. 27, no. 14, Dec. 2017, doi: 10.1142/S0218127417502108.
- [21] Y. Poursad, R. Ranjbarzadeh, and A. Mardani, “A New Algorithm for Digital Image Encryption Based on Chaos Theory,” *Entropy 2021*, vol. 23, Page 341, vol. 23, no. 3, p. 341, Mar. 2021, doi: 10.3390/E23030341.
- [22] A. G. Mohamed *et al.*, “Chaos Fractal Digital Image Encryption Transmission in Underwater Optical Wireless Communication System,” *IEEE Access*, vol. 12, pp. 117541–117559, 2024, doi: 10.1109/ACCESS.2024.3446836.
- [23] O. M. Al Hazaimh, M. F. Al Jamal, A. K. Alomari, M. J. Bawaneh, and N. Tahat, “Image encryption using anti-synchronisation and Bogdanov transformation map,” *International Journal of Computing Science and Mathematics*, vol. 15, no. 1, p. 43, 2022, doi: 10.1504/IJCSM.2022.122144.
- [24] H. Jiexian, Y. Khizar, Z. A. Ali, R. Hasan, and M. S. Pathan, “On the dynamic reconfigurable implementations of MISTY1 and KASUMI block ciphers,” *PLoS ONE*, vol. 18, no. 9, September, p. e0291429, Sep. 2023, doi: 10.1371/journal.pone.0291429.

- [25] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dynamics*, vol. 73, no. 3, pp. 2083–2089, Aug. 2013, doi: 10.1007/s11071-013-0924-6.
- [26] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 22–30, Feb. 2018, doi: 10.1049/iet-spr.2016.0584.
- [27] K. Yildiz, A. Buldu, and H. Saritas, "Elliptic curve coding technique application for digital signature," *Security and Communication Networks*, vol. 9, no. 17, pp. 4242–4254, Nov. 2016, doi: 10.1002/sec.1601.
- [28] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
- [29] B. Schneier, *APPLIED CRYPTOGRAPHY: Protocols, Algorithms, and Source Code in C, 20th Anniversary Edition*. Wiley, 2015. doi: 10.1002/9781119183471.
- [30] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

Article Information Form

Authors Contributions

Adil Ibrahim Khalil: Conceptualization and methodology design; performed data preprocessing, experimental execution, model development, result analysis, and final manuscript preparation.

Adel A. Abed Al Wahaab Al Imam: Dataset preparation, performance evaluation, literature review, and manuscript refinement.

Conflict of Interest Notice

The authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical Approval

It is declared that during the preparation process of this study, scientific and ethical principles were adhered to, and all studies cited are listed in the bibliography.

Artificial Intelligence Statement

No artificial intelligence tools were used while writing this article.

Plagiarism Statement

This article has been scanned by iThenticate™.