






ISSN: 2617-6548

URL: [www.ijirss.com](http://www.ijirss.com)

## Real-time FPGA-based grayscale image hiding with key masking for secure LSB steganography

 Zaid A. Abdulrazzaq<sup>1</sup>,  Fadwa Al Azzo<sup>2</sup>,  Harith G. Ayoub<sup>3\*</sup>

<sup>1,2,3</sup>Norther Technical University (NTU), Iraq.

Corresponding author: Harith G. Ayoub (Email: [harithga@ntu.edu.iq](mailto:harithga@ntu.edu.iq))

### Abstract

The paper presents a novel ZYNQ-FPGA-based real-time grayscale secret image hiding method using a cover RGB image to enhance the security performance of the LSB steganography approach. This work begins with designing a pseudo-random number generator with a 12-bit size using linear feedback shift registers (LFSRs). The two least significant bits (LSBs) are used as indicators for four-position hiding. The key is assumed to be the initial value of the LFSR, exchanged previously between transmitter and receiver over any network. The two position bits extracted through the proposed key masking are resistant to side-channel attacks. All designs are implemented using XSG/SIMULINK environment to verify and validate the results with Xilinx VIVADO tools. The synthesis operation achieved a high frequency of 2.22 GHz and a throughput of 17.7 Gb/s. Statistical analyses include histogram, PSNR, MSE, BER, SSIM, CCR, execution time, frequency, and throughput. Clear structural similarity and processing time contribute to an efficient balance between security and speed performance.

**Keywords:** FPGA, Information Hiding, Key masking, LFSR, PRNG, XSG.

**DOI:** 10.53894/ijirss.v8i6.9813

**Funding:** This study received no specific financial support.

**History:** Received: 7 July 2025 / Revised: 11 August 2025 / Accepted: 13 August 2025 / Published: 12 September 2025

**Copyright:** © 2025 by the authors. 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/>).

**Competing Interests:** The authors declare that they have no competing interests.

**Authors' Contributions:** Research design, implementation, data analysis, manuscript writing, Zaid A. Abdulrazzaq (ZAA); research design, implementation, data analysis, manuscript writing, Fadwa Al Azzo (FAA); research design, implementation, data analysis, manuscript writing, Harith G. Ayoub (HGA). All authors have read and agreed to the published version of the manuscript.

**Transparency:** The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

**Publisher:** Innovative Research Publishing

## 1. Introduction

The prevalence of digital images in various fields has led to a growing need for secure transmission and storage of confidential information. Images transmitted through shared or public networks are particularly vulnerable to attacks, posing a significant challenge in terms of protection [1-11]. Cryptography is used for protection, which is the process of converting known images into undefined images to be non-knowledgeable or unpredictable by attackers [12-17].

Steganography, on the other hand, is the technique of hiding secret data within an ordinary, non-secret file or message in order to avoid detection [18-21]. Recent research in cryptography has focused on the use of pseudo-random number

generators (PRNGs) based on chaotic systems due to their high randomness factor and sensitivity to initial conditions [22-25].

This has led to the development of various steganographic techniques that make use of Pseudo-Random Number Generators (PRNGs) to embed the secret data into cover objects [26-30]. Hardware implementation, specifically field programmable gate array (FPGA) [31-40]. The choice of FPGA is based on several factors: the efficiency of this technology for handling multimedia files such as audio and video, managing real-time meets to reduce latency, low power dissipation for prototyping, no need for hardware redesign, and the ability to integrate with hardware equipment (cameras, sensors).

A digital image is a two-dimensional array containing  $M \times N$  pixels, in which  $M$  is the number of rows or the height of the image, and  $N$  is the number of columns or the width of the image [41-46]. Each pixel in this digital array can only take specific numerical values, and the set of these values depends on the type of image [47-56].

Different pixels in the image carry information that can have various meanings depending on the application it is used for, Smarandache et al. [57], Wang et al. [58], Darwis et al. [59], Reinke et al. [60], Fu et al. [61] and Bemana et al. [62]. It may be a binary image that carries only two specific values, usually zero and one, i.e., a single bit per pixel, or grayscale images carrying 8 bits per pixel for different gray levels, or it may be a color image that carries information about the intensity values of the red, green, and blue components [63-70].

### *1.1. The Main Contribution of this Work Involves*

1. Implementing pseudo random number generator in FPGA with 12 bit linear feedback shift registers (LFSR),
2. Choosing confidential information for cover and secrecy, the choice for this work was digital images.
3. Building the architecture of the LSB algorithm in FPGA with XSG/SIMULINK because of its flexibility for testing and verifying the results of hiding/recovering.
4. Employing the PRNG of step 1 into step 2 and proposing an algorithm named LSB-PRNG for hiding/recovering a secret image.
5. The index of the hiding bit will be chosen according to the 12 bits generated by the LFSR for the first 4 bits (00-11) with a proposed key masking algorithm.
6. Implementing the proposed method (LSB-PRNG) in the hardware module using the ZYNQ-7020 evolution board through the VIVADO software tool with high speed and low silicon area, and then evaluating the execution time in the FPGA.
7. Checking security performance measurements: peak signal-to-noise ratio (PSNR), mean square error (MSE), bit error rate (BER), structural similarity (SSIM), cross-correlation (CCR), overall execution time, frequency for the proposed method.

### *1.2. Literature Survey*

Several studies have been conducted in the field of image steganography due to its significance in data communication. Topic [70] proposed an image steganography method using a deep neural network with a long training time. In comparison, this research does not involve real-time meetings or dealing with randomness in security manners [71] presents a view of several steganography approaches; all approaches have a long processing time, which indicates robustness for real-time steganography applications also [72] presented efficient steganographic approach includes text hiding with cover with a good PSNR but without dealing with the time execution point or randomize LSB positions [73] presented bit pattern steganography approach mixing two techniques: steganography and cryptography for increased robustness, but with two issues: firstly, meeting timing requirements of hardware; secondly, not declaring image MSE or PSNR [74] presented a review of several research approaches to steganography with various techniques such as DNA, network, audio, video, text, and image steganography. [75] introduced a new steganographic method utilizing human visual properties, along with a novel LSB algorithm. The hiding performance metrics, including MSE, PSNR, and SSIM, were satisfactory; however, the researchers did not address the hiding time metric necessary for real-time applications [26] provided different steganography methods, but overall did not address processing time in hardware, as this research had [76]. It offers several methods for steganography with good security performance measurements, focusing on metrics such as MSE, BER, and PSNR, without considering processing time, throughput, or randomness [3, 77, 78] presented a review of multiple image-hiding approaches with spatial domain or transform domain, with no consideration of an important factor, which is processing time [79]. The file hiding method includes a chaotic method but does not mention BER, MSE, processing time, or any performance metrics [3, 26, 71-80].

## **2. Methods**

### *2.1. Steganography*

The predominant technique for fortifying the security of communication and safeguarding the confidential transmission of data is known as steganography [81-85].

This method ensures the secure conveyance of information through communication systems and also facilitates the watermarking process, thereby securing the authenticity of multimedia files such as films and logos. The most prevalent techniques of steganography encompass the Least Significant Bit (LSB), Pixel Value Differencing (PVD), Spread Spectrum, and statistical methodologies [86-89].

**Table 1.**

Comparison between stenographic methods.

Technique	Robustness	Imperceptibility	Payload capacity	Complexity
LSB	Low	High	High	Low
PVD	High	Medium	Low	Low
Spread spectrum	Medium	Low	Low	Medium
Statistical	Medium	High	Low	Medium

Table 1, demonstrates that the LSB method stands out as the optimal approach for accelerating multiple reasons. Firstly, it offers the best peak signal-to-noise ratio and structural similarity index. Secondly, it boasts simplicity for hardware implementation. Thirdly, it executes with remarkable speed. Lastly, it possesses the ability to process large amounts of data for concealment.

## 2.2. Steganography with LSB

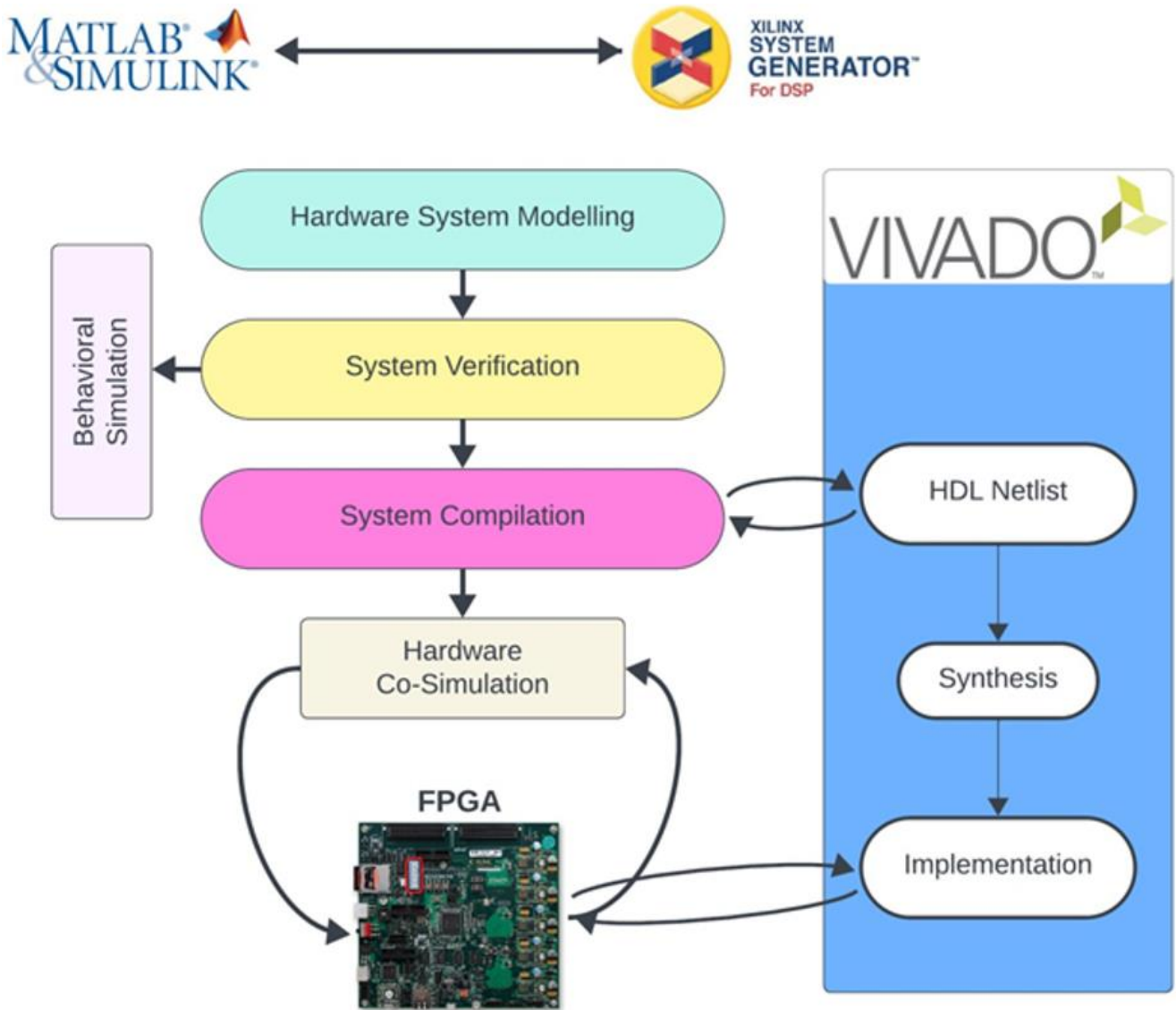
Figure 1 illustrates the concept of LSB hiding, which involves concealing secret image bits within the LSB of cover image pixels. It is important to note that the LSB bit difference of 1 or 0 should not impact the resolution of the cover image.

Two methodologies in the least significant bit (LSB) algorithm:

1. The utilization of LSB steganography in FPGA-based implementation enables the concealment of data within the least significant bits of an image or signal, ensuring a heightened level of security and imperceptibility. Sender's embedding system: eliminate the LSBs of the cover image and replace them with the secret data bits, resulting in the creation of a stego image.
2. The enhanced LSB steganography with random bit positioning provides heightened security, guaranteeing the covert message remains imperceptible. The recipient's extraction algorithm entails fetching the LSB of the stego image pixels to retrieve the concealed data.

## 2.3. ZYNQ FPGA Design with Embedded SIMULINK/XSG

The collaboration between Xilinx Vivado Design Suite and Xilinx System Generator for DSP and HDL is seamless. The latest nodes are supported by the Xilinx Vivado Design Suite, specifically designed for intricate designs [90-93]. It seamlessly integrates hardware and software support and offers system- and device-level design. It comes equipped with toolkits for managing FPGA configuration, synthesis, placement, and routing. Additionally, it incorporates specialized tools such as hardware co-simulation, partial reconfiguration, and hardware design languages like SystemVerilog, VHDL, or Verilog. Fig. 1 illustrates the design methodology using Xilinx System Generator (XSG), with the hardware in this paper implemented using the VIVADO/XSG environment VIVADO 2020.2 associated with MATLAB/SIMULINK 2020 a.

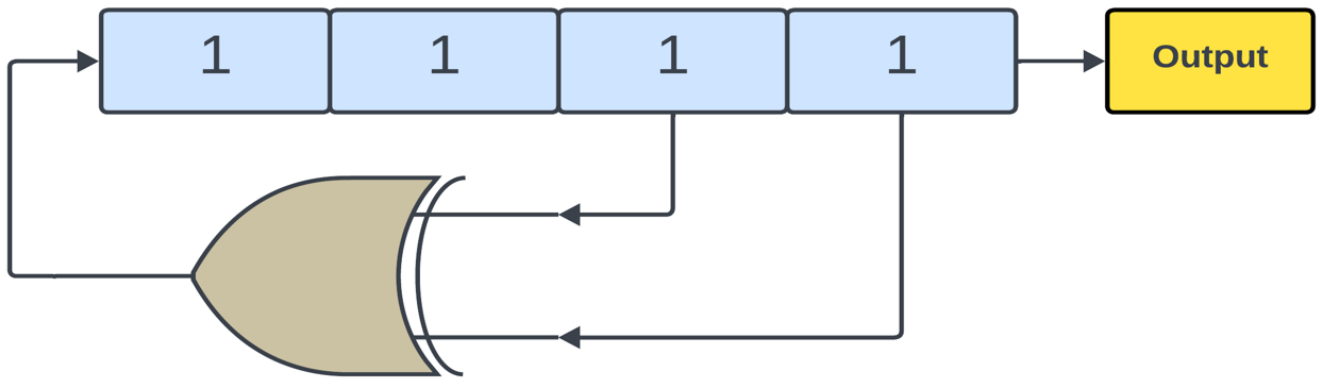


**Figure 1.**  
Hardware flow design using Xilinx System Generator.

#### 2.4. Pseudo-Random Number Generator (PRNG)

A Pseudo-Random Number Generator (PRNG) serves as both a device and an algorithm for producing a series of binary values in a seemingly random fashion. This method finds frequent application in the realms of cryptography and telecommunications. A defining characteristic of PRNG sequences lies in their substantial autocorrelation, rendering them particularly advantageous for encryption and synchronization purposes. PRNGs fabricate a sequence of random numbers over a specific duration through the utilization of mathematical functions contingent upon initial parameters [94-98]. Noteworthy attributes of these PRNG numbers encompass their rapid computational pace, elevated uniformity, and other commendable statistical properties.

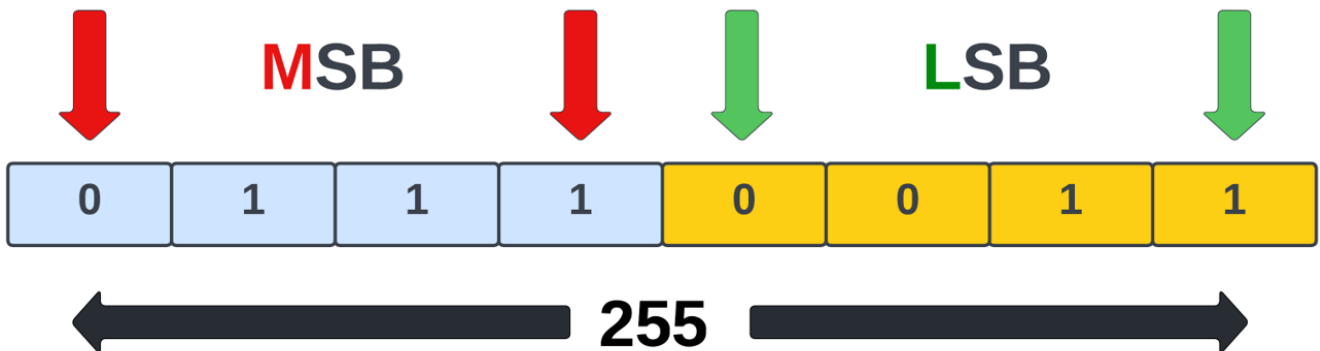
There exist numerous varieties of PRNG, with the Linear Feedback Shift Register (LFSR) standing as one of the most prominent. The LFSR functions as a shift register, employing feedback connections to shift bits from one position to the next [99-102]. This feedback is achieved through the XOR operation on select bits of the register, with the resulting bit then fed back into the register's input. The initial state of the LFSR is represented by a binary vector of a length equivalent to the register. With each clock cycle, the LFSR shifts its contents to the right, and the outgoing shifted bit is termed the LFSR's output. The LFSR continues cycling through its states until it returns to its initial state [103-105]. The number of clock cycles necessary for this return is referred to as the repetition period. Figure 2 illustrates the construction of a 4-bit LFSR.



**Figure 2.**  
Example construction of a 4-bit LFSR.

### 2.5. Proposed Method (LSB-PRNG)

Figure 3 illustrates the 8-bit pixel and the positioning of the least significant bit (LSB) and most significant bit (MSB). This technique involves the selection of the four lower bits of the LSB from the pixels of the cover image, which are then utilized to randomly conceal the bit stream of the secret image. By employing a Pseudo-Random Number Generator (PRNG), the chosen position of the cover bit is substituted with the secret bit within each cover pixel. This innovative method ensures that the integrity and security of the secret image are maintained without compromising the quality of the cover image.



**Figure 3.**  
Binary Bits Representation.

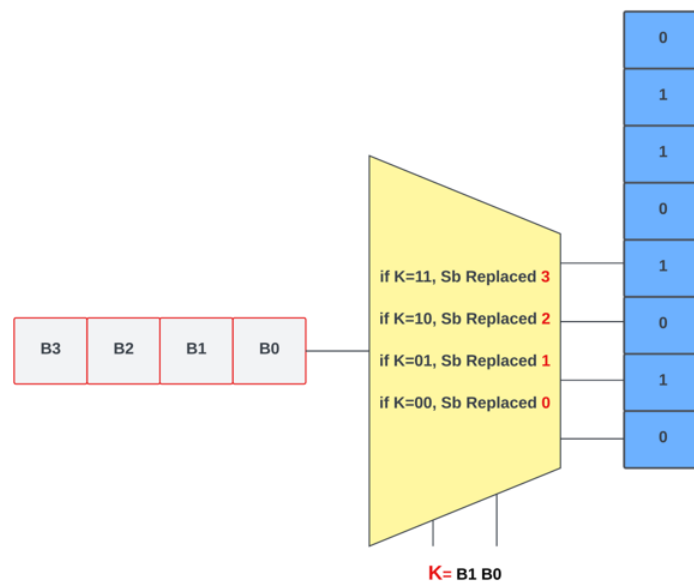
The PRNG plays a crucial role in ensuring the randomness of the concealment process, making it extremely difficult for unauthorized individuals to detect the presence of the secret image. The utilization of the four lower bits of the LSB provides a large number of possibilities for concealing the secret image, thereby increasing the complexity and enhancing the security of the overall system. The substitution of the cover bit with the secret bit ensures that the steganographic process remains robust and resistant to various attacks. Moreover, this method allows for efficient and accurate extraction of the secret image, as the cover bits can be easily reconstructed using the original cover image. In conclusion, the use of a pseudo-random number generator and clever manipulation of the LSB in the cover image allows for effective steganography, ensuring both the concealment and extraction of the secret image with high security and reliability. In terms of steganography, the effectiveness of the Hiding System technique relies heavily on the quality of the PRNG. Employing a PRNG for image steganography can offer an innovative approach to concealing information within an image. A comprehensive summary of the process for utilizing this approach.

1. Choose a PRNG: opt for an LFSR to produce a PRNG. Careful selection of the initial state and feedback taps is essential to ensure the sequence exhibits randomness.
2. Apply key masking to mitigate more steganography systems against fault injection attacks.
3. Encode Confidential Information: Transform the classified data into a binary structure. Every bit of the confidential image will be concealed within the encompassing image.
4. Encode Confidential Information: Utilize the Pseudo-Random Number Generator (PRNG) to select an LSB bit of the cover pixel for each bit of the secret image. Adjust the chosen bit to match the desired hidden bit.

### 2.6. Embedding Strategy

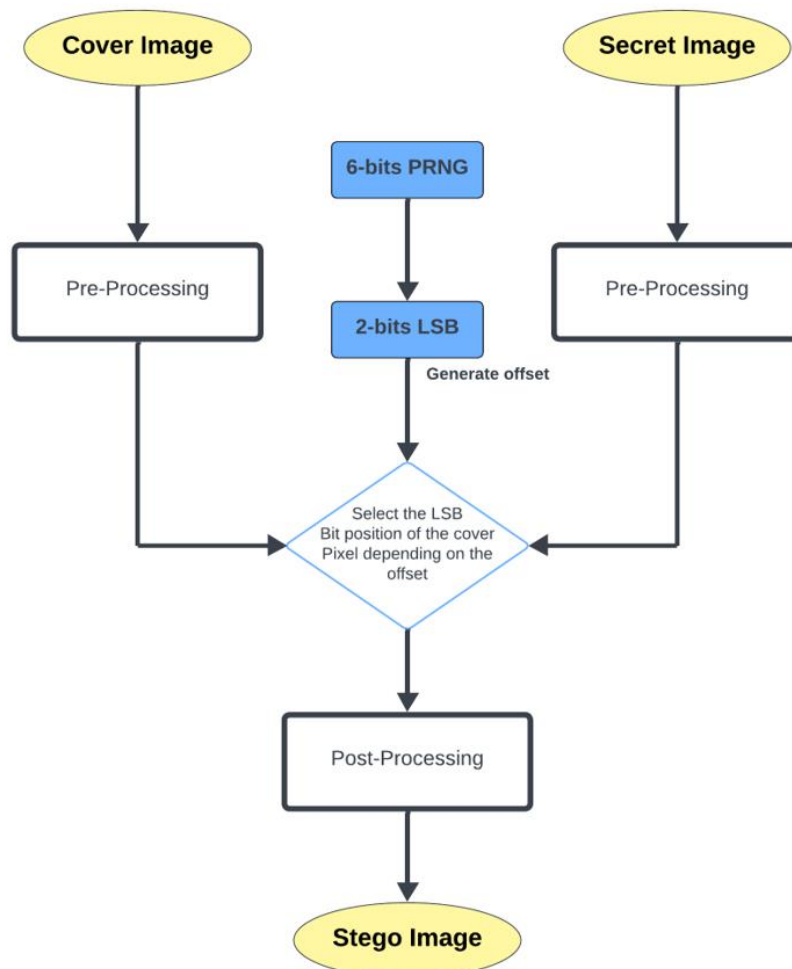
The substitution of the hidden bits with the four least significant bits' location within the cover image pixel is determined by randomly selecting a position for the bit in one pixel to be replaced by the hidden image bit, based on the PRNG-generated  $k$  value at a single clock cycle. Here,  $k$  represents the address value selected with two bits from the output of the LFSR, indicating the position within the cover pixel where the hidden bit is embedded. The strategy of the

embedding algorithm is depicted in Figure 4. Additionally, Figs. 5 and 6 illustrate the flow chart of the hiding and recovering image system utilizing the PRNG. The following map is used for the embedding process.

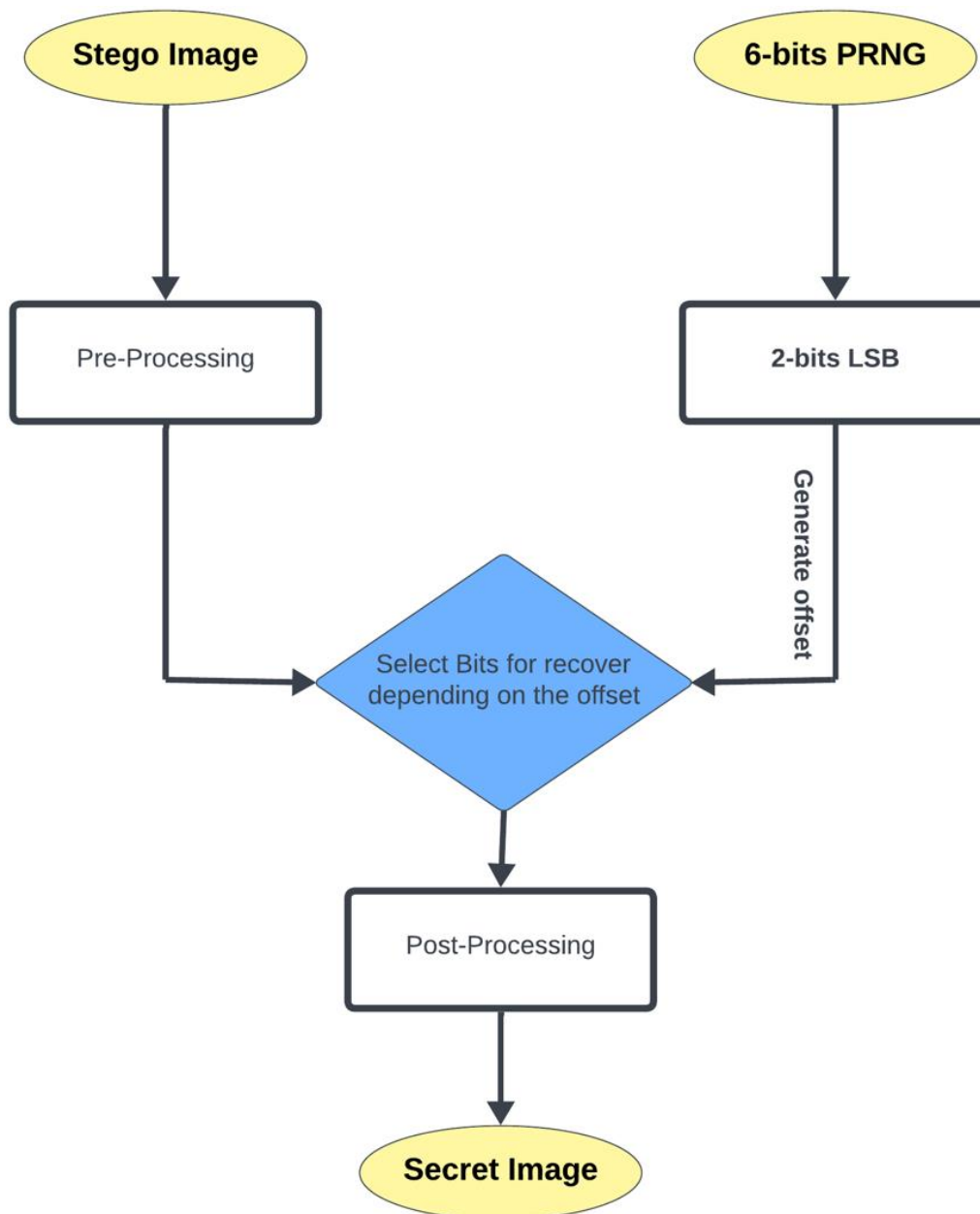


**Figure 4.**  
Embedding strategy of PRNG.

If PRNG generates  $k=0$ , embed in offset 0 of the cover image pixel  
 If PRNG generates  $k=1$ , embed in offset 1 of the cover image pixel  
 If PRNG generates  $k=2$ , embed in offset 2 of the cover image pixel  
 If PRNG generates  $k=3$ , embed in offset 3 of the cover image pixel



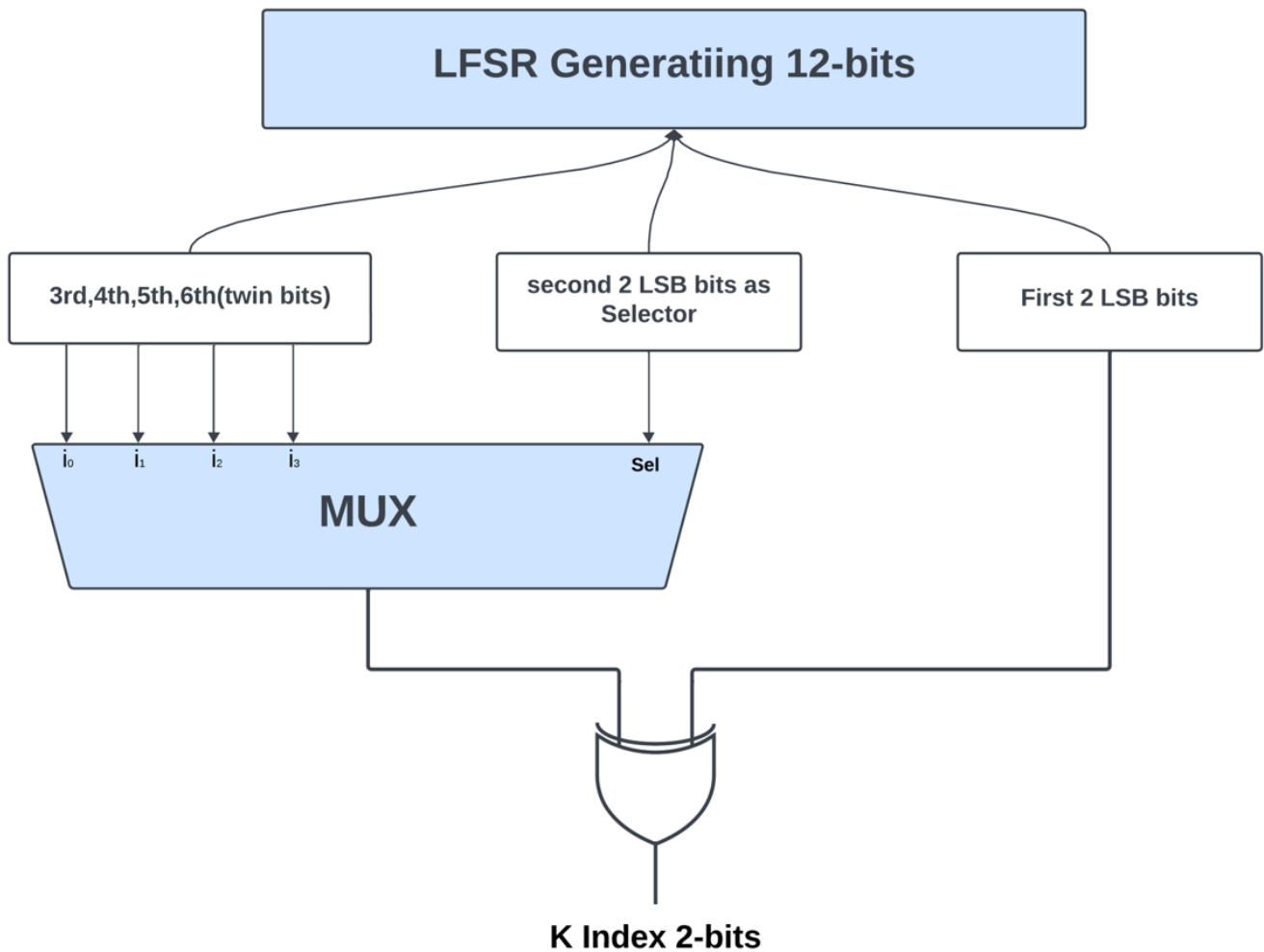
**Figure 5.**  
Flowchart of hiding using PRNG.



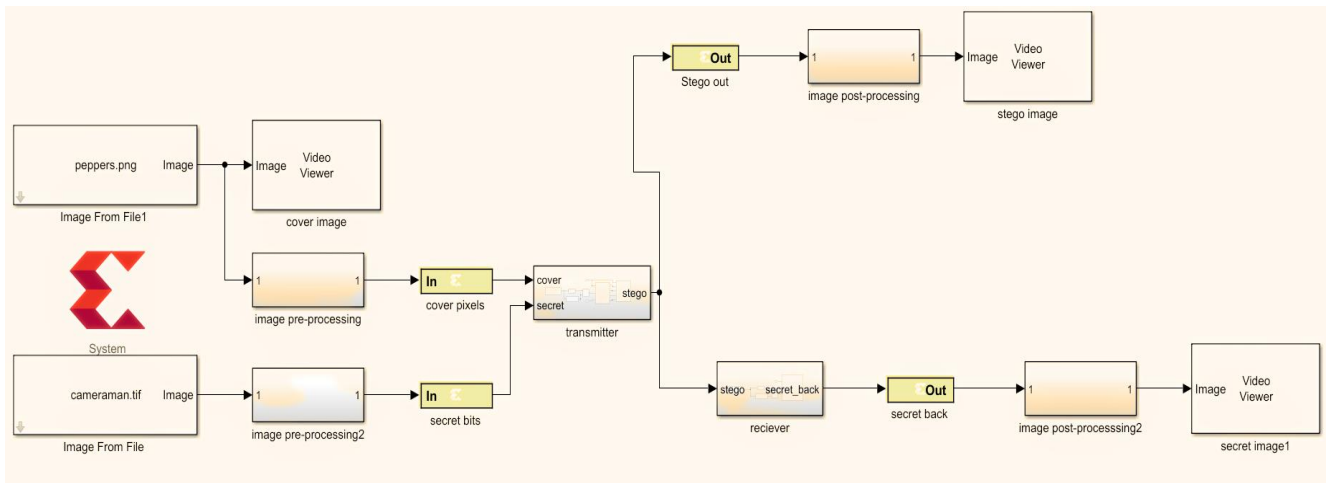
**Figure 6.**  
Flowchart of extracting using PRNG.

### 2.7. Proposed Key-Masking

Figure 7 demonstrates the proposed masking technique with the support of a Linear Feedback Shift Register containing the sequence of 12 bits. The LFSR output is partitioned into different portions for various activities. The first two 'Least Significant Bits' are used as the first pair of keys. The next two LSBs form a selector signal for a multiplexer, which chooses the output depending on the input of the other two LSB bit signals. The MUX inputs are extracted from the 3rd, 4th, 5th, and 6th bits of the LFSR output and are called pair-bits to generate the 2-bit key index. The selected output of the MUX is logically XORed with the first two LSBs in this invention. This design further improves the randomness and security of the key with the help of efficiently used LFSR-generated bits.



**Figure 7.**  
Key Masking.



**Figure 8.**  
System design.

### 3. Results and Discussion

#### 3.1. Hardware design of Hiding System

Figure 8 presents the overall hardware system of the steganography system with the PRNG system that hides an image (secret image) inside the cover image to produce a stego-image by the following steps:

1. Select an image from the file saved on the PC with dimensions that allow covering all secret image bits. The selected image, the cover image, was (peppers.png).
2. Select a secret image with dimensions smaller than the cover image; here, the secret image was (cameraman.tif).
3. Convert the secret image to a stream bit by using the (P-to-S) block of XSG.
4. The transmitter consists of key generation, key masking, selected bit position, and LSB hiding as shown in Figure 9.



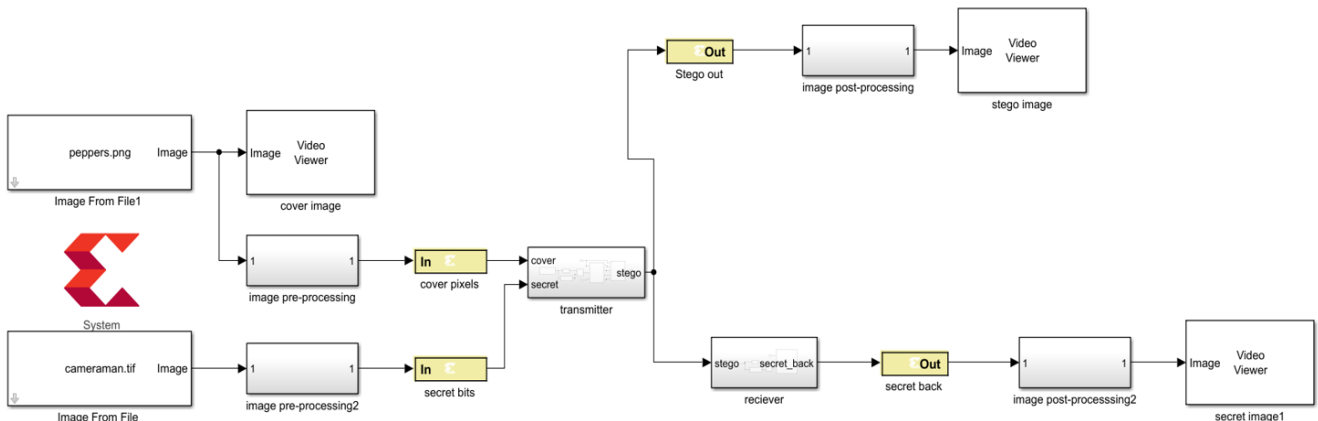
5. Key generation process Design using PRNG by XSG consists of an LFSR with 12- bits.

6. The key masking stage involved XORing the first two least significant bits (LSB) with the bits obtained from entering the second two LSB bits as a selector to a multiplexer with inputs of the remaining two LSB bits of the twelve bits resulting from the key generation process, generating a two-bit masked output key as shown in Figure 10.

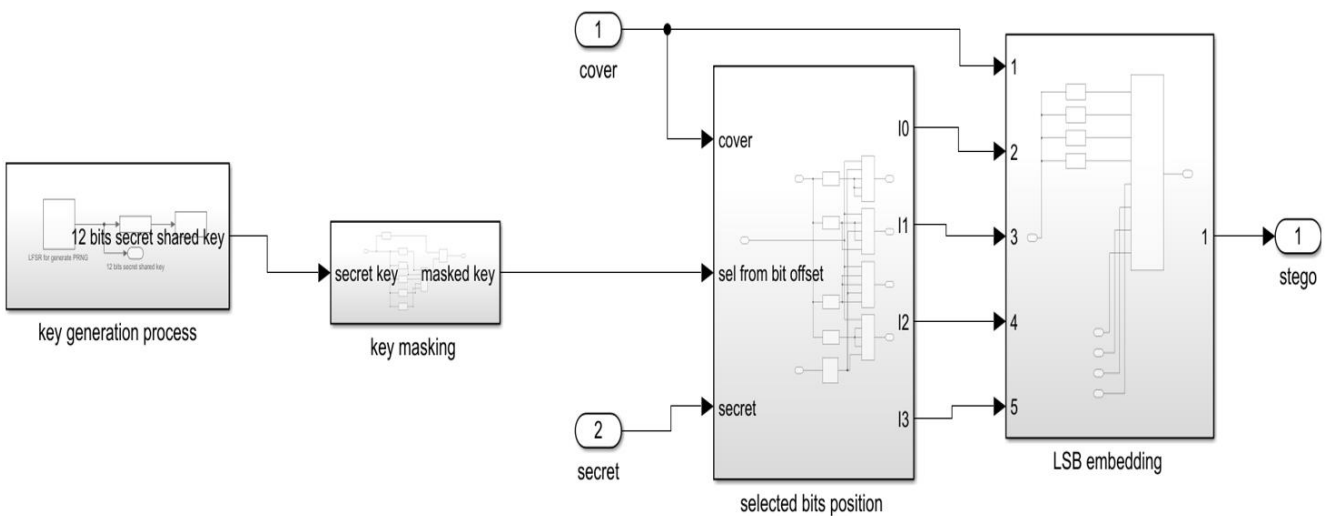
7. Embed each bit from the secret image according to the key mask generated, which selects two bits that refer to the address of the bit. If the key mask was logical 00, then the secret bit was hidden at the first index; else, if the key mask was logical 01, then the secret bit was hidden at the second index; else, if the the key mask was logical 10, then the secret bit was hidden at the third index; else, if the key mask was logical 11, then the secret bit was hidden at the fourth index in Figure 11.

8. The receiver consists of a key generation, key masking, and LSB retrieving system as shown in Figure 12.

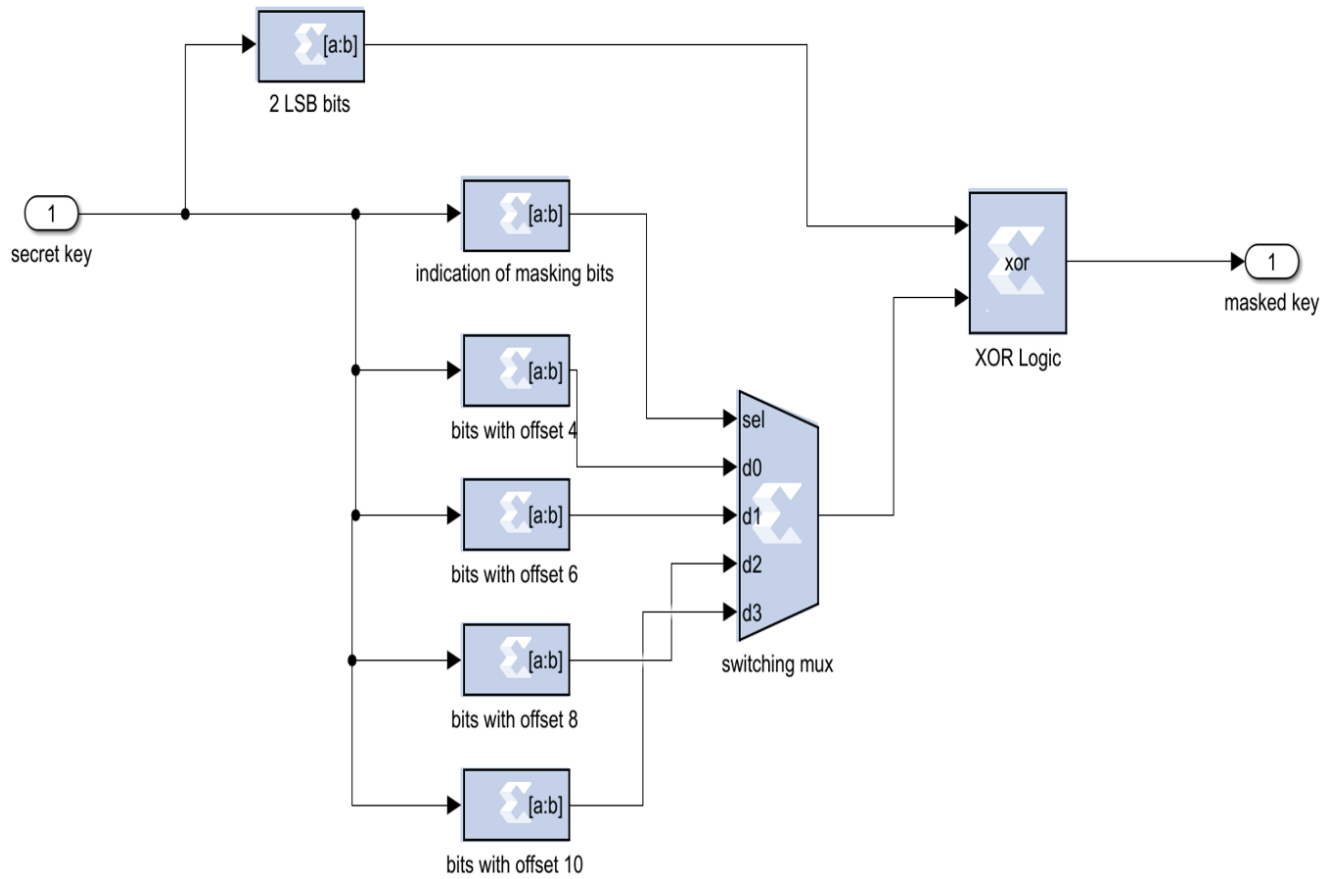
9. The first two stages of the receiver are the same as the transmitter part with a secret key previously exchanged between them, but the difference will be in the last stage of retrieval, as shown in Figure 14, which involves concatenation of the bits' accumulation according to the offset calculated for the masking key generated.



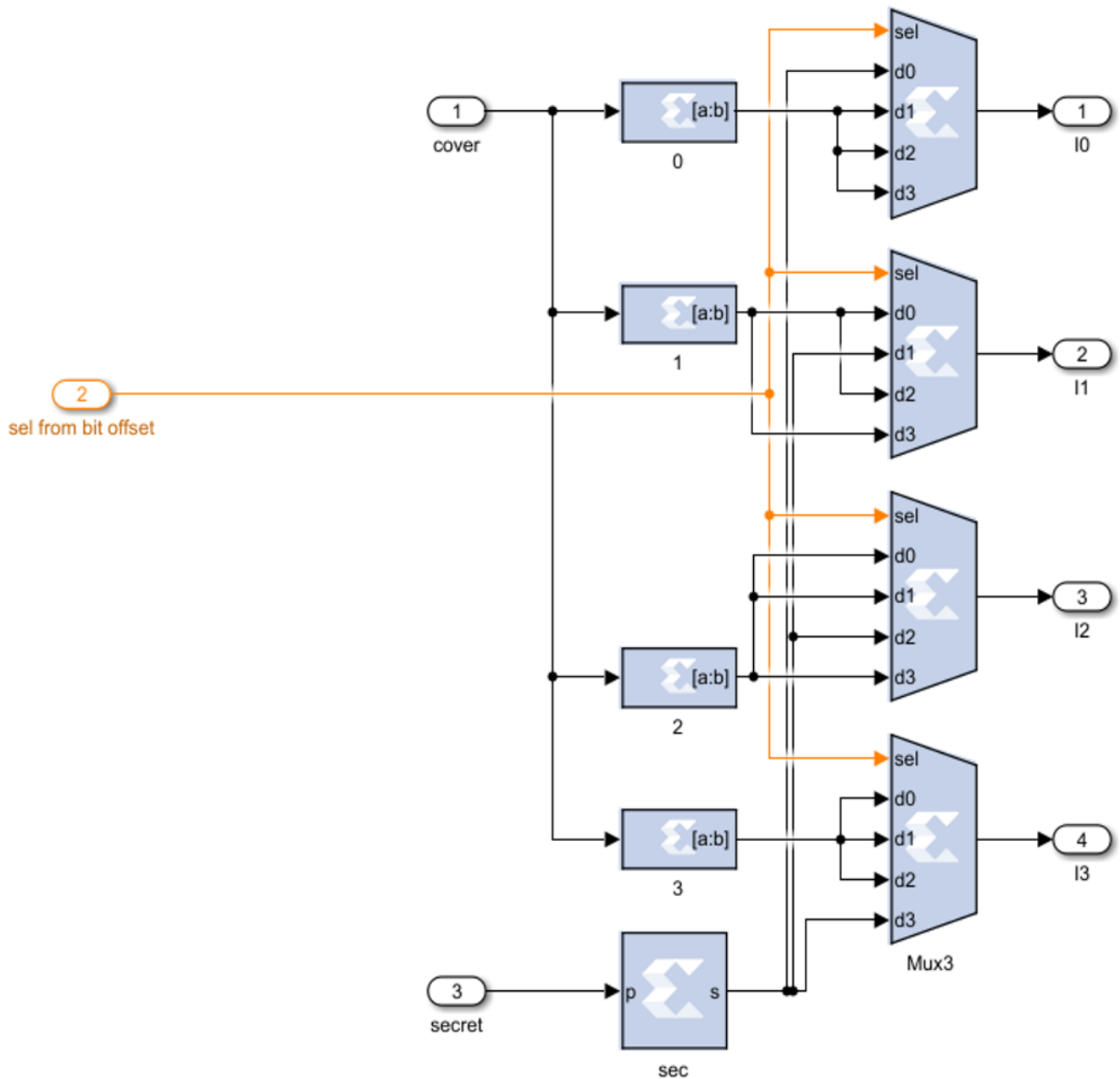
**Figure 9.**  
Hardware design of LSB-PRNG.



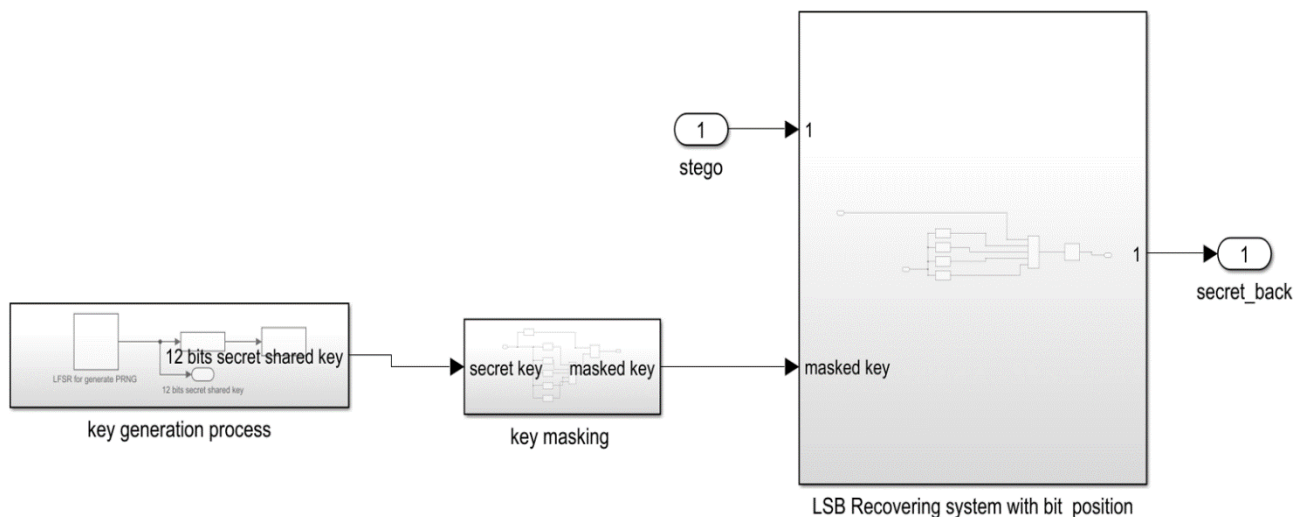
**Figure 10.**  
Hardware design of transmitter part.



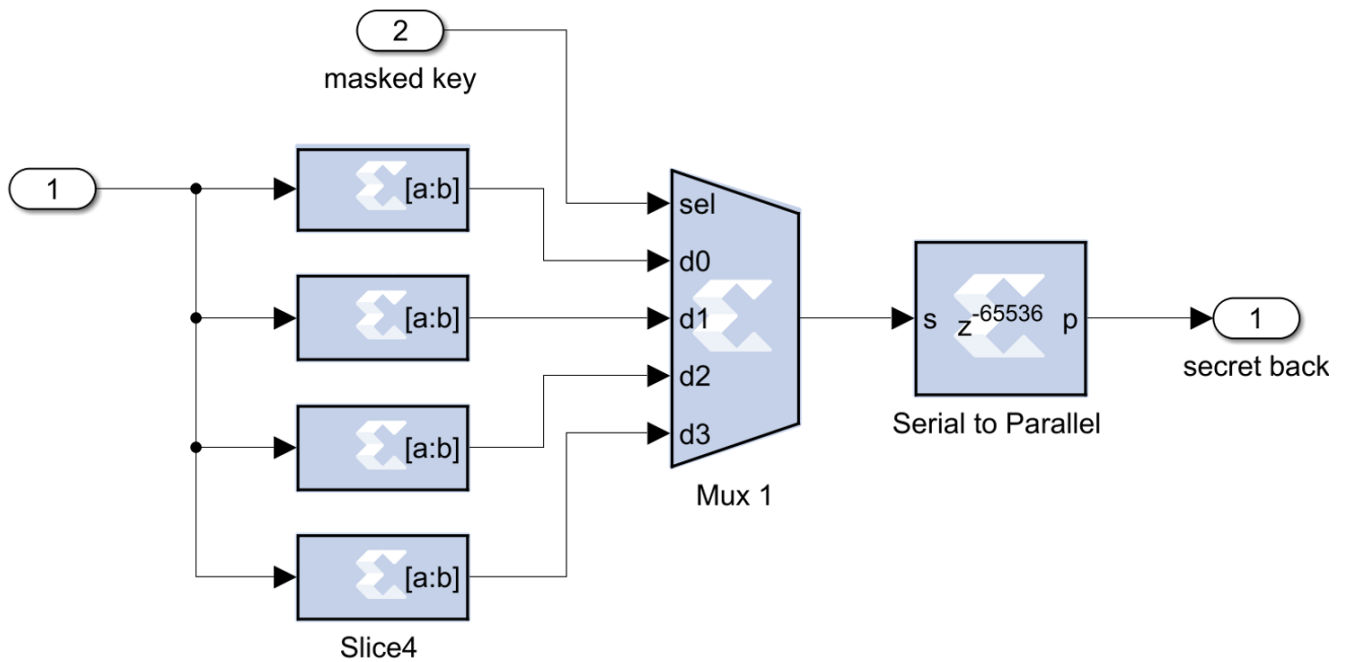
**Figure 11.**  
Hardware design of key masking stage.



**Figure 12.**  
Hardware design of the embedding process.



**Figure 13.**  
Hardware design of receiver part.



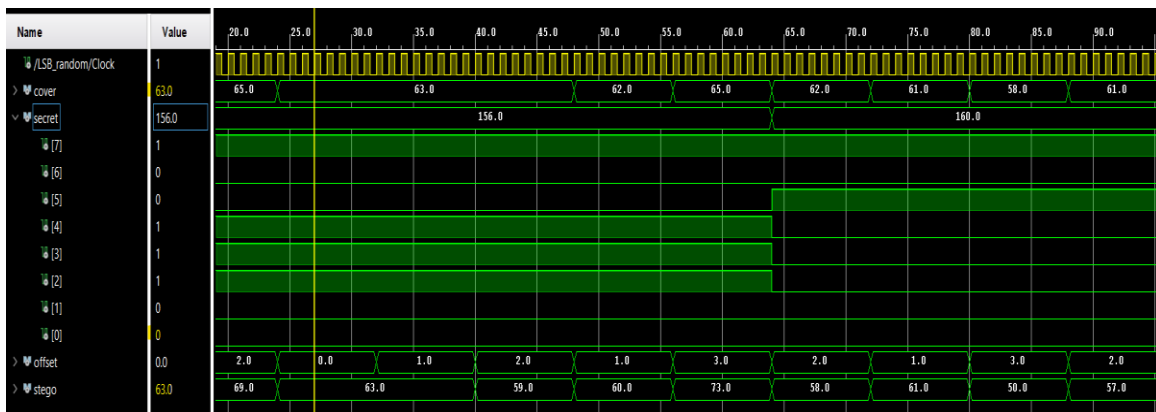
**Figure 14.**  
Hardware design of LSB retrieving algorithm.

The images used in the design represent cover, stego, and secret images shown in Figure 15, the chosen cover image was peppers.png and the secret was cameraman.tif provided by MATLAB/SIMULINK environment.

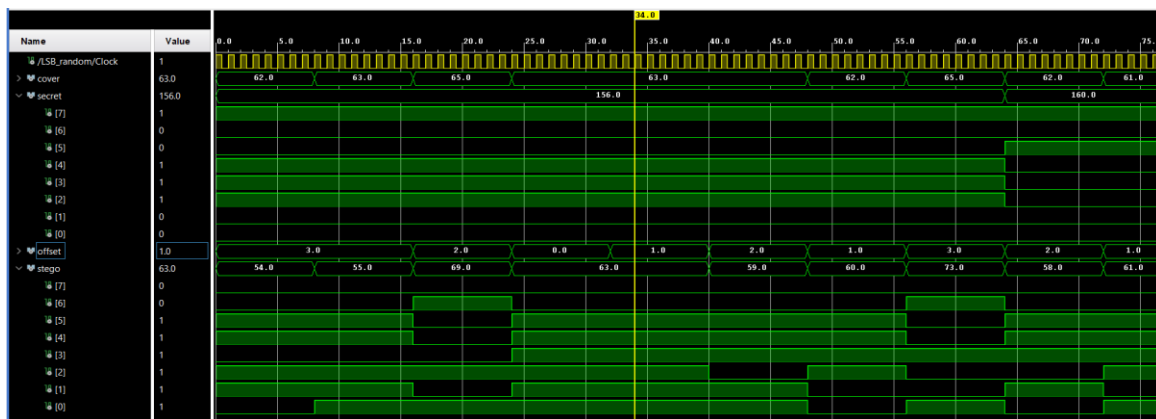


**Figure 15.**  
Secret, cover, and stego images.

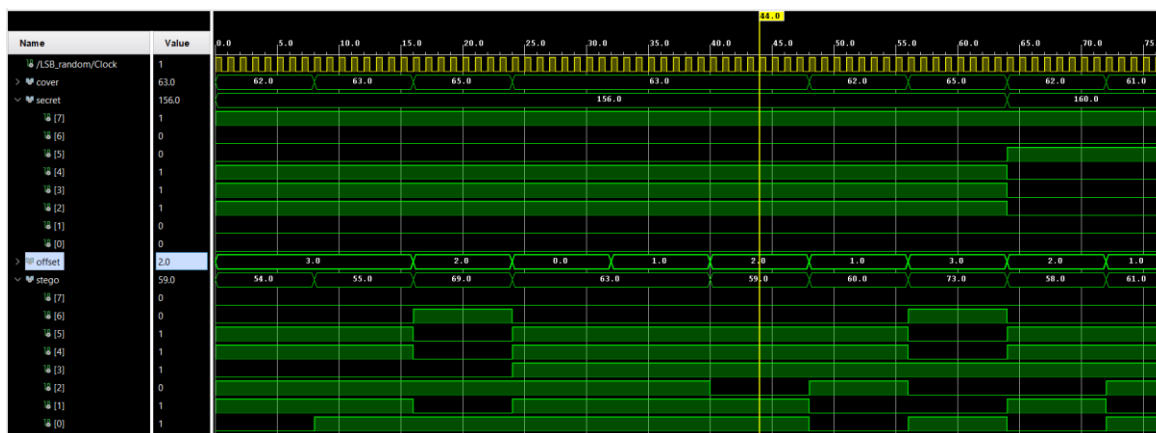
To determine how the pixel of the cover image changed after replacing the LSB, rather than whether the bit from the secret image was equal to the LSB of the cover image pixel, it was observed that, in this case, the cover image pixel did not change. Figure 16 shows the changing of pixels when PRNG was generated with 0, then the LSB with offset = 0 was changed to zero according to the bit from the secret image, which was replaced by the bit from the cover image, when the PRNG = 1 in Figure 17 changed to zero according to the bit from secret image = 0, Figure 18 changed to one according to secret bit and Figure 19 the offset = 3 changed to zero according to the secret bit.



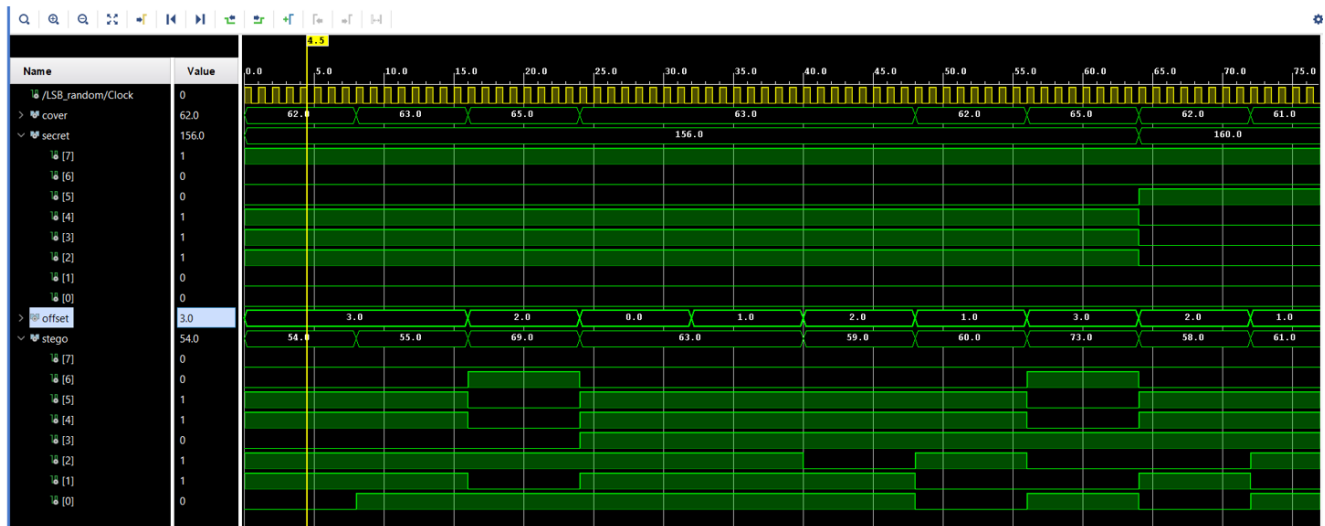
**Figure 16.**  
LSB-PRNG Generating Offset= 0



**Figure 17.**  
LSB-PRNG Generating Offset= 1



**Figure 18.**  
LSB-PRNG Generating Offset= 2



**Figure 19.**  
LSB-PRNG Generating Offset 3.

### 3.2. Hardware Synthesis and Implementation

This section presents HDL compilation using JTAG co-simulation results with the ZYNQ-702 FPGA evaluation board. This board operates at a frequency of 667 MHz. The synthesis process indicated that the optimal time period to meet timing path requirements is 3 ns, resulting in a worst negative slack (WNS) of 2.55 ns. The maximum frequency is calculated based on the following equation.

$$f_{max} = 1/(T - WNS) \quad (1)$$

When  $T = 3\text{ ns}$ ,  $WNS = 2.55\text{ ns}$  then  $F_{max} = 2.22\text{ GHz}$

The throughput (the number of processing bits per second) of the hiding system, which is an important metric, is computed by the following equation.

$$\text{Throughput} = (N \times f_{max})/\text{latency} \quad (2)$$

The maximum frequency was 2.22 GHz with a high throughput near 17.76 Gb/s.

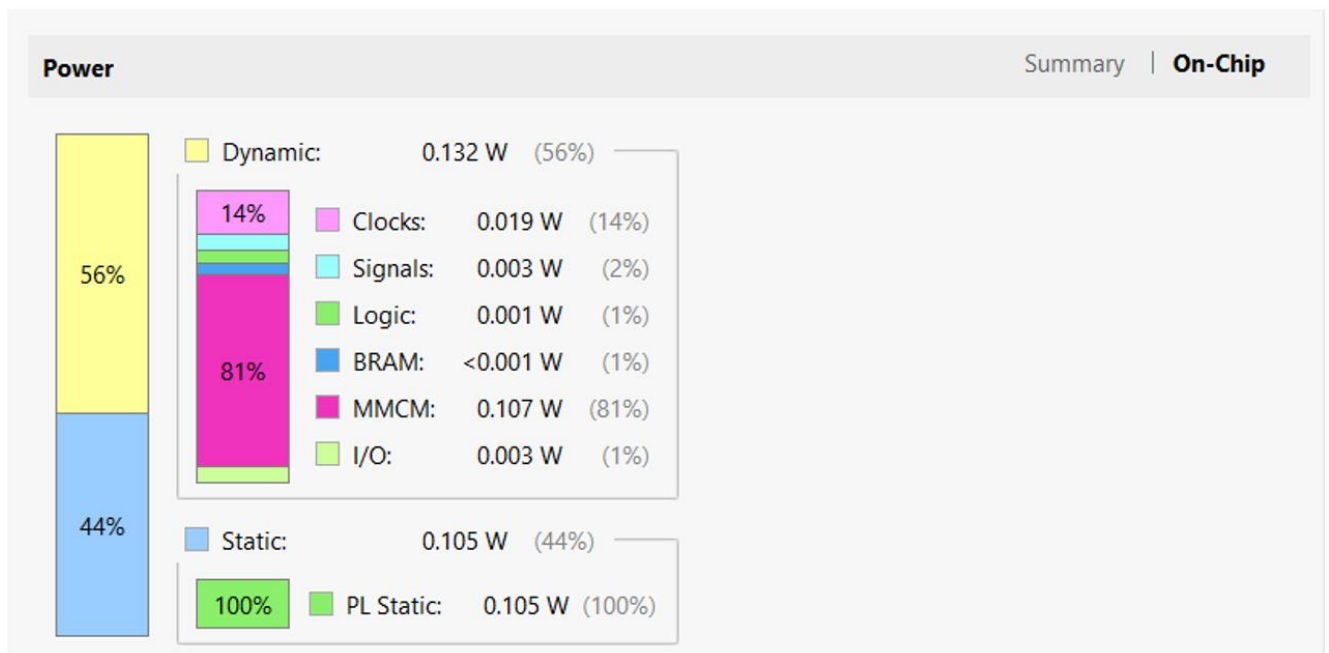
Table 2 presents FPGA utilization, silicon area consists of:

- 1- LUT: Look-Up Tables
- 2- LUTRAM: Look-Up Table RAMS
- 3- FF: Flip-Flops
- 4- BRAM: Block RAMs
- 5- DSP: Digital Signal Processing blocks
- 6- IO: Input/output buffers
- 7- BUFG: Global Buffers
- 8- MMCM: Mixed-Mode Clock Manager

**Table 2.**  
Logic area utilization.

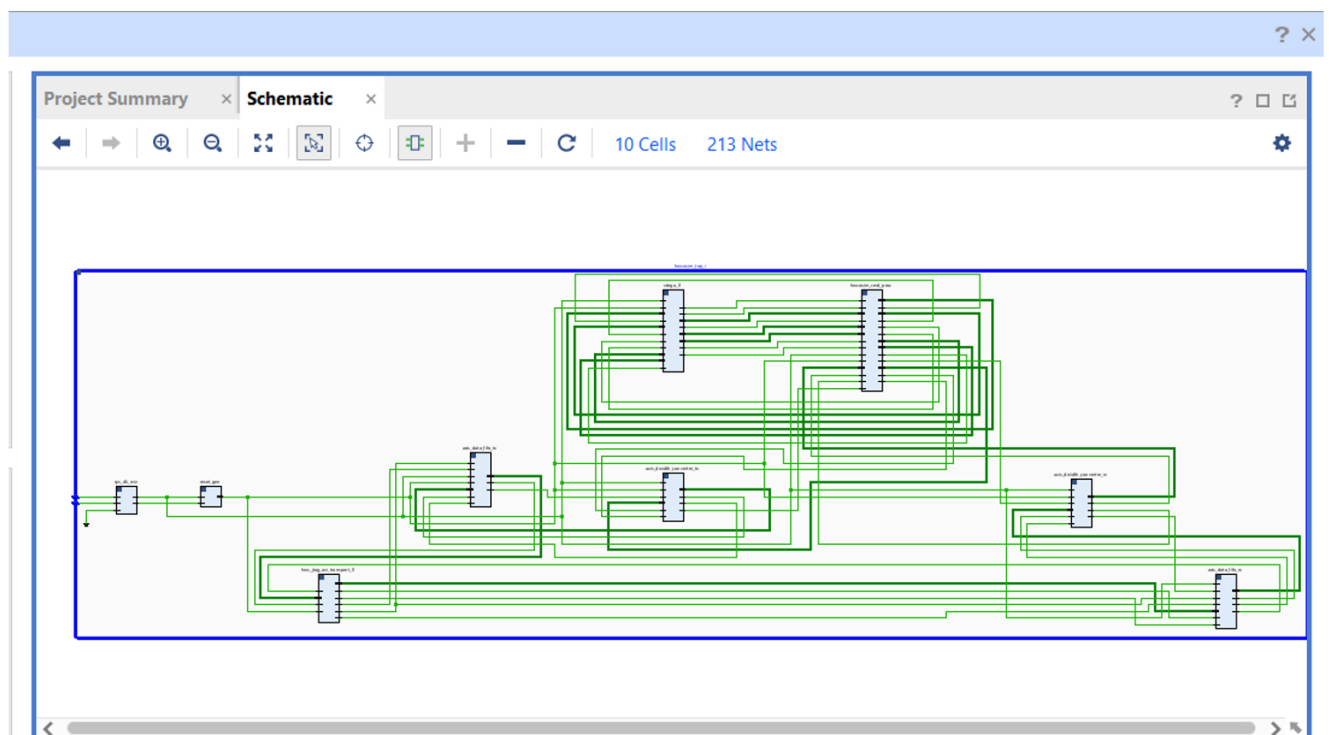
Resource	Utilization	Available	Utilization (%)
LUT	24675	53200	46.3
LUTRAM	7944	17400	45.6
FF	2520	106400	2.36
BRAM	3	140	2.1
IO	6	200	3
BUFG	5	32	15.6
MMCM	1	4	25

Power report, one of the synthesis tools provided by VIVADO software, indicates that dynamic power consumption the active power during switching (charging and discharging of capacitances in the design) was 0.132 W. Static power, which is the power consumed when the design is not active and depends on parameters such as temperature and supply voltage, was 0.105 W. Therefore, the total power consumption was 0.237 W, the overall power report shown in Figure 20.



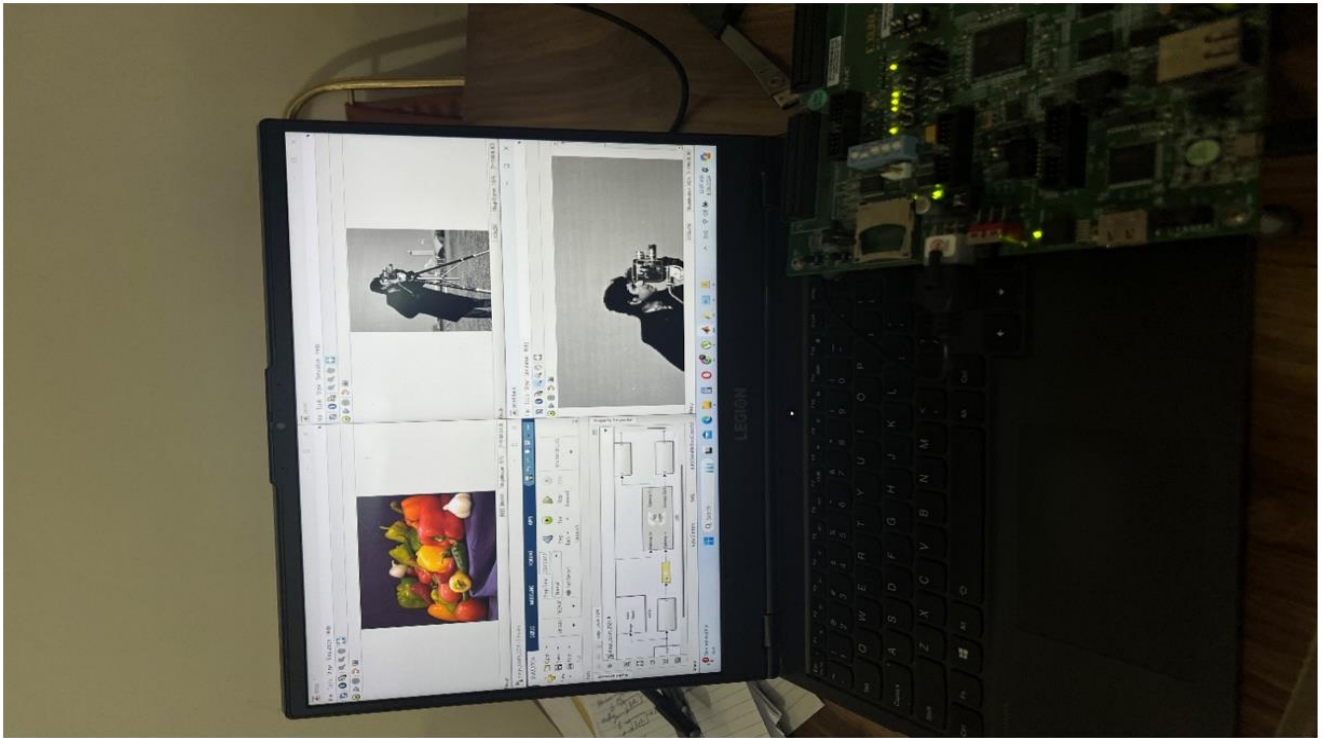
**Figure 20.**  
Power consumption of LSB\_PRNG in ZYNQ702 FPGA.

The final physical implementation of the design, providing clarified details about hardware implementation, is the Register Transfer Level (RTL) schematic. The hardware parameters for LSB-PRNG were 10 cells, 2 I/O ports, and 213 nets, as shown in Figure 21. It can be observed that the hardware is complex, according to the needs of the LSB-PRNG.



**Figure 21.**  
RTL view of the proposed design.

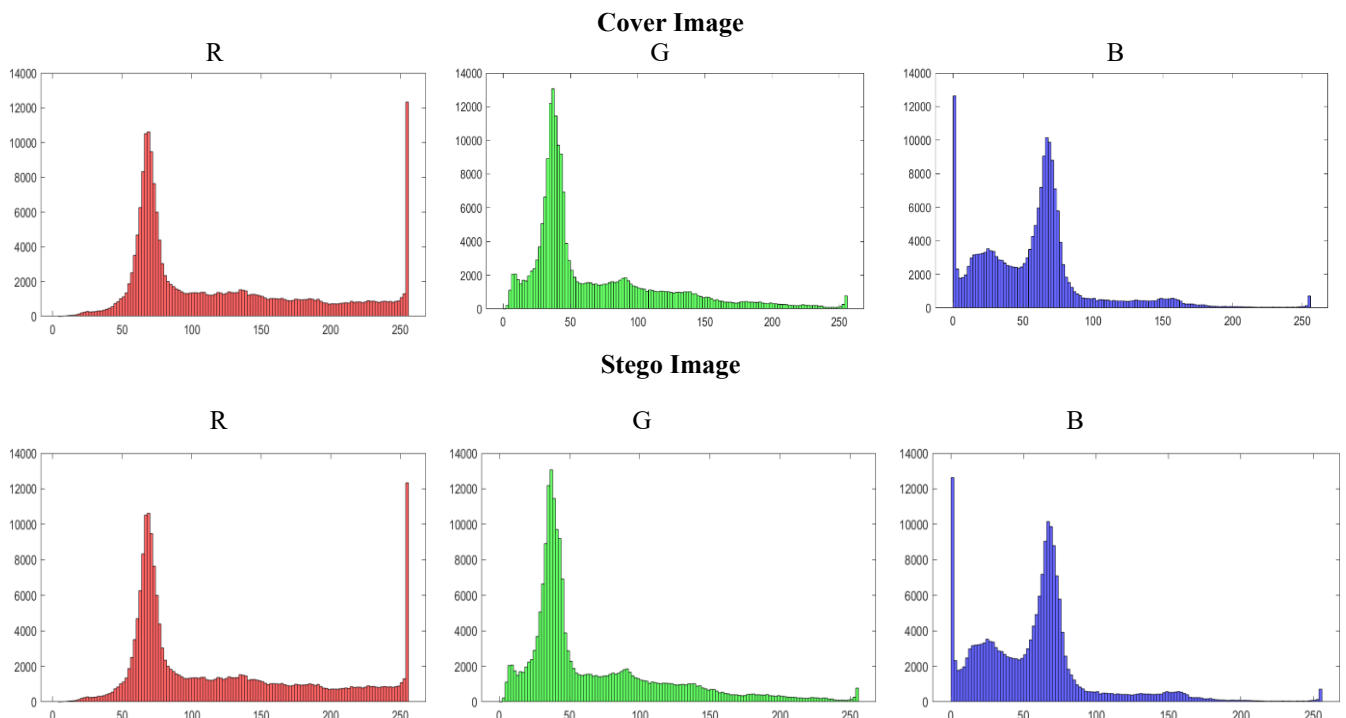
Hardware co-simulation, as shown in Figure 22 represents the final stage of FPGA design, which combines the design model with the ZYNQ702 evaluation board. It presents one secret image ("cameraman.tif") and a cover image ("peppers.png") with the ZYNQ702 FPGA board.



**Figure 22.**  
Hardware co-simulation of the proposed system using the ZYNQ702 FPGA.

### 3.3. Performance Analysis

A number of statistical tests have been conducted to assess whether the impact of data masking on image quality is within the permitted bounds. Several metrics, including histogram analysis, Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Cross-Correlation (CCR), and structural similarity, have been used for this evaluation.



**Figure 23.**  
Histogram Analysis.

### 3.4. Histogram

A visual representation demonstrates the pixel movement by mapping the number of pixels at each grayscale level. The statistical properties of the cover image remain unchanged even after altering certain coefficients, as evidenced by the comparison of the cover image's histogram with that of the stego image. As a result, the histogram of the stego image is nearly identical to that of the cover image as shown in Figure 23.



### 3.5. Mean Squared Error (MSE)

MSE is a statistical method used to evaluate how similar the stego image is to the original image. It works by calculating the error signal, which is the difference between the two signals being compared. The mean energy of this error signal is then determined using the corresponding equation:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (I_{original}(i,j) - I_{encrypted}(i,j))^2 \quad (4)$$

### 3.6. Peak Signal-to-Noise Ratio (PSNR)

PSNR is defined as the ratio of a signal's maximum power to the power of the noise that distorts it. It is usually expressed in decibels and is commonly used to evaluate how accurately an image can be reconstructed. In this context, the original data represents the signal, and the introduced error acts as the noise. The PSNR value reflects the quality of the image, with higher values indicating better quality.

$$PSNR = 10 \log_{10} \left( \frac{MAX^2}{MSE} \right) \quad (5)$$

### 3.7. Correlation

Cross-correlation is a mathematical technique frequently used to assess the similarity between two images. When comparing a Stego image with the original image, cross-correlation helps identify areas or patterns of similarity and difference. This process involves shifting one image across the other and calculating a similarity score at each position.

$$r = \frac{n \sum XY - \sum X \sum Y}{\sqrt{(n \sum X^2 - (\sum X)^2) \cdot (n \sum Y^2 - (\sum Y)^2)}} \quad (6)$$

### 3.8. Bit Error Rate (BER)

This key metric in image hiding for security measures indicates how many bit positions have been altered in the stego image. A value close to 1 suggests a higher number of bit errors, while a lower value indicates fewer errors.

$$BER = Be/Br \quad (7)$$

### 3.9. Structural Similarity

This image quality metric is used to assess the similarity index between images. A value close to one indicates greater similarity, while lower values suggest less similarity. Table 3 presents the overall performance metrics for the proposed hardware LSB algorithm used for data hiding.

**Table 3.**  
Performance measurements.

Performance metrics	Proposed work
PSNR	37.796
MSE	10.799
BER	0.19
SSIM	0.986
CCR	0.9988
Overall Execution Time	0.167 ms
Frequency	2.2 GHz
Throughput	17.76 Gbps

### 3.10. Conclusion and Future Work

This work involved employing XSG/SIMULINK integrated tools to implement an improved LSB steganography algorithm with a random position in the cover image. The study utilizes pseudo-random number generation for randomness using linear feedback shift registers with an initial key that is already shared between sender and receiver.

Employing the proposed key masking enhances the Stego system's resistance against attacks and unauthorized access to data, so the secret key was masked with another key, making it more secure and robust.

Hardware designs have been proposed and implemented on an FPGA chip (Xilinx ZYNQ702 evaluation board) using an XSG programming approach. The proposed design aimed to accelerate the LSB-PRNG algorithm and steganographic process. The following conclusions are obtained:

1. The cover image must be RGB, and the secret image is a grayscale.
2. Design an LFSR with a 12-bit size with the initial value exchanged between the transmitter and receiver.
3. Apply the encoding algorithm for the key to extract a 2-bit index hiding of secret bits inside cover bits utilizing the LSB algorithm.
4. The XSG methodology for FPGA implementation is a flexible tool that provides efficient integration between FPGA hardware-based design and XSG/SIMULINK software tools.
5. Applying FPGA hardware through XSG for hiding accelerates the processing of pixels and achieves a 2.22 GHz processing frequency and 17.76 Gbps throughput.

6. Performance metrics histogram, PSNR, MSE, BER, SSIM, CCR, overall execution time, frequency, and throughput were acceptable for robustness attack, so they increase security and decrease detectability.

The suggestions for future work are

1. FPGA-Based Image Steganography Detection using Artificial Neural Networks.
2. FPGA-based Pixel value differencing hiding method.
3. FPGA-based wavelet method for image steganography.
4. Stego-encryption accelerator system based on FPGA.

## Abbreviations:

FPGA, LFSR, PRNG, PRBG, XSG, CCR, MSE, PSNR.

## References

- [1] B. K. Pandey *et al.*, "Application of integrated steganography and image compressing techniques for confidential information transmission," *Cyber Security and Network Security*, pp. 169-191, 2022. <https://doi.org/10.1002/9781119812555.ch8>
- [2] D. M. Abdullah *et al.*, "Secure data transfer over internet using image steganography: Review," *Asian Journal of Research in Computer Science*, vol. 10, no. 3, pp. 33–52, 2021. <https://doi.org/10.9734/ajrcos/2021/v10i330243>
- [3] O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital steganography and watermarking for digital images: a review of current research directions," *IEEE Access*, vol. 8, pp. 166589–166611, 2020.
- [4] S. A. Parah, J. A. Sheikh, J. A. Akhoun, and N. A. Loan, "Electronic health record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, pp. 935-949, 2020. <https://doi.org/10.1016/j.future.2018.02.023>
- [5] H. G. Ayoub, "Dynamic iris-based key generation scheme during iris authentication process," in *Proc. 8th Int. Conf. Contemporary Information Technology and Mathematics (ICCITM)*, 2022.
- [6] A. T. Suhail, H. G. Ayoub, and A. A. Gharbe, "A strong algorithm for randomly hiding a secret files inside true color image using large primary secret key," *Egyptian Informatics Journal*, vol. 30, p. 100692, 2025.
- [7] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and medical imaging: An overview," *Journal of Digital Imaging*, vol. 33, no. 6, pp. 1527-1542, 2020.
- [8] Z. A. Abdulrazzaq, O. Tareq, O. H. Mohammed, and M. R. Ahmed, "New novel FPGA based image encryption methods using multiple chaotic maps," presented at the International Conference on Computer and Applications (ICCA) 2024.
- [9] A. T. Suhail and H. G. Ayoub, "A new method for hiding a secret file in several WAV files depends on circular secret key," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 33-43, 2022.
- [10] A. A. Salih, Z. A. Abdulrazzaq, and H. G. Ayoub, "Design and enhancing security performance of image cryptography system based on fixed point chaotic maps stream ciphers in FPGA," *Baghdad Science Journal*, vol. 21, no. 5, pp. 1754–1754, 2024.
- [11] H. G. Ayoub *et al.*, "Unveiling robust security: chaotic maps for frequency hopping implementation in FPGA," *Ain Shams Engineering Journal*, p. 103016, 2024.
- [12] S. Mehmood, "Visually meaningful image encryption," Ph.D. Dissertation, Capital Univ, 2020.
- [13] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos, Solitons & Fractals*, vol. 178, p. 114361, 2024. <https://doi.org/10.1016/j.chaos.2023.114361>
- [14] S. Pramanik *et al.*, *A novel approach using steganography and cryptography in business intelligence*. In A. Azevedo & M. F. Santos (Eds.), *Integration challenges for analytics, business intelligence, and data mining*. IGI Global, 2021. <https://doi.org/10.4018/978-1-7998-5781-5.ch010>
- [15] M. Thangamani and P. Thangaraj, "Fuzzy ontology for distributed document clustering based on genetic algorithm," *Applied Mathematics & Information Sciences*, vol. 7, no. 4, pp. 1563–1574, 2013. <https://doi.org/10.12785/amis/070413>
- [16] J. S. Khan and S. K. Kayhan, "Chaos and compressive sensing based novel image encryption scheme," *Journal of Information Security and Applications*, vol. 58, p. 102711, 2021. <https://doi.org/10.1016/j.jisa.2020.102711>
- [17] D. M. Hameed and R. R. Al-Nima, "High-performance character recognition system utilizing deep convolutional neural networks," *NTU Journal of Engineering and Technology*, vol. 3, no. 4, pp. 42–51, 2024. <https://doi.org/10.56286/ntujet.v3i4.1086>
- [18] O. F. AbdelWahab, A. I. Hussein, H. F. Hamed, H. M. Kelash, and A. A. Khalaf, "Efficient combination of RSA cryptography, lossy, and lossless compression steganography techniques to hide data," *Procedia Computer Science*, vol. 182, pp. 5-12, 2021. <https://doi.org/10.1016/j.procs.2021.02.002>
- [19] M. R. Islam, T. R. Tanni, S. Parvin, M. J. Sultana, and A. Siddiqua, "A modified LSB image steganography method using filtering algorithm and stream of password," *Information Security Journal: A Global Perspective*, vol. 30, no. 6, pp. 359-370, 2021. <https://doi.org/10.1080/19393555.2020.1854902>
- [20] P. S. Venugopala and A. Kumar, "CrypticCare: A strategic approach to telemedicine security using LSB and DCT steganography for enhancing patient data protection," *IEEE Access*, vol. 12, pp. 12345–12356, 2024.
- [21] A. A. Khan, O. Cheikhrouhou, and S. Al-Maadeed, "IMG-forensics: Multimedia-enabled information hiding investigation using convolutional neural network," *IET Image Processing*, vol. 16, no. 11, pp. 2854–2862, 2022. <https://doi.org/10.1049/ipr2.12272>
- [22] O. Datcu, C. Macovei, and R. Hobincu, "Chaos based cryptographic pseudo-random number generator template with dynamic state change," *Applied Sciences*, vol. 10, no. 2, p. 451. <https://doi.org/10.3390/app10020451>
- [23] S. Cang, Z. Kang, and Z. Wang, "Pseudo-random number generator based on a generalized conservative Sprott-A system," *Nonlinear Dynamics*, vol. 104, no. 1, pp. 827-844, 2021. <https://doi.org/10.1007/s11071-021-06310-9>
- [24] W. Zhao, Z. Chang, C. Ma, and Z. Shen, "A pseudorandom number generator based on the chaotic map and quantum random walks," *Entropy*, vol. 25, no. 1, p. 166. <https://doi.org/10.3390/e25010166>

- [25] S. Krishnamoorthi, R. K. Dhanaraj, and S. K. Hafizul Islam, "CCM-PRNG: Pseudo-random bit generator based on cross-over chaotic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 83, no. 34, pp. 80823-80846, 2024. <https://doi.org/10.1007/s11042-024-18668-0>
- [26] S. Rahman, M. Ahmed, and M. S. Islam, "A comprehensive study of digital image steganographic techniques," *IEEE Access*, vol. 11, pp. 6770-6791, 2023.
- [27] R. Khanfar, H. Ghannam, A. Alabdouli, and T. Rabie, "Effectiveness of pseudorandom number generators in secret image retrieval fidelity for steganography," *World Journal of Advanced Engineering Technology and Sciences*, vol. 12, no. 1, pp. 289-297, 2024. <https://doi.org/10.30574/wjaets.2024.12.1.0238>
- [28] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7951-7985, 2020. <https://doi.org/10.1007/s11042-019-08427-x>
- [29] F. Al-Shaarani and A. Gutub, "Securing matrix counting-based secret-sharing involving crypto steganography," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6909-6924, 2022. <https://doi.org/10.1016/j.jksuci.2021.09.009>
- [30] B. M. Krishna, C. Santhosh, S. Suman, and S. K. S. Shireen, "Evolvable hardware-based data security system using image steganography through dynamic partial reconfiguration," *Journal of Circuits, Systems and Computers*, vol. 31, no. 01, p. 2250014, 2021. <https://doi.org/10.1142/S0218126622500141>
- [31] D. Ayyed, "Image steganography based sobel edge detection using FPGA," 2020.
- [32] B. K. Yakti and D. Sari, "Processing speed comparison of the least significant bit (LSB) steganography algorithm on FPGA and Matlab," in *Proceedings of the 2021 Sixth International Conference on Informatics and Computing (ICIC)*, 2021.
- [33] S. Hussain, N. Sheybani, P. Neekhara, X. Zhang, J. Duarte, and F. Koushanfar, "FastStamp: Accelerating neural steganography and digital watermarking of images on FPGAs," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design (ICCAD '22)*, 2022, pp. 1-9. <https://doi.org/10.1145/3508352.3549357>
- [34] J.-y. Sun, H. Cai, Z.-b. Gao, C.-p. Wang, and H. Zhang, "A novel non-equilibrium hyperchaotic system and application on color image steganography with FPGA implementation," *Nonlinear Dynamics*, vol. 111, no. 4, pp. 3851-3868, 2023. <https://doi.org/10.1007/s11071-022-07993-4>
- [35] W. A. Al-Musawi, W. A. Wali, and M. A. Al-Ibadi, "Field-programmable gate array design of image encryption and decryption using Chua's chaotic masking," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 3, pp. 2414-2424, 2022. <https://doi.org/10.11591/ijece.v12i3.pp2414-2424>
- [36] J. Wei, L. Zhang, and Y. Li, "Implementing a low-complexity steganography system on FPGA," in *Proceedings of the 2021 9th International Conference on Intelligent Computing and Wireless Optical Communications (ICWOC)*, 2021.
- [37] L. N. Sabeeh and M. A. Al-Ibadi, *FPGA based accelerator for image steganography*. Singapore: Springer Nature Singapore, 2024, pp. 1-12. [https://doi.org/10.1007/978-981-99-7240-1\\_1](https://doi.org/10.1007/978-981-99-7240-1_1)
- [38] W. A. Al-Musawi, M. A. Al-Ibadi, and W. A. Wali, "Artificial intelligence techniques for encrypting images based on the chaotic system implemented on field-programmable gate array," *IAES International Journal of Artificial Intelligence*, vol. 12, no. 1, pp. 347-356, 2023. <https://doi.org/10.11591/ijai.v12.i1.pp347-356>
- [39] S. Jing-yu, C. Hong, W. Gang, G. Zi-bo, and H. Zhang, "FPGA image encryption-steganography using a novel chaotic system with line equilibria," *Digital Signal Processing*, vol. 134, p. 103889, 2023. <https://doi.org/10.1016/j.dsp.2022.103889>
- [40] T. J. Shah and M. T. Banday, *A review of contemporary image compression techniques and standards: Examining fractal image processing and analysis in examining fractal image processing and analysis*. IGI Global, 2020. <https://doi.org/10.4018/978-1-7998-0066-8.ch006>
- [41] C.-W. Kok and W.-S. Tam, *Digital image denoising in MATLAB*. Hoboken, NJ, USA: Wiley-IEEE Press, 2024.
- [42] A. Toktas and U. Erkan, "2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm," *Neural Computing and Applications*, vol. 34, no. 6, pp. 4295-4319, 2022.
- [43] M. Tarek and H. M. Ali, "Digital rights management of image content via LSB embedding and palindrome sequence," *Journal of King Saud University - Computer and Information Sciences*, 2023.
- [44] K. SundaraKrishnan, S. P. Raja, and B. Jaison, "A symmetric key multiple color image cipher based on cellular automata, chaos theory and image mixing," *Information Technology and Control*, vol. 50, no. 1, pp. 55-75, 2021. <https://doi.org/10.5755/j01.itc.50.1.28012>
- [45] K. Shaffa, "A region-based histogram and fusion technique for enhancing backlit images for cell phone applications," Doctoral Dissertation University of Nairobi, 2023.
- [46] N. Genser, J. Seiler, and A. Kaup, "Camera array for multi-spectral imaging," *IEEE Transactions on Image Processing*, vol. 29, pp. 9234-9249, 2020.
- [47] A. Ibrahim and E. M. El-Kenawy, "Image segmentation methods based on superpixel techniques: A survey," *Journal of Computer Science and Information Systems*, vol. 15, no. 3, pp. 1-11, 2020.
- [48] G. Ramesh, J. Logeshwaran, J. Gowri, and A. Mathew, "The management and reduction of digital noise in video image processing by using transmission based noise elimination scheme," *ICTACT Journal on Image & Video Processing*, vol. 13, no. 1, pp. 2797-2801, 2022.
- [49] G. M. Gibson, S. D. Johnson, and M. J. Padgett, "Single-pixel imaging 12 years on: A review," *Optics Express*, vol. 28, no. 19, pp. 28190-28208, 2020. <https://doi.org/10.1364/OE.403195>
- [50] S. Zeng, C. Liu, X. Huang, Z. Tang, L. Liu, and P. Zhou, "An application-specific image processing array based on WSe<sub>2</sub> transistors with electrically switchable logic functions," *Nature Communications*, vol. 13, no. 1, p. 56, 2022. <https://doi.org/10.1038/s41467-021-27644-3>
- [51] Y. Xian, X. Wang, and L. Teng, "Double parameters fractal sorting matrix and its application in image encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 6, pp. 4028-4037, 2021.
- [52] H. Cruz, M. Véstias, J. Monteiro, H. Neto, and R. P. Duarte, "A review of synthetic-aperture radar image formation algorithms and implementations: A computational perspective," *Remote Sensing*, vol. 14, no. 5, p. 1258, 2022. <https://doi.org/10.3390/rs14051258>
- [53] A. A. Hussain and G. K. AL-Khafaji, "A pixel based method for image compression," *Tikrit Journal of Pure Science*, vol. 26, no. 1, pp. 1813-1662, 2021.

- [54] M. S. Woolf, L. M. Dignan, A. T. Scott, and J. P. Landers, "Digital postprocessing and image segmentation for objective analysis of colorimetric reactions," *Nature Protocols*, vol. 16, no. 1, pp. 218-238, 2021.
- [55] M. Demirtaş, "A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos," *Optik*, vol. 265, p. 169430, 2022. <https://doi.org/10.1016/j.ijleo.2022.169430>
- [56] X. Jiang, J. Ma, G. Xiao, Z. Shao, and X. Guo, "A review of multimodal image matching: Methods and applications," *Information Fusion*, vol. 73, pp. 22-71, 2021.
- [57] F. Smarandache, M. A. Quiroz-Martínez, J. E. Ricardo, N. B. Hernández, and M. Y. L. Vázquez, "Application of neutrosophic offsets for digital image processing," *Investigación Operacional*, vol. 41, no. 5, pp. 603-611, 2020.
- [58] Z. Wang, E. Wang, and Y. Zhu, "Image segmentation evaluation: A survey of methods," *Artificial Intelligence Review*, vol. 53, no. 8, pp. 5637-5674, 2020. <https://doi.org/10.1007/s10462-020-09830-9>
- [59] D. Darwis, N. B. Pamungkas, and Wamiliana, "Comparison of least significant bit, pixel value differencing, and modulus function on steganography to measure image quality, storage capacity, and robustness," *Journal of Physics: Conference Series*, vol. 1751, no. 1, p. 012039, 2021. <https://doi.org/10.1088/1742-6596/1751/1/012039>
- [60] A. Reinke *et al.*, "Common limitations of image processing metrics: A picture story," *arXiv preprint arXiv:2104.05642*, 2021.
- [61] J. Fu, X. Zhang, Y. Wang, W. Zeng, and N. Zheng, "Understanding mobile GUI: From pixel-words to screen-sentences," *Neurocomputing*, vol. 601, p. 128200, 2024. <https://doi.org/10.1016/j.neucom.2024.128200>
- [62] M. Bemana, K. Myszkowski, H.-P. Seidel, and T. Ritschel, "X-Fields: Implicit neural view-, light-, and time-image interpolation," *ACM Transactions on Graphics*, vol. 39, no. 6, p. 1, 2020. <https://doi.org/10.1145/3414685.3417827>
- [63] H. Qin, R. Gong, X. Liu, X. Bai, J. Song, and N. Sebe, "Binary neural networks: A survey," *Pattern Recognition*, vol. 105, p. 107281, 2020. <https://doi.org/10.1016/j.patcog.2020.107281>
- [64] F. Pérez-Hernández, S. Tabik, A. Lamas, R. Olmos, H. Fujita, and F. Herrera, "Object detection binary classifiers methodology based on deep learning to identify small objects handled similarly: Application in video surveillance," *Knowledge-Based Systems*, vol. 194, p. 105590, 2020. <https://doi.org/10.1016/j.knosys.2020.105590>
- [65] T. Tuncer, S. Dogan, and F. Ozyurt, "An automated residual exemplar local binary pattern and iterative ReliefF based COVID-19 detection method using chest X-ray image," *Chemometrics and Intelligent Laboratory Systems*, vol. 203, p. 104054, 2020. <https://doi.org/10.1016/j.chemolab.2020.104054>
- [66] L. Vincent and E. R. Dougherty, *Morphological segmentation for textures and particles in digital image processing methods*. Boca Raton, FL: CRC Press, 2020. <https://doi.org/10.1201/9781003067054-2>
- [67] D. Chicco and G. Jurman, "The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC Genomics*, vol. 21, no. 1, p. 6, 2020. <https://doi.org/10.1186/s12864-019-6413-7>
- [68] M. Liao, Z. Wan, C. Yao, K. Chen, and X. Bai, "Real-time scene text detection with differentiable binarization," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 34, no. 7, pp. 11474-11481, 2020. <https://doi.org/10.1609/aaai.v34i07.6812>
- [69] L. Fan, K. W. Ng, C. Ju, T. Zhang, and C. S. Chan, "Deep polarized network for supervised learning of accurate binary hashing codes," in *Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI)*, 2020, pp. 825-831. <https://doi.org/10.24963/ijcai.2020/115>
- [70] N. Subramanian, "Image steganography using deep learning methods to detect covert communication in untrusted channels," Master's Thesis Qatar University, 2021. <http://hdl.handle.net/10576/17713>
- [71] P. C. Mandal, S. Saha, and S. Saha, "Digital image steganography: A literature survey," *Information Sciences*, vol. 609, pp. 1451-1488, 2022.
- [72] E. H. J. Halboos and A. M. H. Albakry, "Hiding text using the least significant bit technique to improve cover image in the steganography system," *Bulletin of Electrical Engineering and Informatics*, no. 6, pp. 3258-3271, 2022. <https://doi.org/10.11591/eei.v11i6.4337>
- [73] K. H. Abuhmaidan, M. A. Al-Share, A. M. Abualkishik, and A. Kayed, "Enhancing data protection in digital communication: A novel method of combining steganography and encryption," *KSII Transactions on Internet and Information Systems*, vol. 18, no. 6, pp. 1619-1637, 2024. <https://doi.org/10.3837/tiis.2024.06.011>
- [74] R. S. Hameed, A. H. B. Ahmad, M. M. Taher, and S. S. Mokri, "A literature review of various steganography methods," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 5, pp. 1-10, 2022.
- [75] A. AbdelRaouf, "A new data hiding approach for image steganography based on visual color sensitivity," *Multimedia Tools and Applications*, vol. 80, no. 15, pp. 23393-23417, 2021. <https://doi.org/10.1007/s11042-020-10224-w>
- [76] S. Bandyopadhyay, V. Goyal, S. Dutta, S. Pramanik, and H. H. R. Sherazi, *Unseen to seen by digital steganography: Modern-day data-hiding techniques*. In S. Pramanik, M. M. Ghonge, R. V. Ravi, & K. Cengiz (Eds.), *multidisciplinary approach to modern digital steganography*. IGI Global, 2021. <https://doi.org/10.4018/978-1-7998-7160-6.ch001>
- [77] M. Idakwo *et al.*, "An extensive survey of digital image steganography: state of the art," *ATBU Journal of Science, Technology and Education*, vol. 8, no. 2, pp. 40-54, 2020.
- [78] C. Zhang, P. Benz, A. Karjauv, G. Sun, and I. S. Kweon, "Udh: Universal deep hiding for steganography, watermarking, and light field messaging," *Advances in Neural Information Processing Systems*, vol. 33, pp. 10223-10234, 2020.
- [79] K. Sudha, "Text steganography using LSB insertion method along with chaos theory," *arXiv preprint arXiv:1205.1859*, 2012.
- [80] Z. Zhang, L. Wang, W. Zheng, L. Yin, R. Hu, and B. Yang, "Endoscope image mosaic based on pyramid ORB," *Biomedical Signal Processing and Control*, vol. 71, p. 103261, 2022. <https://doi.org/10.1016/j.bspc.2021.103261>
- [81] A. Mishra, M. Aggarwal, and A. Tiwari, "Concealing and encrypting: Dual approaches to data security in the digital age," *International Research Journal on Advanced Engineering and Management (IRJAEM)*, vol. 2, no. 8, pp. 2543-2552, 2024.
- [82] M. A. Bamanga, A. K. Babando, and J. Mayer, *Recent advances in steganography*. New York: IntechOpen, 2024.
- [83] S. S. Hashmi, A. A. Khan Mohammad, A. M. Abdul, C. Atheeq, and M. K. Nizamuddin, "Enhancing data security in multi-cloud environments: A product cipher-based distributed steganography approach," *International Journal of Safety & Security Engineering*, vol. 14, no. 1, 2024.
- [84] O. Kuznetsov, E. Frontoni, and K. Chernov, "Beyond traditional steganography: Enhancing security and performance with spread spectrum image steganography," *Applied intelligence*, vol. 54, no. 7, pp. 5253-5277, 2024.



- [85] I. Haverkamp and D. K. Sarmah, "Evaluating the merits and constraints of cryptography-steganography fusion: A systematic analysis," *International Journal of Information Security*, vol. 23, no. 4, pp. 2607-2635, 2024. <https://doi.org/10.1007/s10207-024-00853-9>
- [86] H. K. Tayyeh and A. S. A. Al-Jumaili, "A combination of least significant bit and deflate compression for image steganography," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, pp. 358-364, 2022. <https://doi.org/10.11591/ijece.v12i1.pp358-364>
- [87] M. A. Aslam *et al.*, "Image steganography using least significant bit (lsb)-a systematic literature review," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, 2022.
- [88] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, vol. 10, pp. 124053-124075, 2022.
- [89] Y. Bhavani, P. Kamakshi, E. Kavya Sri, and Y. Sindhu Sai, "A survey on image steganography techniques using least significant bit," in *Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2021*: Springer, 2022.
- [90] G. Brignone, M. T. Lazarescu, and L. Lavagno, "A DSP shared is a DSP earned: HLS task-level multi-pumping for high-performance low-resource designs," in *2023 IEEE 41st International Conference on Computer Design (ICCD)*, 2023: IEEE.
- [91] T. Prabu and K. Srinivasan, "Design and implementation of high-performance fpga accelerator for non-separable discrete fourier transform optimizing real-time image and video processing," *Journal of Nanoelectronics and Optoelectronics*, vol. 19, no. 8, pp. 843-856, 2024.
- [92] A. Choudhury, "Signal generation and evaluation using digital-to-analog converter and signal defined radio," Virginia Tech, Blacksburg, VA, USA, 2023.
- [93] S. Kashani, "Building chips faster: Hardware-compiler co-design for accelerated RTL simulation (Master's thesis, École Polytechnique Fédérale de Lausanne). EPFL repository," Lausanne, Switzerland, 2023.
- [94] X. Dai, X. Wang, H. Han, and E. Wang, "Construction algorithm of non-degenerate complex domain chaotic system with application on PRNG," *Nonlinear Dynamics*, vol. 112, no. 24, pp. 22439-22462, 2024.
- [95] T. Umar, M. Nadeem, and F. Anwer, "A new modified skew tent map and its application in pseudo-random number generator," *Computer Standards & Interfaces*, vol. 89, p. 103826, 2024. <https://doi.org/10.1016/j.csi.2023.103826>
- [96] Moussa K. H. *et al.*, "Various pseudo random number generators based on memristive chaos map model," *Multimedia Tools and Applications*, vol. 83, no. 21, pp. 59561–59576, 2024.
- [97] E. A. Albahrani, T. K. Alshekly, and S. H. Lafta, "New secure and efficient substitution and permutation method for audio encryption algorithm," *The Journal of Supercomputing*, vol. 79, no. 15, pp. 16616-16646, 2023.
- [98] F. Yu *et al.*, "Dynamic analysis and application in medical digital image watermarking of a new multi-scroll neural network with quartic nonlinear memristor," *The European Physical Journal Plus*, vol. 137, no. 4, p. 434, 2022.
- [99] S. Boancă, "Optimizations for learning from linear feedback shift register variations with artificial neural networks," in *IFIP International Conference on Artificial Intelligence Applications and Innovations*, 2024.
- [100] K. Vooke, N. K. Toramamidi, K. K. Thodeti, and S. Singh, "Design of pseudo-random number generator using non-linear feedback shift register," in *2022 First International Conference on Electrical, Electronics, Information and Communication Technologies 2022*. <https://doi.org/10.1109/ICEEICT53079.2022.9768456>
- [101] A. Devrari and A. Kumar, "Reconfigurable linear feedback shift register for wireless communication and coding," *International Journal of Reconfigurable and Embedded Systems*, vol. 12, no. 2, p. 195, 2023. <https://doi.org/10.11591/ijres.v12.i2.pp195-204>
- [102] S. Abdel-Hafeez, "Programmable feedback shift register," *Circuits, Systems, and Signal Processing*, vol. 42, no. 8, pp. 4784-4808, 2023. <https://doi.org/10.1007/s00034-023-02332-3>
- [103] M. Grymel, "New programmable lfsr counters with automatic encoding and state extension," *Electronics*, vol. 13, no. 2, p. 405, 2024.
- [104] S. Gupta, G. Goyal, and A. K. Rana, "Analysis of different LFSRs for VLSI IC testing," in *2024 IEEE 4th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA)*, 2024: IEEE.
- [105] A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, "Analysis of synchronous stream cryptoconversions," in *Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies*. Cham: Springer International Publishing, 2022, pp. 47-64. [https://doi.org/10.1007/978-3-030-79770-6\\_4](https://doi.org/10.1007/978-3-030-79770-6_4)