*International Journal of Computational and Experimental Science and ENgineering (IJCESEN)*

*Vol. 11-No.3 (2025) pp. 4475-4482*
*http://www.ijcesen.com*

***ISSN: 2149-9144***



**Research Article**

# Efficient FPGA Implementation of Visual Cryptography Using AES Algorithm and Share Generation Technique

**Sapna P J[1*], Sudha K L[2], Deepa N P[3], K N Pushpalatha[4]**

[1]Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka, India.
* **Corresponding Author Email:** sapnanoorithaya@gmail.com- **ORCID:** 0000-0001-9359-5426

[2] Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka, India
**Email:** drsudha-ece@dayanandasagar.edu - **ORCID:** 0000-0001-8301-1669

[3] Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru-560111, Karnataka, India
**Email:** deepnp@gmail.com- **ORCID:** 0000-0003-4840-7689

[4] Department of Computer Science and Engineering (Data Science), Sai Vidya Institute of Technology, Bengaluru-560064, Karnataka, India.
**Email:** knpdrs@gmail.com - **ORCID:** 0000-0002-2313-1148

**Article Info:**

**DOI:** 10.22399/ijcesen.3070
**Received :** 23 March 2025
**Accepted :** 19 June 2025

**Keywords**

AES Algorithm
Share Generation Technique
Visual Cryptography

**Abstract:**

Visual Cryptography is the latest secure communication technique where the secured data is always in the form of an image from which a finite number of shares are generated using a mathematical model. At the receiver side, the secret image is generated from these shares using a reverse mathematical approach. In this Article, Efficient FPGA Implementation of Visual Cryptography using AES Algorithm and Share Generation Technique is proposed. To increase security, AES algorithm is used for encoding, and is further subjected to share generation, the entire architectural level is designed to achieve optimum utilization without affecting the reconstruction quality, which is then coded using VHDL language and implemented on Zybo Z7-10 FPGA board. The comparison results show that the proposed technique is better in terms of both hardware parameters and reconstructed image quality.

## 1. Introduction

In the rapid evolution of communication technologies over recent decades, the speed and scale of data transmission have experienced exponential growth. This has facilitated seamless communication across various platforms, from internet-based services to mobile networks. However, alongside these advancements comes the heightened risk of unauthorized access and interception of sensitive data during transmission. To mitigate these risks, encryption techniques are employed to safeguard information by converting it into an unintelligible format for unauthorized users. Despite the effectiveness of encryption, vulnerabilities exist within traditional cryptographic methods, making them susceptible to specific types of attacks. In response, researchers have continually sought to enhance encryption techniques, incorporating advancements in cryptography and related fields to bolster security and protect against evolving threats.

As encryption methodologies continue to evolve, leveraging innovations in chaos-based encryption [1], curve-based cryptography [2], quantum cryptography [3], neuro-chaos cryptography [4], and lightweight cryptography [5], the landscape of data protection is evolving rapidly. Among these advancements, visual cryptography has garnered significant attention for its unique approach to enhancing data transmission security. By employing dual layers of encoding, visual cryptography provides an additional layer of security, complementing traditional cryptographic algorithms. However, the integration of cryptographic algorithms with visual cryptography

introduces complexities, particularly in software implementations where processing time can be a limiting factor. To address this challenge, hardware-based implementations, particularly those leveraging Field-Programmable Gate Arrays (FPGAs), offer promising solutions. FPGA technology allows for hardware reconfiguration, enabling efficient execution of complex cryptographic algorithms while minimizing processing time and resource utilization.

In this article, we propose a novel hardware architecture designed to address the challenges associated with implementing visual cryptography using FPGA technology. Our architecture aims to efficiently encrypt and decrypt images while maintaining high-quality decrypted images. By leveraging the capabilities of FPGAs, our proposed architecture offers a robust solution for enhancing data transmission security in image encryption applications. Through this research, we aim to contribute to the advancement of visual cryptography techniques and their practical implementation in real-world applications.

## 2. Literature Survey

Advancements in cryptography and image encryption have been showcased through various studies. A novel splitting methodology [6] for the mix column method within AES, yielding significant improvements in area and power efficiency was first proposed. Building on this foundation, subsequent research [7] presented a median-based technique for FPGA-based image encryption, focusing on reducing encryption time while [8] extended the AES block with ALU blocks to offer users customizable security options. Further enhancing performance, [9] advanced pipeline and expansion technologies, significantly improving throughput and latency in AES encryption was proposed.In terms of security, correlations between intermediate data and energy traces within AES was explored [10], highlighting the effectiveness of certain attack methods. A novel S-Box design [11] using Composite Field Arithmetic, addressing vulnerabilities was implemented along with ECC techniques [12] for Visual Cryptography, ensuring security in color images. Specialized applications were also addressed, tailoring a visual cryptography technique [13][14][15] for secure transactions in QR-based online payment systems, providing users with an accessible interface. Additionally, innovative approaches such as the collaborative visual cryptography framework [16] proposed showcased advancements in cryptographic operations.Finally, as advanced reconstruction techniques an error diffusion-based framework [17] for generating high-quality reconstructed images were explored. These studies collectively contribute to the continual improvement and evolution of cryptography and image encryption techniques.

## 3. Proposed Architecture

The hardware architecture proposed for visual cryptography is illustrated in Fig. 1. and the architecture is divided into two main sections: transmitter and receiver. On the transmitter side, the input image undergoes encryption using the "modified AES encryption" block. The output pixels from this encryption process are then utilized by the "share generation" block, along with assistance from the "Random Sequence Generator" block, to generate shares. Subsequently, these shares are transmitted through communication channels. On the receiver side, the encrypted version of the input image is reconstructed from the received shares using the "Random Sequence Generator" and "Merging" blocks. Following this reconstruction, the outputs are decrypted using the "Modified AES decryption" block to properly reconstruct the hidden image.

### 3.1. AES Encryption and Decryption

The Advanced Encryption Standard (AES), widely recognized for its effectiveness, is extensively utilized in encryption procedures [18]. AES operates through bitwise operations on input data, making it particularly suitable for implementation at the hardware level. For processing 128 bits of plaintext, it is imperative to partition the entire plaintext into multiple blocks, each containing 16 bits. These 16 bytes are then organized into a matrix format comprising rows and columns, facilitating encryption and decryption operations

The encryption process, as depicted in Fig. 2. encompasses several stages: Sub-byte substitution, Shift Rows, Mix Columns and Add Round Key.

(a) Sub-byte: This stage utilizes a Rajendel S-box matrix and is implemented through a shifter architecture.

(b) Shift Rows: The rows of the matrix undergo left shifting, with the "fall-off" bits reinserted to the right of the row. At the hardware level, this operation is achieved through a simple rotate register architecture.

(c) Mix Columns: Each column's four bytes undergo transformation using a mathematical function, thereby replacing the original column and resulting in a new matrix.

(d) Add Round Key: The 16 bytes of the matrix are concatenated to form a 128-bit block, which is then XORed with the round key.

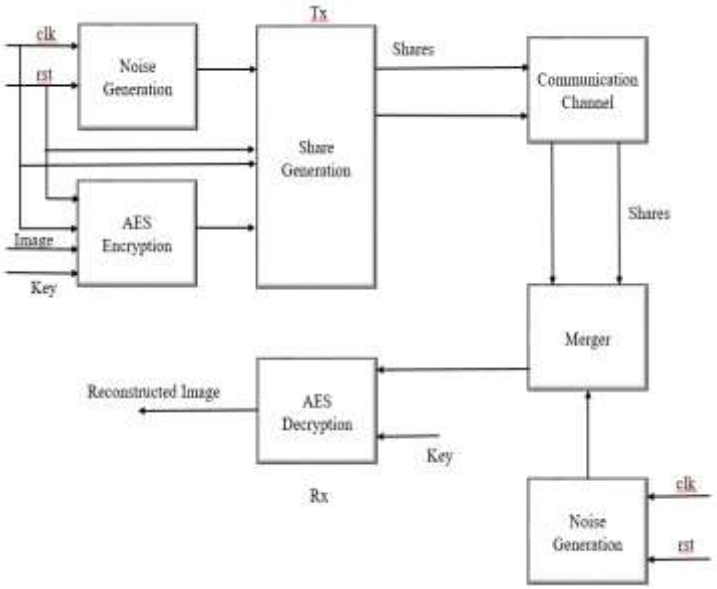


***Figure 1**. Hardware architecture of visual cryptography algorithm*

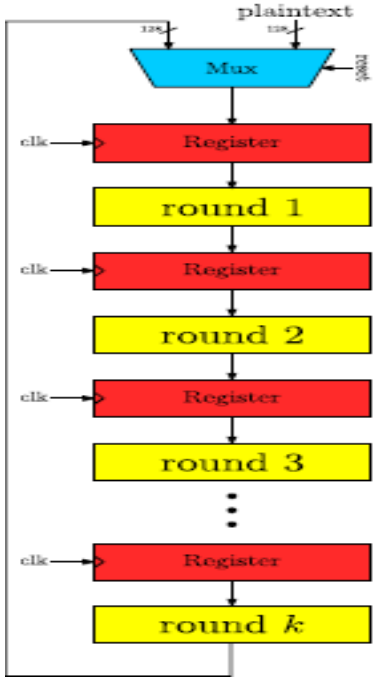


***Figure 2.** Basic structure of AES*

The complete encryption algorithm is described in Fig.3. At the hardware level, the complex architecture of the S-box utilized in AES can be simplified to a look-up table, easing implementation challenges and ensuring minimal area consumption for the pre-processing technique. The key schedule round function computes all round keys. The decryption process involves the reverse operations of encryption, as depicted in Fig.4. Inverse Subbytes, Inverse Shift Rows, Inverse Mix Columns, and Inverse Round Function constitute the steps followed in decryption.

### 3.1.1. Mathematical analysis

The input secret image P is used along with Key K for the encryption. The block-wise encryption of P, which is the secret image, is done using Eq. (1)

$$C1=AES\_(K,M\ XOR\ P1) \quad (1)$$

Here AES_E is the AES encryption algorithm for which the inputs is the secret key C1 that is block 1 of the ciphered image C. ith block is encrypted using Eq. (2)

$$Ci=AES\_(K,C(i-1)\ \ XOR\ Pi) \quad (2)$$

Where i= 2,.....n

### 3.2. Noise generation and linear feedback shift register (LFSR) encoding

Noise generation is a critical aspect in various applications, although true randomness is often difficult to achieve. To address this challenge, pseudo-random sequence generators (PRSGs) [19] are commonly utilized. In this paper, we focus on employing a 16-bit PRSG equation to generate noise with improved randomness characteristics. Linear Feedback Shift Register (LFSR) sequences [20] are frequently employed for approximating white noise signals in communication systems and for masking codes. For instance, consider a 2x2 matrix serialized to [1 2 3 4]. This serialized matrix is then combined with an LFSR table, derived from the LFSR 1+x^6+x^9 equation , resulting in a sequence represented as [1023 1022 1020 1016 1008 992 960 896 769 515 7...].

This process effectively incorporates the LFSR-generated sequence to enhance the randomness of

the noise signal, thus demonstrating its utility in practical applications. As a result the output becomes [1021 1018 1011 996]. During the share generation process, two bits are considered from opposite directions. For instance, when considering the number 1021, it is represented as 1011111111. In the receiver, the inverse operation is conducted to recover the original numbers by employing a concatenation operation (e.g., [1021 1018 1011 996]). These recovered numbers are then subtracted from the LFSR sequence generated using the same equation/architecture. This process enables the retrieval of the exact input numbers. Any discrepancies observed can be attributed to the truncation error inherent in the AES algorithm.

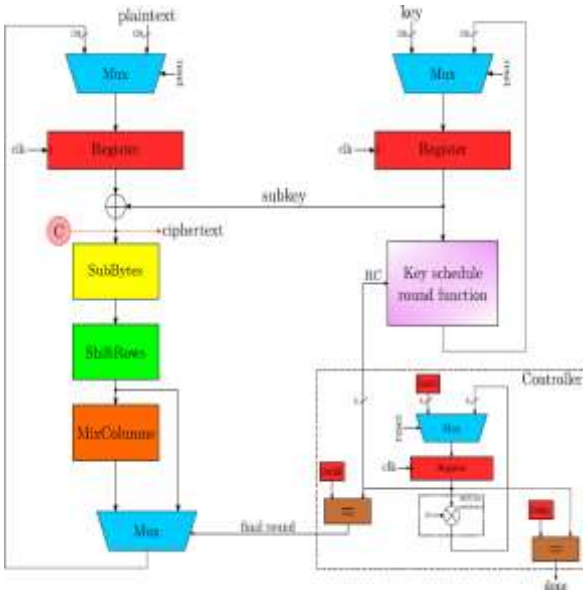


***Figure 3.*** *AES encryption algorithm*

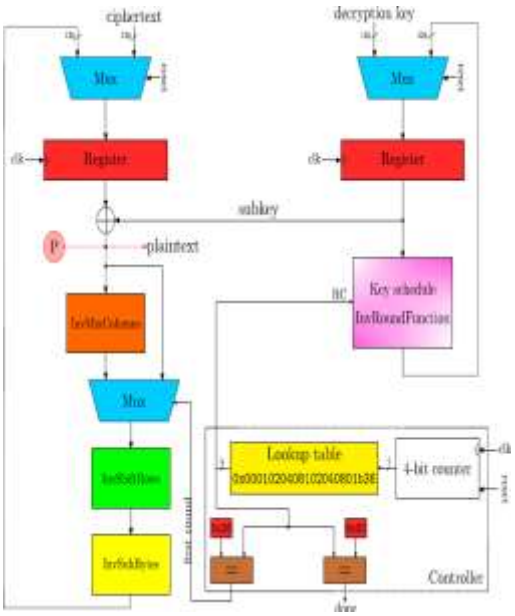


***Figure 4.*** *Algorithm for AES decryption*

## 3.3. Visual cryptography

Visual cryptography serves as a robust secret image sharing technique, ensuring secure preservation of sensitive information. In this method, a secret image containing confidential data is securely transmitted from the sender to the recipient, maintaining utmost security and confidentiality. This is achieved by dividing the secret image into multiple shares, which are then transmitted through separate channels to the recipient. Upon reception, the shares are collected and subjected to reverse visual cryptographic techniques to reconstruct the original secret image [21]. One of the primary advantages of visual cryptography is its ability to prevent image tampering, as adversaries would only possess disjoint segments of the original image even if they manage to intercept the shares [22]. In the proposed scheme, an AES-encrypted image, combined with noise generated from LFSR coding, serves as input to the visual cryptography scheme, resulting in the generation of four shares as depicted in Fig 5. The encryption and decryption processes involved in generating these shares are elucidated in detail below.

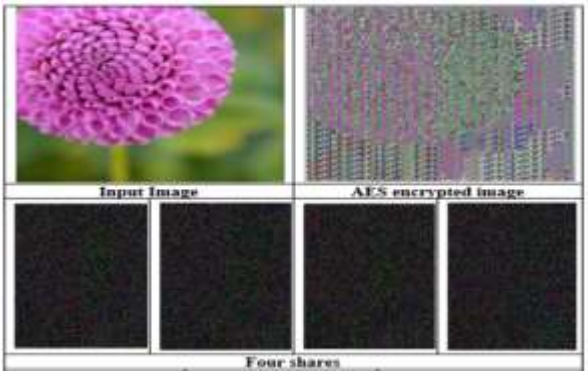


***Figure 5.*** *Visual cryptography scheme for share generation*

### 3.3.1. Encryption

At this stage, a finite set of images, each matching the size of the input images, is generated using mathematical modeling. This process guarantees that each share resembles noise. Additionally, without the correct sequencing of the shares, it becomes impossible to reconstruct the original image. The hardware architecture for visual cryptographic encryption is depicted in Fig. 6. The encryption process comprises three main operations: addition, concatenation, and mixing of blocks. Both the AES encrypted image and the noise image are of equal size. Initially, the input pixel value is added with a specific noise point amplitude in the first stage, resulting in a matrix of the same size as the input. Subsequently, in the second stage, the binary values of all pixels are concatenated in reverse order, thereby enhancing image security. Given that each

pixel value consists of eight bits, concatenating 2 bits per share generates four shares. This concatenation

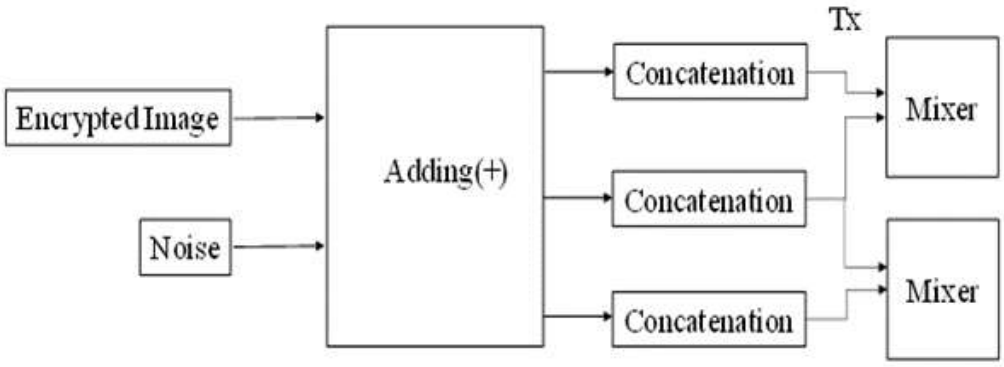


***Figure 6.*** *Hardware architecture for encryption using visual cryptography*

is facilitated by a dedicated concatenation block, producing distinct bytes. These bytes are then mixed using a mixer in the third stage to generate noise-like shares.

### 3.3.2. Decryption

The decryption method mirrors the encryption process, as illustrated in Fig. 7. For successful decryption, the noise generator source employed must exhibit similar characteristics to the noise generator used during transmission. To initiate decryption, each byte from the shares is extracted, and the last two bits are concatenated from all shares. Subsequently, all concatenated bits are combined using a mixer block. These pixel values are then subtracted from the noise image to recover the encrypted image.

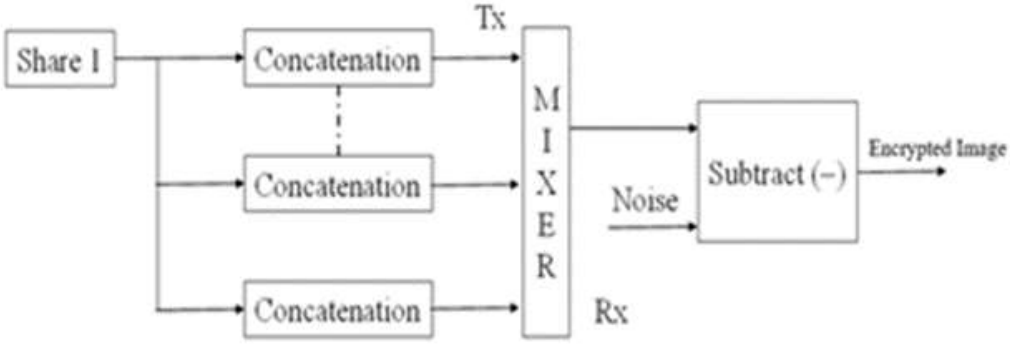


***Figure 7.*** *Hardware architecture for decryption using visual cryptography*

## 4. FPGA Implementation

FPGA, an extensively utilized integrated circuit, offers reconfigurability, enabling rapid switching between different functions with each configuration. Programmable interconnects facilitate the connection of configurable logic blocks within the FPGA [23]. In the implementation of visual cryptography in hardware, the transition occurs from behavioral description to physical design. Given the paramount importance of security and practicality in cryptography, FPGA emerges as a preferred choice for implementation [24]. The proposed architecture is realized on the Digilent Zybo Z7-10 FPGA board, with coding performed using standard VHDL language [25]. Synthesis is conducted using the Xilinx ISE tool. Hardware utilization metrics of the proposed architecture, along with its sub-blocks, are presented in Table 1.

***Table 1.*** *Hardware utilizations*

| Parameters | AES Algorithm | | Visual Cryptography | | Total Architecture |
|---|---|---|---|---|---|
| | Encryption | Decryption | Transmitter | Receiver | |
| **Slice Registers** | 264 | 260 | 402 | 414 | 734 |
| **Slice LUT's** | 1104 | 1490 | 1138 | 1603 | 2720 |
| **LUT-FF pairs** | 264 | 260 | 336 | 321 | 698 |
| **Frequency(MHz)** | 255.68 | 336.4 | 255.68 | 336.443 | 255.68 |

The actual wiring and lower-level representations in Hardware Description Language (HDL) are achieved through the creation of high-level representations. This process involves Register-Transfer Level (RTL) abstraction. To ensure the correctness of the design, the RTL schematic is utilized. Fig. 8. illustrates the top-level RTL block, while Fig.9. provides a detailed technological block representation.

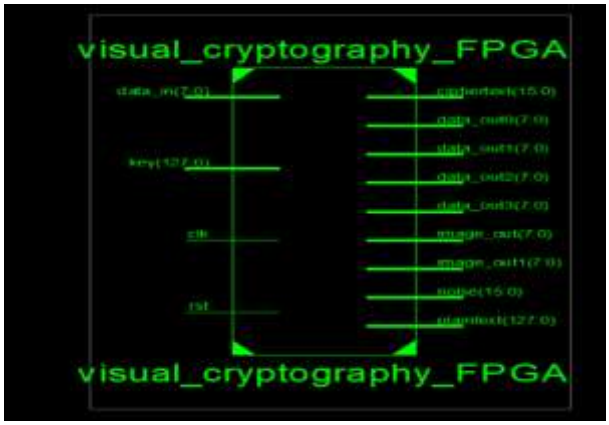


***Figure 8.*** *Top level RTL block*

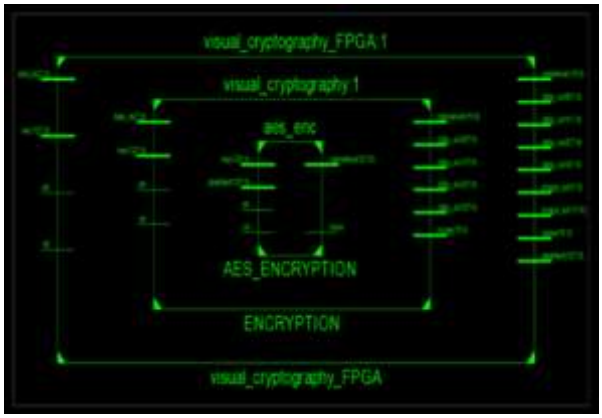


***Figure 9.*** *Technological block*

Fig. 10. depicts an illustration of the pre-optimized design, represented in terms of generic symbols. These symbols include multipliers, counters, adders, AND gates, and OR gates, which are not specific to the targeted Xilinx device. Likewise, Fig. 11. presents the technology schematic of the proposed Visual Cryptography architecture, which has been HDL optimized for a specific Xilinx architecture. This schematic represents components such as LUTs, buffers, I/Os, and other technological elements essential for early detection of design issues. Additionally, Fig. 12. showcases images generated from each sub-block of the proposed architecture. MATLAB image processing toolboxes [26] were utilized for this purpose. The sequence begins with the input secret image, followed by the AES encrypted image, which undergoes visual cryptography to produce four shares: share1, share2, share3, and share4.

## 5. Comparison With Existing Techniques

Table 2 presents a comparison between existing techniques and the proposed architecture in terms of hardware parameters. It is evident from the table that the proposed architecture requires fewer resources compared to existing techniques. This reduction in resource utilization can be attributed to the architectural optimizations implemented in the proposed approach. During the recovery stage, inverse visual cryptography is applied to reconstruct the image before decryption. Subsequently, AES decryption is employed to retrieve the reconstructed image.

***Table 2.*** *Hardware comparisons of different AES architectures*

| Author's | Device | Slice Registers | Frequency (MHz) |
|---|---|---|---|
| **Harshali et al., [22]** | Virtex-7 | 4089 | ---- |
| **Q. Liu. et al., [23]** | Virtex-4 | 1975 | 192.68 |
| **Y. Wang et al., [24]** | Virtex-6 | 15,612 | 14.69 |
| **Proposed Architecture** | Zynq-7 | 734 | 255.689 |

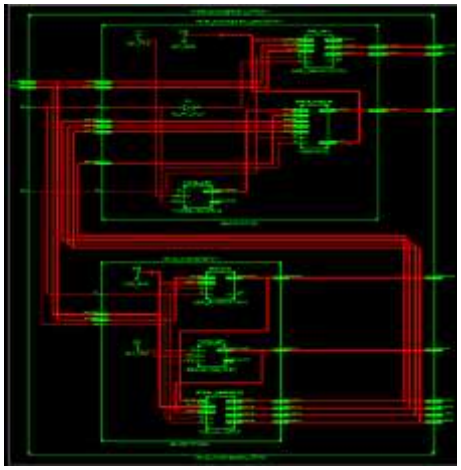

***Figure 10.*** *RTL Schematic of proposed visual cryptography architecture*

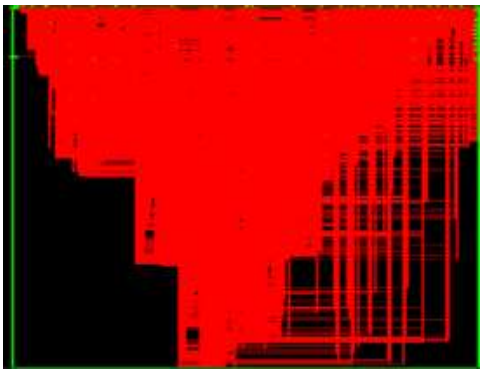

***Figure 11.*** *Technology schematic of proposed visual cryptography architecture*

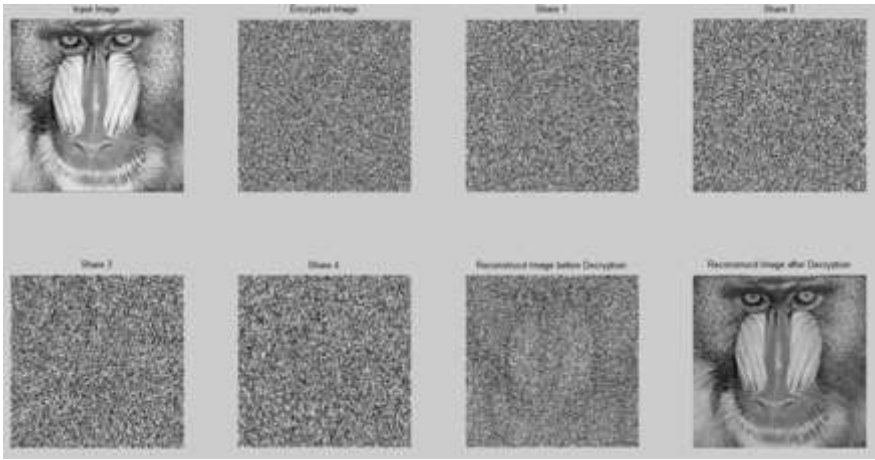

***Figure 12.*** *Generated images from proposed visual cryptography architecture*

## 6. Conclusion

This paper presents an efficient hardware architecture for visual cryptography, utilizing VHDL language for coding and tested on the Digilent Zybo Z7-10 FPGA board. Architectural optimizations are applied to reduce hardware requirements while maintaining accuracy through adequate bit sizing for internal computations. To enhance security, AES algorithms are integrated with LFSR technique. Validation of results is conducted through comparisons with existing techniques, with functionality verified by comparing output images with secret images. Results indicate similarity between the recovered image and the secret image, highlighting the effectiveness of the proposed technique. Comparative analysis in a tabular format demonstrates the advantage of the proposed algorithm over current methods. Given that this study represents the initial implementation of a Visual cryptographic algorithm using FPGA, future work may explore the adoption of more robust visual cryptographic algorithms. Additionally, consideration can be given to incorporating multiple secret images for enhanced secret sharing capabilities.

## Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

## References

[1] Maazouz, M., Toubal, A., Bengherbia, B., Houhou, O., & Batel, N. (2022). FPGA implementation of a chaos-based image encryption algorithm. *Journal of King Saud University – Computer and Information Sciences, 34*, 9926–9941.

[2] Morales-Sandoval, M., Rodriguez Flores, L. A., Cumplido, R., Garcia-Hernandez, J. J., Feregrino, C., & Algredo, I. (2020). A compact FPGA-based accelerator for curve-based cryptography in wireless sensor networks. *Journal of Sensors, 2021*, Article ID 8860413. https://doi.org/10.1155/2021/8860413

[3] Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. *IEEE Access, 12*, 23206–23219.

[4] Bonny, T., & Al Nassan, W. (2024). Neuro Chaos Crypt: Revolutionizing chaotic-based cryptosystem with artificial neural networks—A comparison with traditional cryptosystems. *IEEE Access, 4*. https://doi.org/10.1109/ACCESS.2024.3395527

[5] Kumar, S., Kumar, D., Lamkuche, H., Sharma, V. S., Alkahtani, H. K., Elsadig, M., & Bivi, M. A. (2024). SHC: 8-bit compact and efficient S-Box structure for lightweight cryptography. *IEEE Access, 12*, 39430–39449.

[6] Rupanagudi, S. R., Bhat, V. G., Anushree, R., & Kavitha, Y. (2016). A novel and highly secure encryption methodology using a combination of AES and visual cryptography. In *2016 International Conference on Advances in Computing,*

*Communications and Informatics (ICACCI)* (pp. 1682–1688). IEEE.

[7] Goel, A., & Chaudhari, K. (2016). FPGA implementation of a novel technique for selective image encryption. In *2nd International Conference on Frontiers of Signal Processing (ICFSP)* (pp. 15–19). IEEE.

[8] Gaur, N., Mehra, A., & Kumar, P. (2018). Enhanced AES architecture using extended set ALU at 28nm FPGA. In *5th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 437–440). IEEE.

[9] Chen, S., Hu, W., & Li, Z. (2019). High performance data encryption with AES implementation on FPGA. In *IEEE 5th International Conference on Big Data Security on Cloud (Big Data Security), High Performance and Smart Computing (HPSC), Intelligent Data and Security (IDS)* (pp. 149–153). IEEE.

[10] Bu, A., Dai, W., Lu, M., Cai, H., & Shan, W. (2018). Correlation-based electromagnetic analysis attack using Haar wavelet reconstruction with low-pass filtering on an FPGA implementation of AES. In *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference on Big Data Science and Engineering* (pp. 1897–1900). IEEE.

[11] Gangadari, B. R., & Ahamed, S. R. (2015). FPGA implementation of compact S-Box for AES algorithm using composite field arithmetic. In *Annual IEEE India Conference (INDICON)* (pp. 1–5). IEEE.

[12] Shankar, K., & Eswaran, P. (2017). RGB-based multiple share creation in visual cryptography with aid of elliptic curve cryptography. *China Communications, 14*(2), 118–130.

[13] Jia, X., Wang, D., Ni, D., & Zhang, C. (2018). Collaborative visual cryptography schemes. *IEEE Transactions on Circuits and Systems for Video Technology, 28*(5), 1056–1070.

[14] Porwal, P., Panda, A. K., Sarad, H., Hritvij, H., & Sapna, P. J. (2022). Security system based on image encryption using fractal matrix method. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), 4*(7), e-ISSN: 2582-5208.

[15] Ahmad, L., Al-Sabha, R., & Al-Haj, A. (2021). Design and implementation of a secure QR payment system based on visual cryptography. In *7th International Conference on Information Management (ICIM)*. IEEE.

[16] Yan, B., Xiang, Y., & Hua, G. (2019). Improving the visual quality of size-invariant visual cryptography for grayscale images: An analysis-by-synthesis (AbS) approach. *IEEE Transactions on Image Processing, 28*(2), 681–694.

[17] ,Stallings, W. (2014). *Cryptography and network security: Principles and practice*. Prentice Hall.

[18] Roth, C. H. (Jr.). (1992). *Fundamentals of logic design* (1st ed.). Jaico Publishing House.

[19] Bakeva, V., Dimitrova, V., & Kostadinoski, M. (2014). Pseudo random sequence generators based on the parastrophic quasigroup transformation. In *ICT Innovations 2014* (pp. 125–134). Springer.

[20] Panda, A. K., Rajput, P., & Shukla, B. (2012). FPGA implementation of 8, 16 and 32-bit LFSR with maximum length feedback polynomial using VHDL. In *International Conference on Communication Systems and Network Technologies* (pp. 769–773). IEEE.

[21] Sasaki, M., & Watanabe, Y. (2018). Visual secret sharing schemes encrypting multiple images. *IEEE Transactions on Information Forensics and Security, 13*(2), 482–491.

[22] Karolin, M., & Meyyappan, T. (2019). Secret multiple share creation with color images using visual cryptography. In *IEEE Advance Technology of Humanity*. https://doi.org/10.1109

[23] Sikka, P., Asati, A. R., & Shekhar, C. (2020). Speed optimal FPGA implementation of the encryption algorithms for telecom applications. *Microprocessors and Microsystems, 79*, 103324. https://doi.org/10.1016/j.micpro.2020.103324

[24] Garipcan, A. M., & Erdem, E. (2021). FPGA implementation and statistical analysis of a high-speed, and low-area TRNG based on an AES S-box post-processing technique. *ISA Transactions*. https://doi.org/10.1016/j.isatra.2021.01.054

[25] Roth, C. H. (Jr.). (2006). *Digital system design using VHDL*. Cengage Learning.

[26] Gonzalez, R. C., Woods, R. E., & Eddins, S. L. (2009). *Digital image processing using MATLAB* (2nd ed.). Gatesmark Publishing.