SRI VENKATESWARA COLLEGE OF ENGINEERING&TECHNOLOGY
(AUTONOMOUS)
R.V.S NAGAR, CHITTOOR – 517127. (A.P)
Department of Electronics and Communications Engineering

PROJECT PRESENTATION SUBMITTED BY THE TEAM
BATCH NO: **A 12**

VLSI Implementation of Image Encryption and Decryption Using Reversible Logic Gates

UNDER THE GUIDENCE OF :

S.Lavanya (M Tech)

Assistant Professor,

Dept of ECE

Presentation by:

A.Siva Prasad [21781A0404]
B.Poorna Chandu [21781A0420]
B.Jaswanth Kumar [21781A0421]
B.Vinay Kumar [21781A0429]
B.Karthik [21781A0432]

CONTENTS

ABSTRACT:

Reversible logic synthesis and testing is a fascinating research area as it is an important approach for low power design and quantum computing. Reversible computations have different applications such as quantum computing, nanotechnology, digital signal processing, bio-information etc. All these applications require a cryptography system to restrict the unauthorized access and thus maintain the confidentiality of data. High area and power requirements are some of the major problems of well se cured cryptography algorithms. In this work, a Reversible Logic Gates Cryptography Design (RLGCD) is proposed to overcome these problems. RLGCD is used to design both encryption and decryption architectures. Linear Feedback Shift Register is used to generate the key for encryption and decryption processes. To further improve the security of data watermarking is done using Least Significant Bit (LSB) method. The FPGA performance of RLGCD architecture is evaluated. There is a great improvement in the performance of RLGCD architecture when compared to other conventional systems.

INTRODUCTION :-

1.Cryptography Ensures Data Confidentiality By Converting Plain Text Into Unreadable Cipher Text And Recovering It Back Through Decryption.

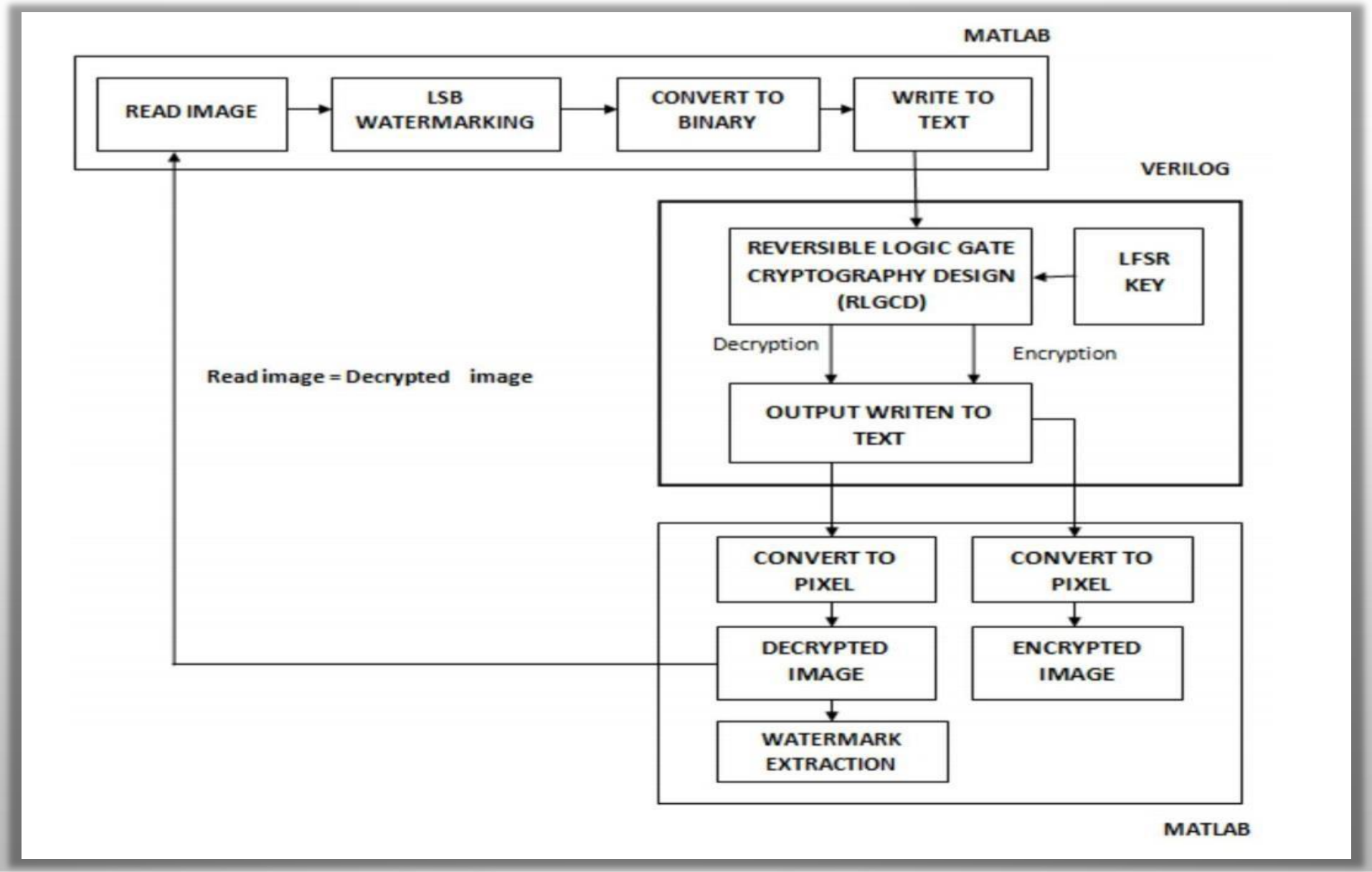
2. VLSI Design Faces Challenges Like Heat Dissipation Due To Increasing Transistor Density, Which Affects Power Efficiency.

3.Reversible Logic Gates Minimize Information Loss And Heat Dissipation, Offering An Energy-efficient Solution.

4.This Project Uses Linear Feedback Shift Registers (LFSR) For Key Generation, Enhancing Security In Encryption And Decryption Processes.

5.Watermarking Using The Least Significant Bit (LSB) Technique Further Strengthens Data Protection.

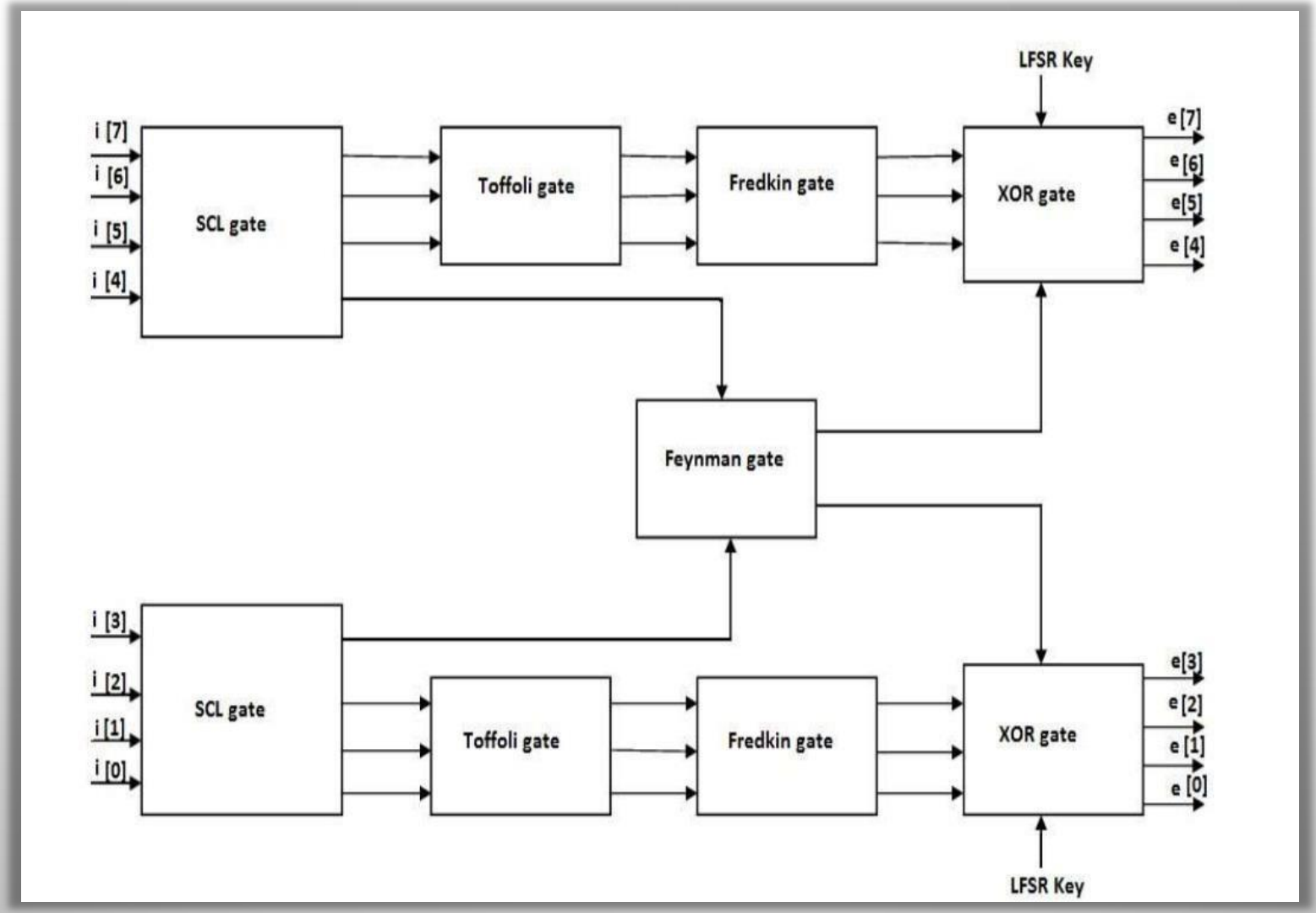
BLOCK DIAGRAM



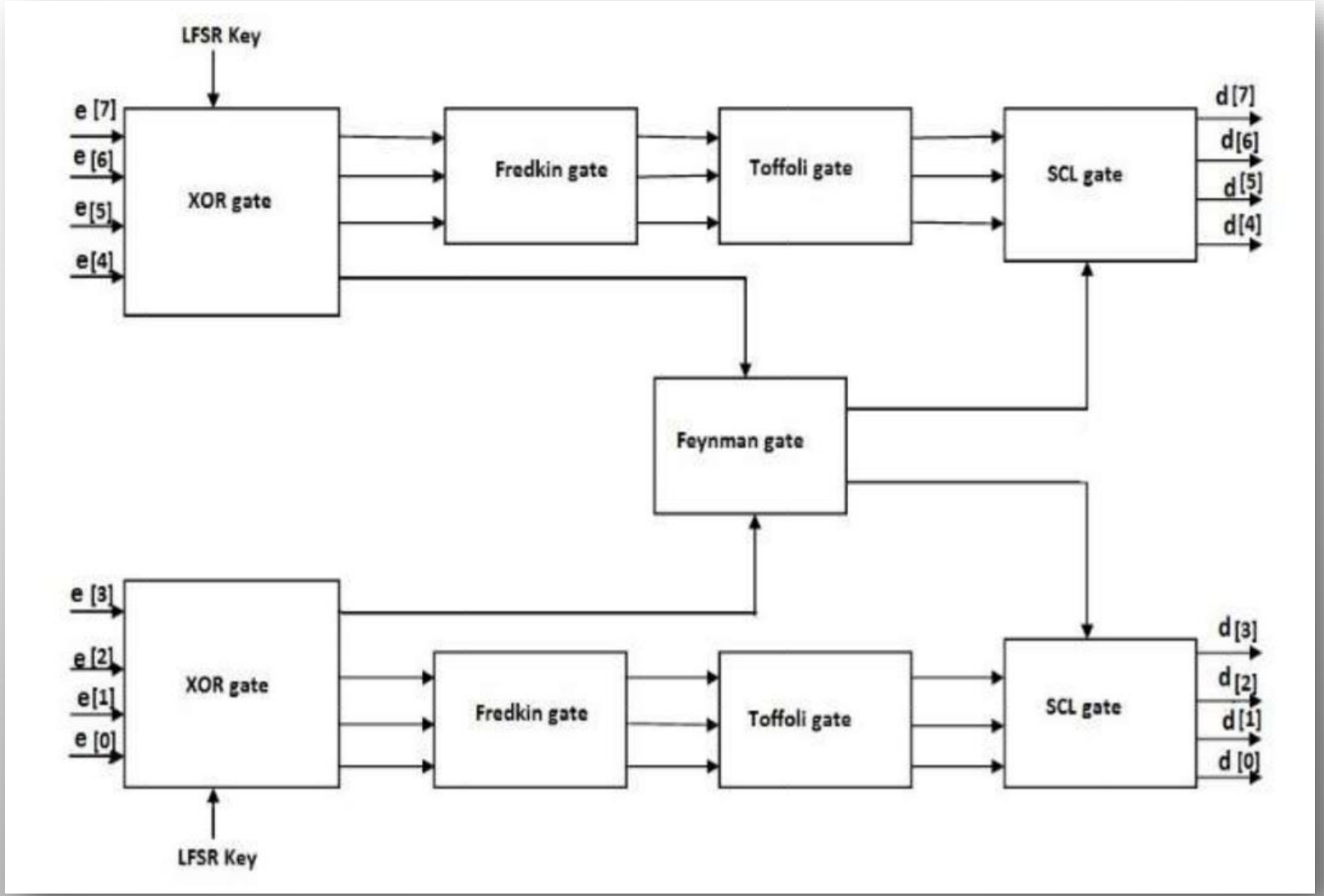
SYSTEM WORKFLOW:-

- **Image Input**: The System Takes The Original Image As Input For Encryption.
- **Pixel Processing**: The Image Pixels Are Converted Into Binary Data For Processing.
- **Encryption With Reversible Logic**: Reversible Gates (E.G., Fredkin, Toffoli) Apply Encryption Operations.
- **Key Generation**: A Random Key Is Generated Using A Reversible Logic-based Key Generator.
- **Encrypted Image Output**: The Encrypted Image Is Generated And Stored Or Transmitted.
- **Decryption Process**: The Encrypted Image Is Processed With The Same Key Using Reversible Gates.
- **Original Image Recovery**: The System Reconstructs The Original Image After Decryption.

Encryption Block



Decryption Block



ADVANTAGES:-

- Low Power Consumption: Reversible Logic Reduces Energy Dissipation, Making The System More Power-efficient.
- Improved Security: Enhances Data Protection With Complex Encryption Using Reversible Gates.
- Fault Tolerance: Reversible Circuits Offer Better Error Correction Capabilities.
- Reduced Heat Generation: Minimizes Power Loss, Leading To Lower Heat Production In Hardware.

ADVANTAGES:-

Parameters	Existing System	Proposed System
Delay Report	3.08ns	2.734ns

Area Report	69 LUTS	12 LUTS
Power	25mw	17.50mw

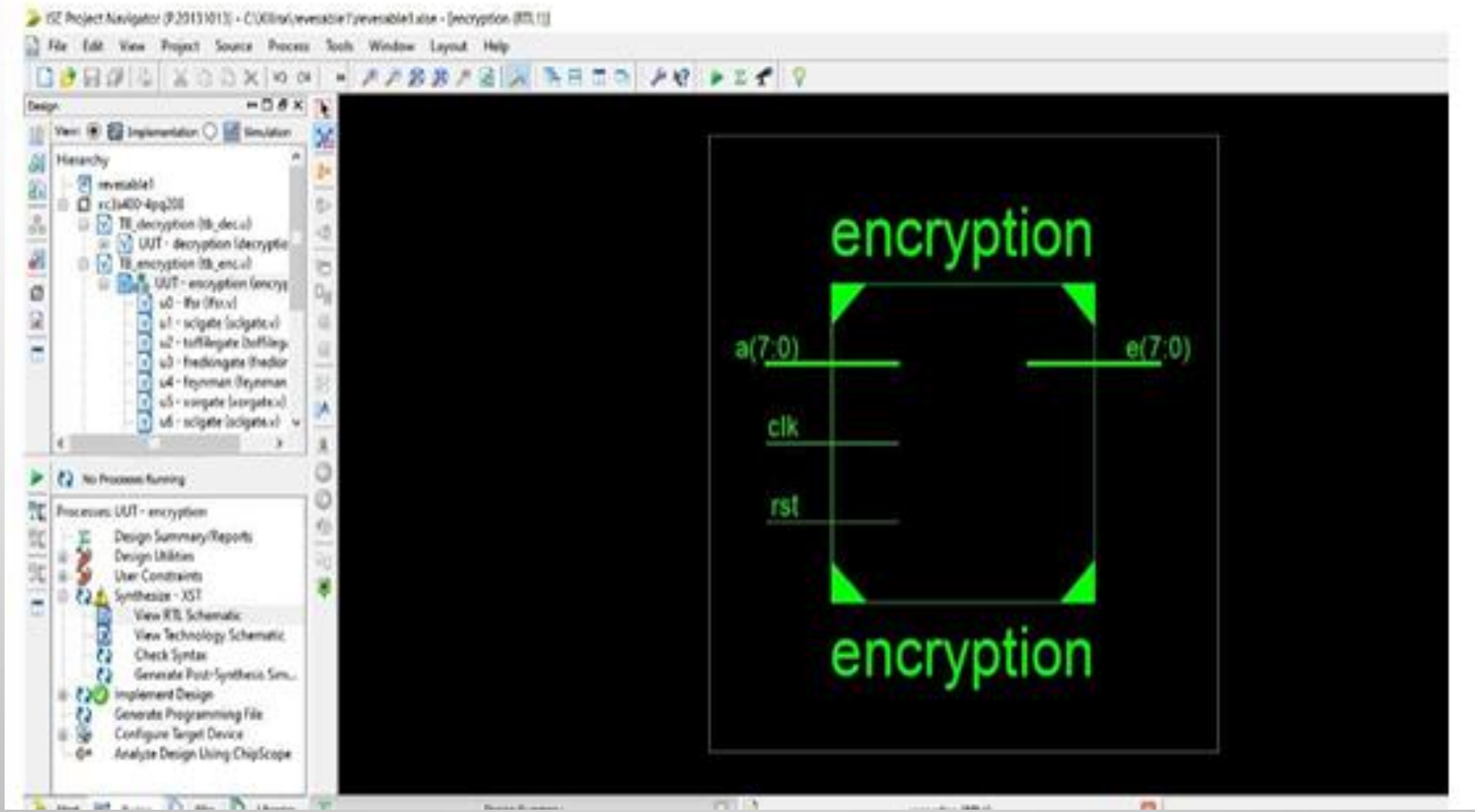
Operation

The proposed system operates through an efficient sequence of steps that integrate MATLAB processing with VLSI-based Verilog implementation. Initially, an input image is loaded into MATLAB, where watermarking is applied using the Least Significant Bit (LSB) technique. This method subtly embeds watermark data into the third and fourth LSB's of the image pixels, making the watermark invisible to the human eye while ensuring secure data hiding. The watermarked image is then converted into a binary format and saved as a text file. This file serves as the input to the Verilog-based encryption module.

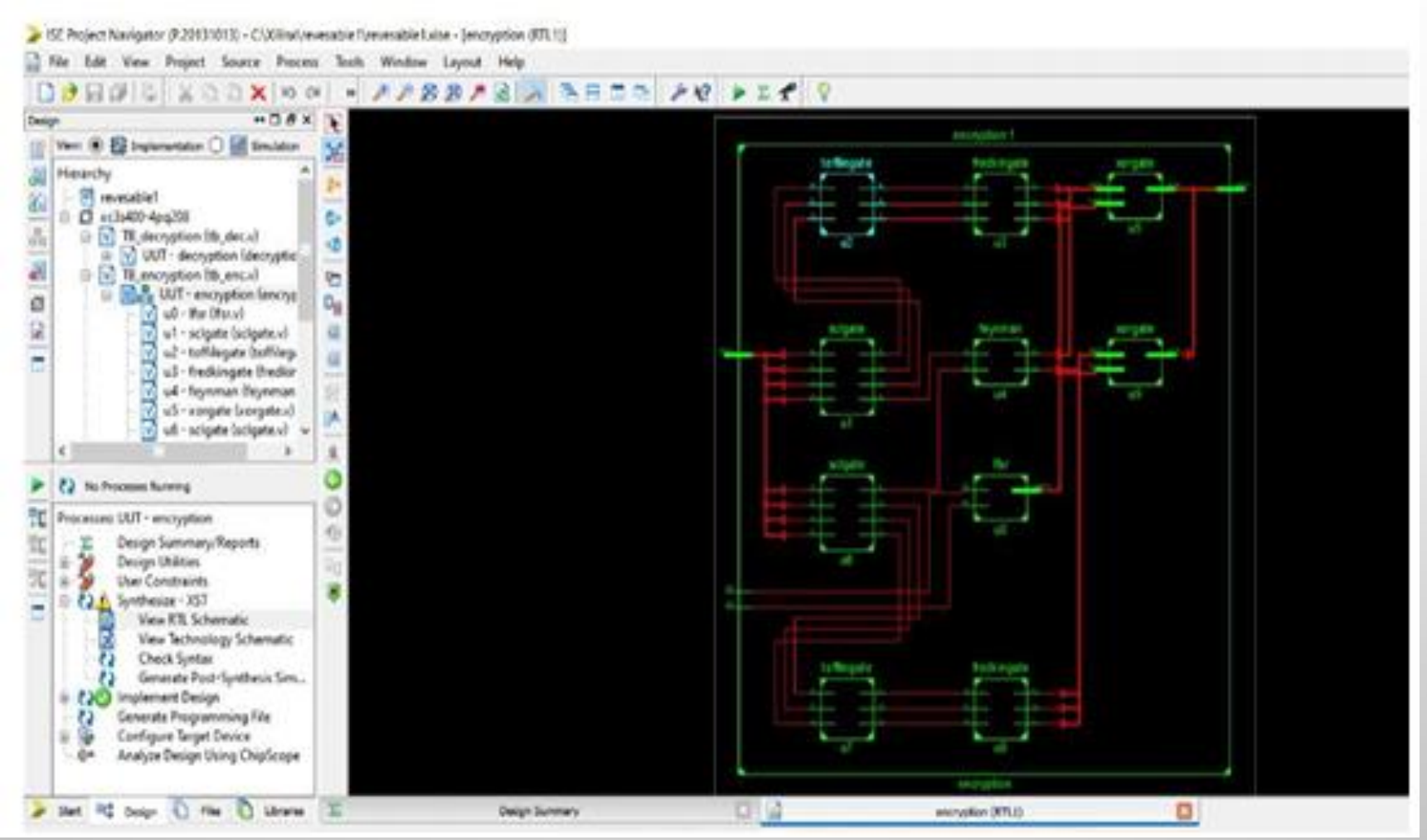
In the encryption phase, a cryptographic key is generated using a Linear Feedback Shift Register (LFSR), which ensures a pseudo-random key sequence for secure data encryption. The actual encryption is performed using a combination of Reversible Logic Gates (RLG's) such as Feynman, Fredkin, Toffoli, and Peres gates. These gates facilitate low-power, information-lossless processing of the binary data. The encrypted data is stored and later used in the decryption module, which reverses the encryption operations using the same RLG logic and key.

Finally, the decrypted binary data is read back into MATLAB, where it is reconstructed into the original image and the embedded watermark is extracted. The process confirms both image fidelity and data security, showcasing the advantages of reversible logic in cryptographic VLSI applications.

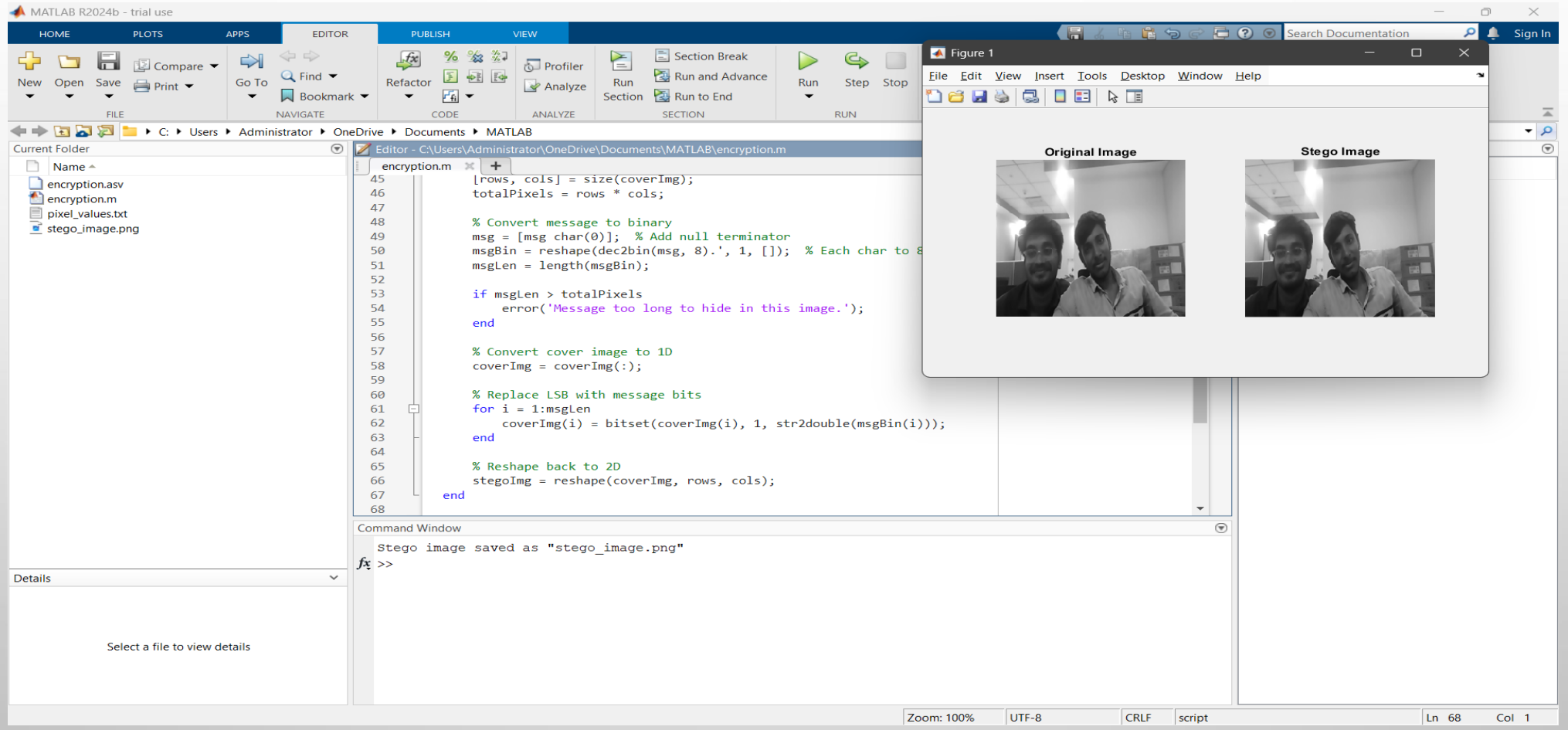
Operation



Operation


File Edit View Project Source Process Tools Window Layout Help
Design
Hierarchy
reversible1
xc3s400-4pq208
TB_decryption (tb_dec.v)
UUT - decryption (decryptic
TB_encryption (tb_enc.v)
UUT - encryption (encryp
u0 - tfor (for.v)
u1 - sclgate (sclgate.v)
u2 - toffilegate (toffileg
u3 - fredkingate (fredkir
u4 - feynman (feynman
u5 - xorgate (xorgate.v)
u6 - sclgate (sclgate.v)
No Processes Running
Processes: UUT - encryption
Design Summary/Reports
Design Utilities
User Constraints
Synthesize - XST
View RTL Schematic
View Technology Schematic
Check Syntax
Generate Post-Synthesis Sim...
Implement Design
Generate Programming File
Configure Target Device
Analyze Design Using ChipScope
Start
Design
File
Libraries
Design Summary
encryption (RTL)

OUTPUT


MATLAB R2024b - trial use
HOME
PLOTS
APPS
EDITOR
PUBLISH
VIEW
Search Documentation
Sign In
New
Open
Save
Compare
Print
Go To
Find
Bookmark
Refactor
Profiler
Analyze
Run Section
Section Break
Run and Advance
Run to End
Run
Step
Stop
FILE
NAVIGATE
CODE
ANALYZE
SECTION
RUN
C: ▸ Users ▸ Administrator ▸ OneDrive ▸ Documents ▸ MATLAB
Current Folder
Name
encryption.asv
encryption.m
pixel_values.txt
stego_image.png
Editor - C:\Users\Administrator\OneDrive\Documents\MATLAB\encryption.m
encryption.m
[rows, cols] = size(coverImg);
totalPixels = rows * cols;
% Convert message to binary
msg = [msg char(0)]; % Add null terminator
msgBin = reshape(dec2bin(msg, 8).', 1, []); % Each char to 8
msgLen = length(msgBin);
if msgLen > totalPixels
error('Message too long to hide in this image.');
end
% Convert cover image to 1D
coverImg = coverImg(:);
% Replace LSB with message bits
for i = 1:msgLen
coverImg(i) = bitset(coverImg(i), 1, str2double(msgBin(i)));
end
% Reshape back to 2D
stegoImg = reshape(coverImg, rows, cols);
end
Command Window
Stego image saved as "stego_image.png"
>>
Details
Select a file to view details
Figure 1
File Edit View Insert Tools Desktop Window Help
Original Image
Stego Image
Zoom: 100%
UTF-8
CRLF
script
Ln 68
Col 1

OUTPUT

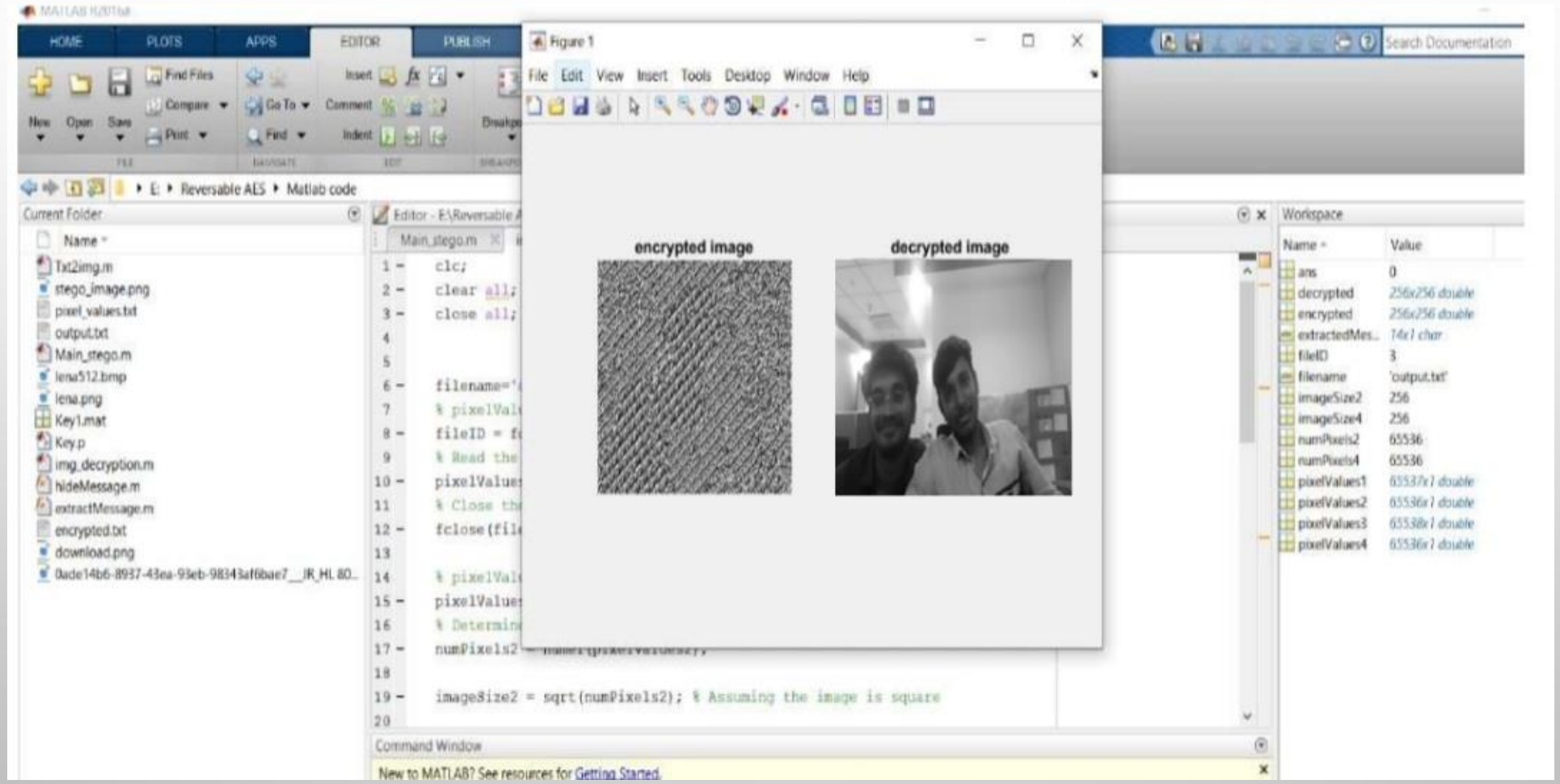


Figure 1
File Edit View Insert Tools Desktop Window Help
encrypted image
decrypted image
Current Folder
Workspace
Command Window
New to MATLAB? See resources for Getting Started.

Conclusion

This work presents a Reversible Logic Gate Cryptography Design using LFSR key with watermarking. The reversible gates like Feynman, Fredkin, Toffoli and SCL gates are used in this new cryptography system design. Since a cryptography system demands not only high security but low power consumption this work is one of the best among existing systems. those binary values are written into a text file. This input pixel values are read using Xilinx ISE. The RLGCD architecture consisting of LFSR, encryption block and decryption block is implemented in Xilinx software.

The Xilinx performance result for Spartan3E XC3S500E device gives a far better performance as compared to other existing systems. The reversible logic gates are the fundamental requirement in the emerging field of quantum computation. Thus, each work using the reversible logic gates will help to move forward in the field of quantum logic.

FUTURE SCOPE: Since the successful implementation of Reversible Logic Gates-based Image Encryption and Decryption (RLGCD) using Verilog code, there is a strong potential for its future deployment on Application-Specific Integrated Circuits (ASICs). This suggests that the encryption and decryption process, already proven effective in a digital simulation environment, can be translated into dedicated hardware, potentially offering enhanced performance and efficiency.

References

1) Meenal Dadhe, Prof. Anup. R. Nage, “Design of high-speed VLSI architecture for LFSR with maximum length feedback polynomial,” in International Journal for Scientific Research & Development, vol .3, no. 5, 2015.
2) Y. G. Praveen Kumar, B. S. Kriyappa, M. Z. Kurian, “Implementation of power efficient 8-bit reversible linear feedback shift register for BIST,” in 2017 International Conference on Inventive Systems and Control, Coimbatore, 2017.
3) B. Koziel, R. Azarderakhsh, M. Mozaffari Kermani, D. Jao, “Post- SEMANTIC SEGMENTATION AND CLASSIFICATION OF LIVER CANCER FROM MRI IMAGES Dept of E.C. E, SRIT Page 54 quantum cryptography on FPGA based on isogenies on elliptical curve,” in IEEE Trans.Circuits Syst.I, vol. 64, no. 1, pp. 86–99, Jan. 2019.
4) B. Koziel, R. Azarderakhsh, M. Mozaffari Kermani, “A high performance and scalable hardware architecture for isogeny-based cryptography,” in IEEE Trans.Comput., vol. 67, no. 11, pp. 1594–1609, Nov,2018. 15) H. Zodpe, A. Sapkal, “An efficient AES implementation using FPGA with enhanced security features,” in J. King Saud Univ.Eng.Sci., 2022, in press.

THANK YOU