ISSN: 2366-1313

AN EFFECTIVE DESIGN FOR DATA ENCRYPTION AND DECRYPTION USING REVERSIBLE LOGIC GATES

[1]P.Naga Mani, [2]Y.Anusha, [3]Y. Pavan Kumar , [4]T.Siva Teja, [5]Ms. Sk.Gousiya Begum, [6]Dr.D. Vijaya Saradhi

[1]BTech student, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

[2]BTech student, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

[3]BTech student, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

[4]BTech student, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

[5]Assistant Professor, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

[6]Associate Professor, Dept. Of ECE, Malineni Perumallu Educational Society's Group of institutions, Guntur, AP.

Abstract: *The development in the field of nano-meter technology is reducing the power consumption of common-sense circuits. Common sense reversible design has been one of the most promising technologies that have received the most attention due to coffee's low heat dissipation and electricity consumption. On the other hand, it can reduce the power dissipation of the reversible common-sense gates to zero. Recently, an approach to cryptography-based primarily on reversible governance circuits has been proposed. This document presents a solution for designing data encoding and decoding schemes based on reversible reconfigurable logic. Our solution's basic building block of the encoder and decoder is a 4-input reversible gate string. This way, the building block can perform any reversible function of four variables. For this reason, a reversible logic gate has been proposed. This type of reconfigurable reversible gate is designed from standard ones, such as NOT, CNOT, Fredkin, and Toffoli. This document provides a complete scheme for encoding and decoding nine-bit statistics using Verilog HDL. Simulation of this scheme received and verified in Xilinx ISE 14.7*

ISSN: 2366-1313

***Keywords**: nano-meter technology, Image encryption, Image decryption, Least Significant Bit.*

I. INTRODUCITON

Increasing technology has increased the demand for high-performance computing. According to J. Moore's rule, the number of transistors to be combined according to the unit area of

the devices will roughly double in a year and a half. An increased packing density is required within the logic circuits, which leads to increased heat dissipation to achieve fast computation. Conventional computing cannot handle the low power, excessive compactness, and heat dissipation issues of the next-generation computing environment. More recently, it has been transferred to cryptography. A reversible gate is a one-to-one correspondence between its inputs and its outputs. Research into reversible circuits of governance is stimulated by advances in quantum computing, nanotechnology, and coffee and electricity design. As a final result, the reversible synthesis of good judgment has been extensively studied. Interest is focused on synthesizing circuits generated from the NCT gate library: the NOT, CNOT, and Toffoli gates. Modern simulation equipment based on FPGAs made it possible to model such circuits. In the research paper, we look at the application of reverse logic to incremental encoding and decoding circuits [1] . The goal of this work became the easy implementation of coding using common sense reversible circuits. The primary key identifies each gate used in a reversible gate chain. Encryption and decryption statistics are determined by selecting private primary keys, unique cascades, and specific substitutions. For this reason, a reconfigurable and reversible logic door has been proposed. Mainly Xilinx ISE-based simulation results for simple fact encoding and decoding circuits generated from reversible and reconfigurable wise gates are presented in the research paper.

ISSN: 2366-1313

Encryption is a technique of protecting information by changing it into an unreadable format, thus keeping statistics confidential. This procedure involves converting plain text content into ciphertext using encryption and the method by which unique statistics, i.e., cleartext, are retrieved, called decryption. Heat dissipation is one of the primary tasks in designing a VLSI. Now, the miniaturization of the size of integrated circuits and the increase in the diversity of transistors are happening every day. So far, this is subject to Moore's Law [2]. But with further integration and scaling, the amount of heat dispersed increases even more. Landauer's panels confirmed that for every small amount of information lost, there could be heat dissipation within the KTln range (2).

K is the normal Boltzmam, and T is the temperature on the Kelvin scale. The panels created with Bennett's help suggested that this heat dissipation could be eliminated if conventional irreversible systems were converted to reversible systems [3]. Reverse computation is the process in which there are no missing records; therefore, a small amount of heat is better dispersed. This means that there can be no less than the system's entropy. Encryption is one of the most important elements in statistics and communications because communication occurs through untrusted means, as records can be easily compromised. An ineffective encoder requires a great deal of security, but it also requires low power consumption. Implementing an encoder using common sense inverse gates provides a good solution. This document provides a reverse logic gate cipher (RLGCD) design. The biggest motivation for reversible technology in cryptography is that it offers a much higher strength yield than other traditional structures, and this type of crypto machine is useful for exceptional software, including clinical, banking, government, and many more. The encryption key is generated using LFSR [4]. The overall FPGA performance of the RLGCD texture is higher than existing strategies. Information privacy can be

ISSN: 2366-1313

very important nowadays because hackers are everywhere. A watermark is made to improve security using LSB technology on the input image. Watermarking is the technique by which the pattern is embedded in unique stats, and this sample is a hidden statistic that helps in fact-checking. Those imperceptible facts that are embedded are known as a watermark.

II. CRYPTOLOGY

Cryptography is a process that uses a certain set of codes to improve privacy and provide secure communication. Modern cryptography uses specific algorithms and security keys to encrypt and decrypt data. Encryption is the process of translating data into unexpected symbols. An authenticated key is critical to access encrypted data.

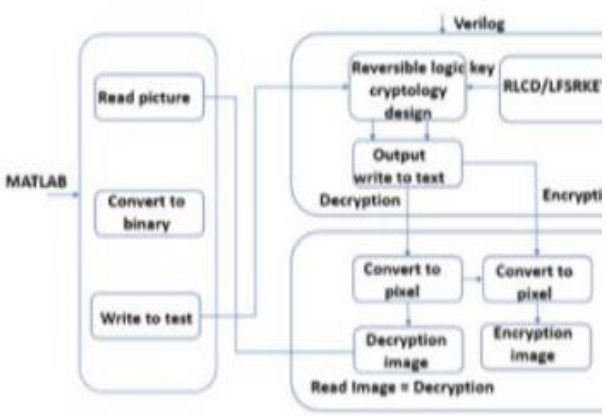

Fig.1 Image Cryptology using Reversible Logic Gates

There are two types of encryption techniques, symmetric and asymmetric, to protect sensitive electronic data such as email, folders, files, and entire drives. The retrieval system of the original facts of encryption with an authenticated key and a few operations is known as decryption. The data can be encrypted with specific private keys so that the intruder cannot interpret the records to protect statistics from hackers. Algorithms and keys are designed so that only decrypted users are allowed to encrypt and decrypt the data.

III. PROPOSED METHODOLOGY

The encryption and decryption process of Image cryptology using reversible logic gates is shown in figure 1. An Image is converted into a binary pixel format which is an acceptable in Xilinx Vivado Tool using MATLAB. HDL is used to read binary pixel values and apply reversible logic with random key generated by RLFSR for data encryption. To decrypt the original

ISSN: 2366-1313

image an irreversible logic with random key is applied on received cipher a new binary pixel values are generated. MATLABplays a crucial role in converting binary pixel values to original image vice-versa.

Reversible logic gates

Reversible logic gates should fall the below two conditions. No of inputs and outputs should be same. The pattern of input and output should be unique. Let input be 101 is applied to the reversible logic gate, and then it gives the output as 010. If the output is the same as input, then it represents the existence of reversible logic operation in the system. HING, PERES, CNOT reversible gates plays a crucial role to design the encryption and decryption.

RPGs are circuits with an identical number of inputs and outputs with at least one unique assignment relationship. Therefore, it is quite possible to retrieve the input pattern from the output pattern, so there is no data loss during the computation. For example, permission 110 is the sample provided as input to the RLG. Then after the wise operation, it produces 001 as the output. If we look at this 001 as the input and get one hundred and ten as the output, it represents the occurrence of a reverse process. Similar to traditional harmonic common-sense circuits, there can be a dissipation of the same thermal power for every small bit of data lost during operation. This reasoning is in line with the second rule of thermodynamics; there may be no way to reproduce data once it is lost. Therefore, when the calculation ends in reverse, it is possible to obtain a logical dissipation of electricity. That is, there is no shortage of device entropy. RLG's design limitations include

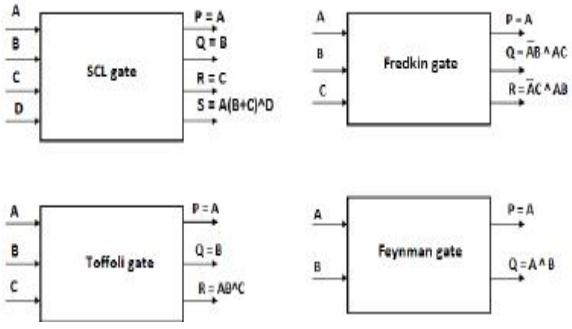

Fig.2 Block diagram for RLG

Fig.2 presents the block diagram of the overall cryptography process. The

ISSN: 2366-1313

working principle of the proposed RLGCD is described below.

Step 1: MATLAB is used to read the input image and on this image watermarking is performed.

Step 2: The LSB watermarking is used and after watermarking process the watermarked input image is converted into binary image.

Step 3: The binary image pixel values will be written into a text file with in the MATLAB.

Step 4: In order to perform the cryptography processes a key is required. This key is created using the LFSR.

Step 5: The input to Verilog code is the text file output from MATLAB and in Verilog the cryptography processes such as encryption and decryption are performed.

Step 6: Then, both the encryption output and decryption output are copied in to text files in Verilog for output verification.

Step 7: In MATLAB the pixels are reconstructed from the encrypted binary pixel values and decrypted binary pixel values in the text file. The encrypted and decrypted images are then generated from these pixel values.

Step 8: Then, input image and decrypted image will be the same.

Step 9: The watermark is extracted back from the decrypted image.

Step 10: FPGA performances are evaluated using the Verilog code

CNOT Gate

Figure 3: CNOT Gate

The logic for the CNOT gate, if the input is A then output will be P=A. If another input is B, then the output will be Q=A^B.

HING Gate

The HING gate is shown in figure 3 is a 4*4 reversible logic gate where A, B, C, D are inputs and P, Q, R, S are outputs. The logic for the HING gate, if A is given as input, then the output P will be A itself Similar to B. The output of R

ISSN: 2366-1313

will be A^B^C. The final output of S=(A^B) &(C^A) &(B^D)

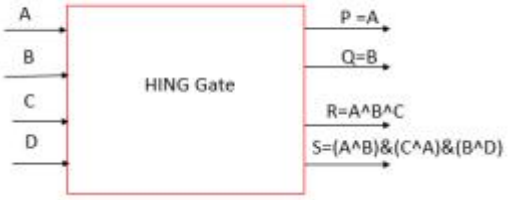

Figure 4: HING Gate

IV. SIMULATION RESULTS

The simulation results of ICRLG encryption and decryption process are shown below

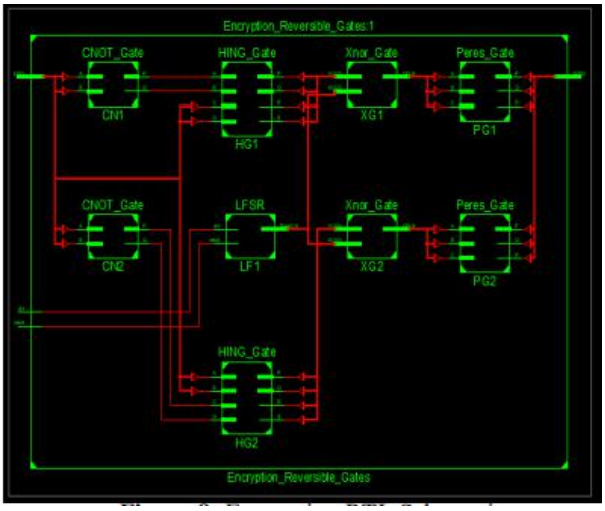

Fig.5 Encryption RTL Schematic

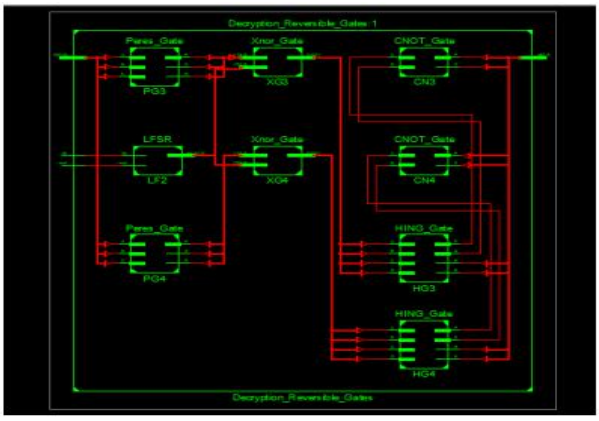

Fig.6 Decryption RTL Schematic

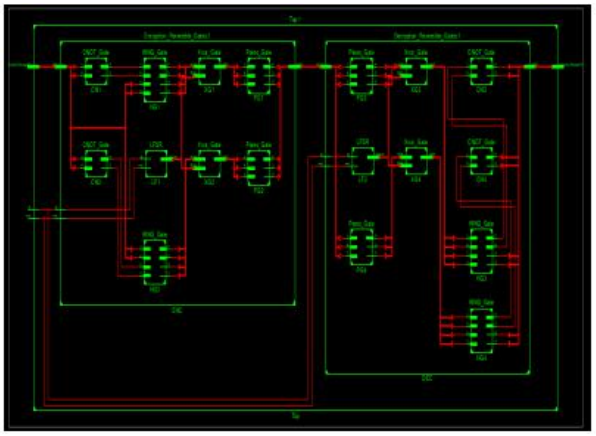

Fig.7 Encryption and Decryption RTL Schematic

Fig.8 Encrypted and Decryption Plain Text

V. CONCLUSION

This work presents a Reversible Logic Gate Cryptography. Design using LFSR key with watermark. Inverse gates such as Feynman, Fredkin, Toffoli, and SCL gates are used in the design of this new encoder. Since the encryption system does not need high protection but low power consumption, this

ISSN: 2366-1313

system is one of the best. The image input, the watermark, and the conversion to a binary layout operation are read in MATLAB, and these binary values are written directly into a textual content file. The entered pixel values are taught using Xilinx ISE. The RLGCD architecture, including LFSR, cipher block, and decoder block, is implemented in Xilinx software. This structure is suitable for both grayscale and color images. Watermarking was completed to use LSB technology to improve information security. The Xilinx performance score for the Spartan3E XC3S500E provides a much higher overall performance than other current frameworks.

REFERENCES

1. Mehaboob Mujawar, D. Vijaya Saradhi, 2022, "Design of Low-Cost Active Noise Cancelling (ANC) Circuit Using Ki-CAD", Innovations in Electronics and Communication Engineering. Springer DOI: 10.1007/978-981-16-8512-5_13, pp. 109–116.
2. MehaboobMujawar, D. Vijaya Saradhi, "Design and performance comparison of arrays of circular, square and hexagonal meta-material structures for wearable applications" Journal of Magnetism and Magnetic Materials,
3. D. Vijaya Saradhi, Swetha Katragadda, Hima Bindu Valiveti , 2021,"Hybrid filter detection network model for secondary user transmission in cognitive radio networks" International Journal of Intelligent Unmanned Systems, ISSN: 2049-6427.
4. Chandana Muppalla, Shaik Khader Zelani, D. Vijaya Saradhi, 2021, "Implementation of Digital Micro Fluidic Biochip with Machine Learning for Drug Development" Efflatounia, Pages:457-462.
5. Swetha K., P.V.Y. Jayasree, Vijay Saradhi, 2021, "Orthogonal mode dual band MIMO antenna system for 5G Smartphone applications using characteristic mode analysis" Circuit World, ISSN 0305-6120.
6. Mehaboob Mujawar, D. Vijaya Saradhi, S. Lenin Desai, M. Venkateswararao, 2021, "Performance Analysis of Dipole and Bow-Tie Antenna for Underwater Communication Using FEKO" IEEE 2021 Emerging Trends in Industry 4.0 (ETI 4.0).
7. Prasadu Peddi (2021), "Deeper Image Segmentation using Lloyd's Algorithm",

ISSN: 2366-1313, Vol 5, issue 2, pp:22-34.

8. Rolf Landauer, Irreversible and heat generation in the computing process, IBM Research and Development, vol.5, pp.183–191, July 1961.
9. C.H. Bennett, "Logical reversibility of computation" IBM Research and Development, vol.17, pp.525–532, 1973.
10. Saranya Karunamurthi, Vineyakumar Krishnasamy Natarajan, "VLSI implementation of reversible logic gates cryptography with LFSR key," Microprocessors and Microsystems, Elsevier, vol. 69, pp.68–78, September 2019.
11. Prasadu Peddi (2019), Data Pull out and facts unearthing in biological Databases, International Journal of Techno-Engineering, Vol. 11, issue 1, pp: 25-32.