IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 10, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.122

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15662/IJAREEIE.2021.1005014

Design and Implementation of 256-bits Hybrid Data Security Algorithm Written in VHDL Code with Data Integrity Test

Paresh Kumar Pasayat[1], Ayan Lodh[2], Madhusmita Das[3]

B Manoranjan Patra[4], Barsha Baisakhi Priyadarshini[5], Ashis Kumar Samal[6], Monalisha Sethi[7]

Assistant professor, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[1]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[2]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[3]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[4]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[5]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[6]

B.Tech. Student, Dept. of Electronics & Telecommunication Engineering, I.G.I.T., Odisha, India[7]

ABSTRACT: The proposed paper aims to create a virtual model for a newly developed hybrid data security algorithm which is implemented using the modified version of the Data Encryption Standard (DES), Transposition cipher and Hamming (448,256) code techniques with message integrity test. The proposed work deals with the generation of 256-bit digital data using 256-bits data generation uit and encryption of 256 -bits digital data using various data security techniques. The 256-bits data is encrypted using 224-bits cipher key to produce 256-bits middletext and this 256-bits middletext is given to the transposition cipher to produce 256-bits data. The output of transposition cipher is given to the Hamming (448,256) code encryption block to generate 448-bits encrypted data. The 256-bits original data has been recovered by using the reverse order operations with respect to the encryption process. As the hybrid data security algorithms have been used with various security features, the proposed data security algorithm is resistant towards the brute-force attack, timing attack and Statistical attack respectively. In order to check the integrity of the data, the message digests are created at the transmitter and receiver ends and both the message digests are compared. If both the message digests are same, then the integrity of the data is preserved and if both are different, then the integrity of the data is lost. The proposed work can be implemented in the banking sector, telecommunication sector and military sector etc.

KEYWORDS: Data Encryption Standard (DES), Transposition Cipher, Hamming (448,256) code, Brute-force attack, Message digests, Integrity.

I.INTRODUCTION

Cryptography is the process of hiding the content of the message by the process of encryption with or without the use of chip code. In this technique, the original message is converted into a message of unreadable format so that the attacker cannot access the original message easily. In the proposed work, the 256-bit data is generated using a data generation unit and this 256-bit data is converted into 448-bits encoded data using 256-DES, Tranposition cipher and Hamming (448,256) code encryption techniques at the transmitter end. In order to recover the original data at the receiver end, the reverse operations are performed with respect to the algorithm used in the encryption process. The proposed algorithm is different from the existing algorithm in terms of number of data bits and design styles with logic in addition to the achievement of robustness and newness of the algorithm. The main goals of Cryptography are data confidentiality, data integrity and data availability.

II.PROJECT MODEL

The project model describes the flow chart for the proposed project work. The diagrammatic representation of the proposed work is given as follows:

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15662/IJAREEIE.2021.1005014

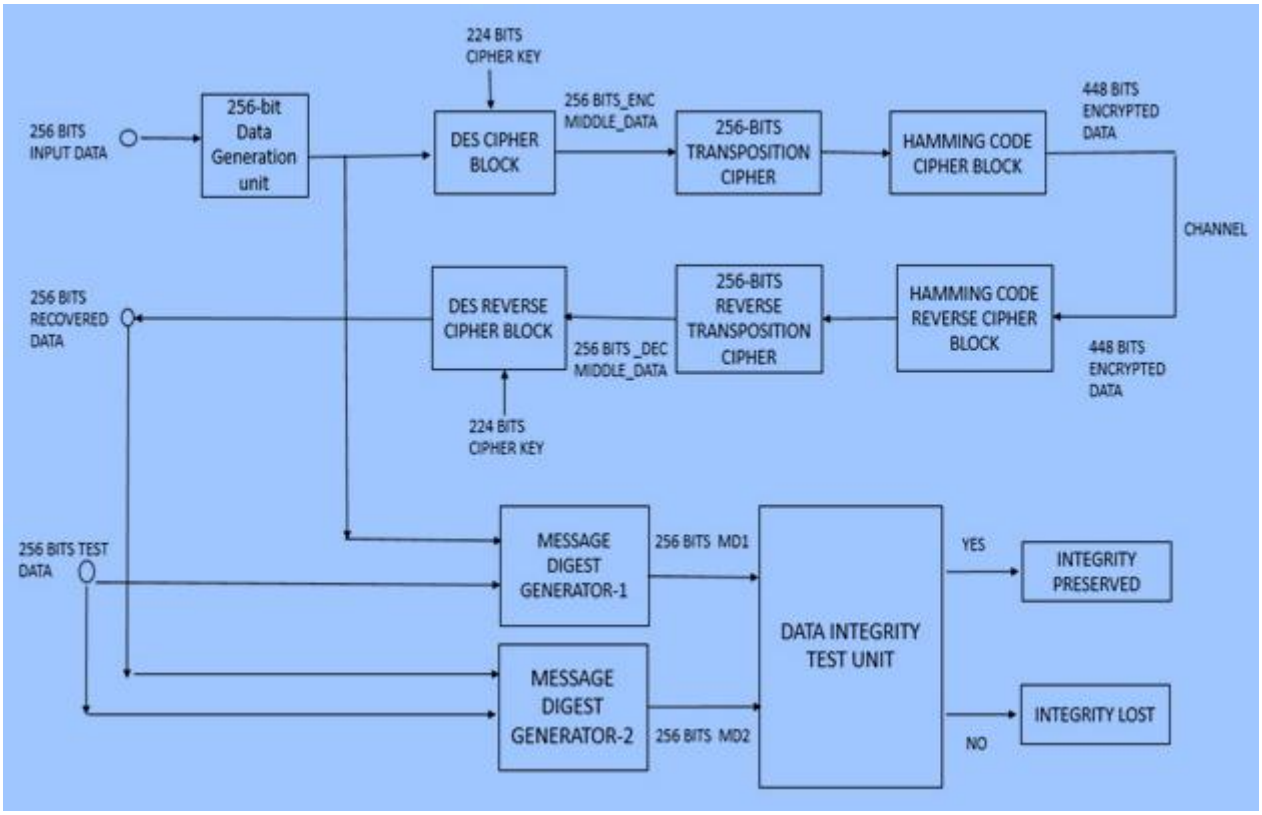


Fig 1: Block diagram of the proposed design

III. ALGORITHM OF THE PROPOSED DESIGN

Step 1: At the Tranmitter end, the 256-bit Digital data to be encrypted is generated using a 256-bit Data Generation Unit.

Step 2: This 256-bits digital data is given to the modified DES cipher block which generates 256-bits middle encrypted data1.

Step 3: The middle 256-bits encrypted data1 is given to the input of Transposition Cipher block which generates 256-bits middle encrypted data2.

Step 4: The 256-bits middle encrypted data2 is given to the input of Hamming code encryption block which generates 448-bits actual encrypted data.

Step 5: The 448-bits actual encrypted data is transmitted towards the receiver end through the wireless channel.

Step 6: At the Receiver end, the receiver receives 448-bits encrypted data and detects the bit error (if any) in the data and corrects the error in data bits (if any).

Step 7: The corrected 448-bits encrypted data is passed through the Hamming code decryption block which produces 256-bits middle decrypted data3.

Step 8: The 256-bits middle decrypted data3 is passed through the Transposition Decipher block which produces 256-bits middle decrypted data4.

Step 9: The 256-bits middle decrypted data4 is given to the input of the DES Reverse cipher block which produces the 256-bit recovered data and this data is the exact replica of the original 256-bits input data transmitted at the transmitter end.

Step 10: In order to check the integrity of the data, two message digests such as MD1 & MD2 are created both at the transmitter and the receiver ends.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15662/IJAREEIE.2021.1005014

Step 11: The two message digests are given as the inputs of the data integrity test unit and if MD1 is equal to MD2, the integrity of the data is preserved and if MD1 is not equal to MD2, then the integrity of the data is lost.

IV. SIMULATION RESULTS AND DISCUSSION

The VHDL code of the proposed design is written and simulated using Xilinx ISE 9.2i software and the desired simulation results have been obtained. The simulation results of the proposed work is given as follows:

SIMULATION RESULT OF THE 256-BIT DATA GENERATION UNIT:
FOR MEMORY CHIP ENABLE = '1'

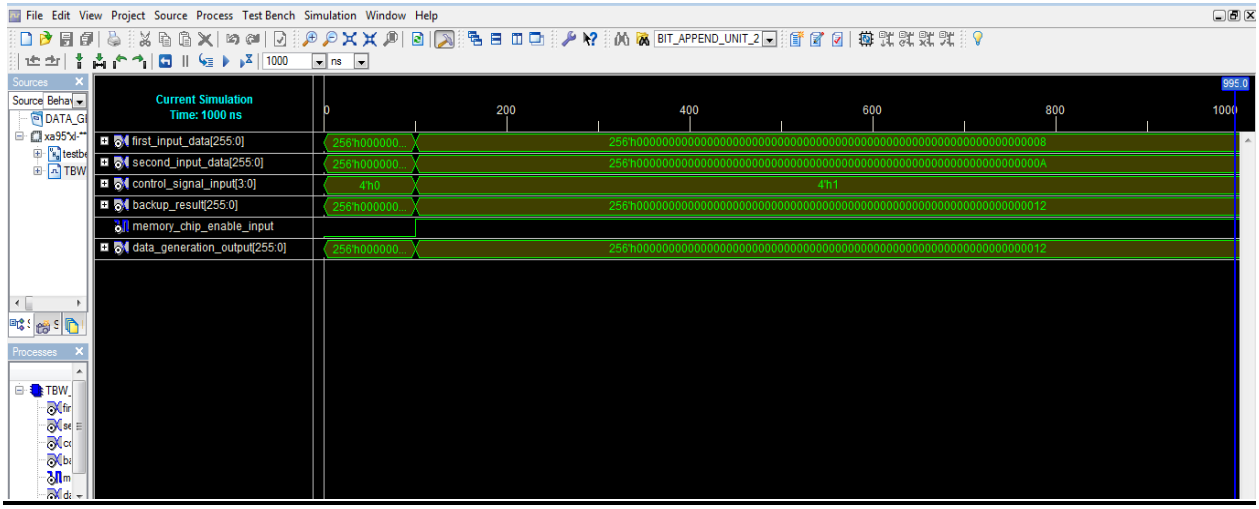


Fig 2: Simulation result of the 256-Bit Data Generation Unit for Memory Chip Enable = '1'

DATA_GEN_INPUT_1: 0000000000000000000000000000000000000000000000000000000000000008
DATA_GEN_INPUT _2: 000000000000000000000000000000000000000000000000000000000000000A
CONTROL_INPUT: 1
MEMEORY_CHIP_ENABLE: 1
BACKUP_RESULT_OUTPUT: 0000000000000000000000000000000000000000000000000000000000000012
DATA_GEN_OUTPUT: 0000000000000000000000000000000000000000000000000000000000000012

FOR MEMORY CHIP ENABLE = '0'

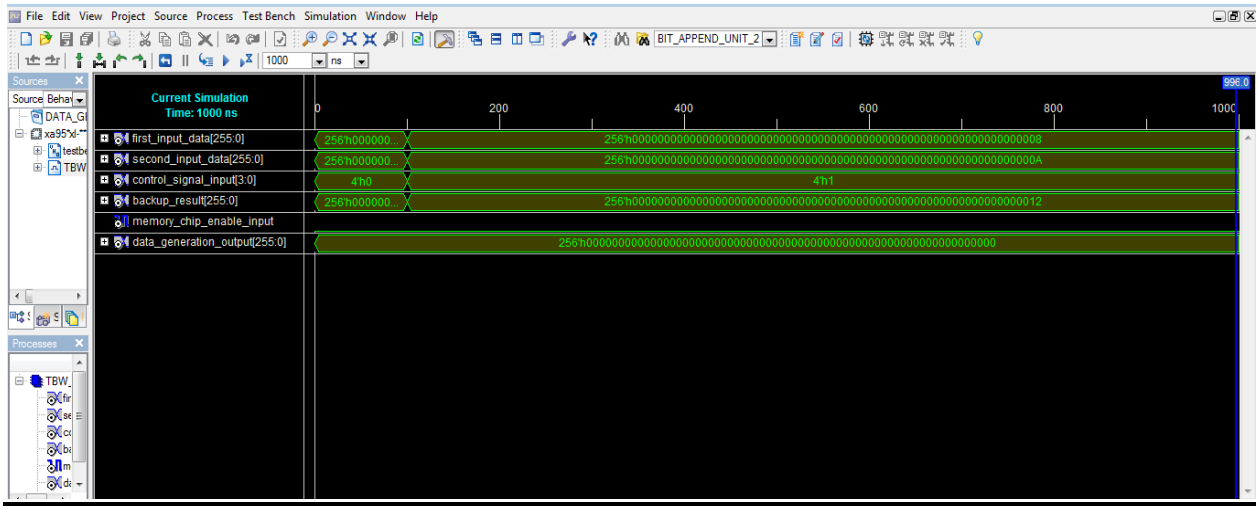


Fig 3: Simulation result of the 256-Bit Data Generation Unit for Memory Chip Enable = '0'

DATA_GEN_INPUT_1: 0000000000000000000000000000000000000000000000000000000000000008

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15662/IJAREEIE.2021.1005014

DATA_GEN_INPUT _2: 0000000000000000000000000000000000000000000000000000000000000000A
CONTROL_INPUT: 1
MEMEORY_CHIP_ENABLE: 0
BACKUP_RESULT_OUTPUT: 0000000000000000000000000000000000000000000000000000000000000012
DATA_GEN_OUTPUT: 0000000000000000000000000000000000000000000000000000000000000000

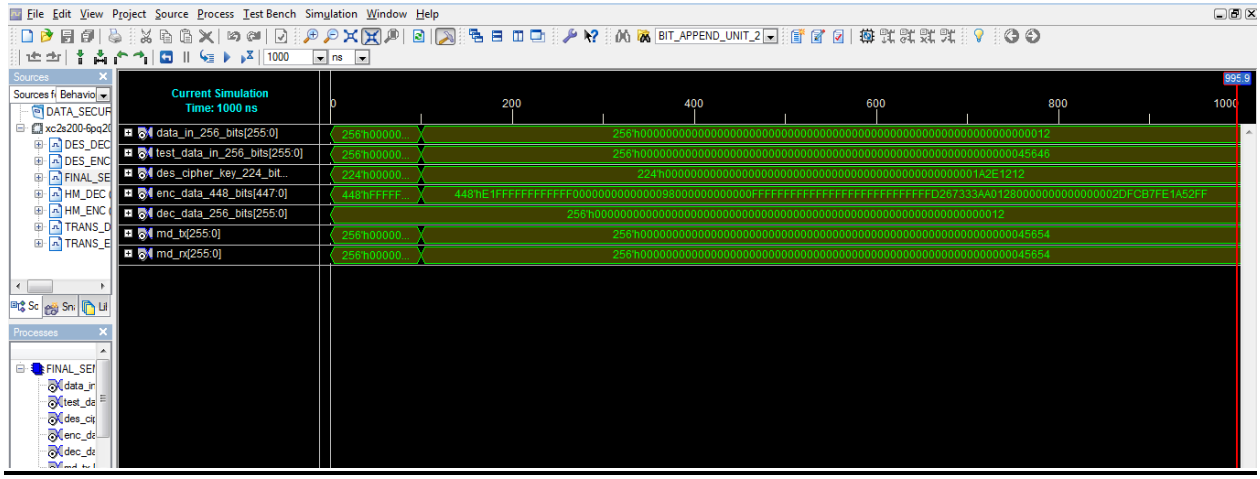


Fig 4: Simulation result of the Data Security Unit (Encryption and Decryption Processes) with Data Integrity Test

DATA_INPUT: 0000000000000000000000000000000000000000000000000000000000000012
CIPHER_KEY_INPUT: 00000000000000000000000000000000000000000000001A2E1212
TEST_DATA_INPUT: 0000000000000000000000000000000000000000000000000000000000045646
ENCRYPTED_DATA_OUTPUT:
E1FFFFFFFFFFFF000000000000009800000000000FFFFFFFFFFFFFFFFFFFFFFFFFFFD267333AA0128000000
0000000002DFCB7FE1A52FF
DECRYPTED_DATA_OUTPUT: 0000000000000000000000000000000000000000000000000000000000000012
MESSAGE_DEGEST_TX_OUTPUT: 0000000000000000000000000000000000000000000000000000000000045654
MESSAGE_DEGEST_RX_OUTPUT:0000000000000000000000000000000000000000000000000000000000045654

V.CONCLUSION

It is concluded that the proposed work is best suited in the field of data security to provide protection to the 256-bits digital data from unauthorized access by using newly developed hybrid data security algorithms. It is resistant towards the brute-force attack, timing attack and Statistical attack which makes the algorithm more robust. The VHDL code of the proposed design is compiled, synthesized and simulated using Xilinx ISE 9.2i software. The maximum combinational path delay required to convert 256-bits original data into 448-bits encrypted data is 6.556 ns.

REFERENCES

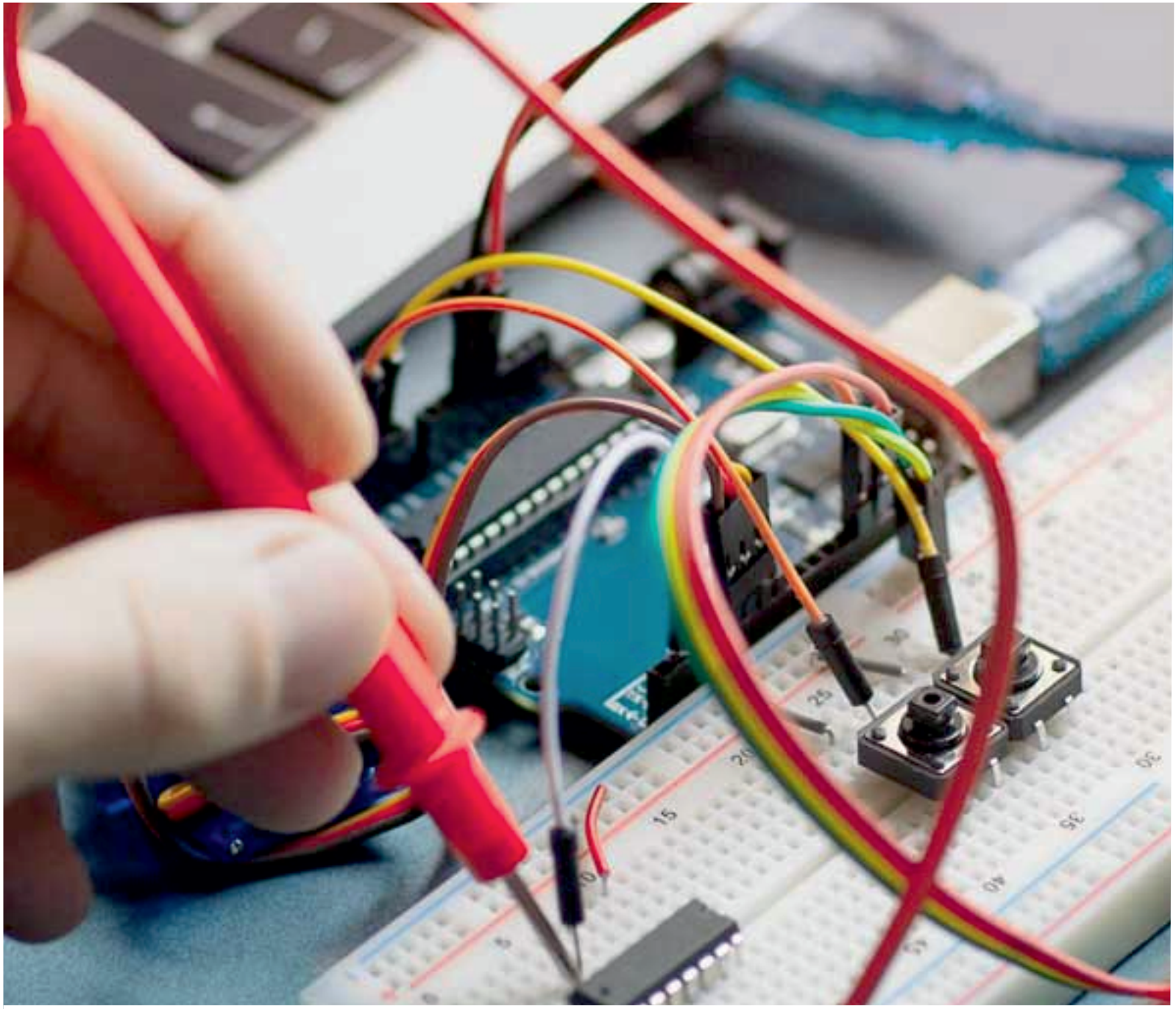
[1] F. E. Potestad-Ordóñez, E. Tena-Sánchez, R. Chaves,M. Valencia-Barrero, A. J. Acosta-Jiménez, “Hamming-Code Based Fault Detection Design Methodology for Block Ciphers” IEEE,2020.
[2] Karthikeyan B, Asha S, Poojasree B, “Gray Code Based Data Hiding in an Image using LSB Embedding Technique ” IJRTE,VOL.8, 2019.
[3] Deena Nath Gupta, Rajendra Kumar, “Lightweight Cryptography: an IoT Perspective” IJITEE, VOL.8, 2019.
[4] Abdalbasit Mohammed Qadir, Nurhayat Varol, “A Review Paper on Cryptography”, IEEE, 2019.
[5] Caleb Hiller, Vipin Balyan, “Error Detection and Correction On-Board Nanosatellites Using Hamming Code”, Hindwai, 2019.
[6] AlpaAgath, Chintan Sidpara, “Critical analysis of cryptography and steganography”, JSRSET, VOL.4, 2018.
[7] Achmad Solichin, Erwin Wahyu Ramadhan, “Enhancing data security using DES-based cryptography and DCT-based steganography”, ICSITECH, 2017.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.122|

|| Volume 10, Issue 5, May 2021 ||

DOI:10.15662/IJAREEIE.2021.1005014

[8] Divya Mokara, Sushmi Naidu, Akash Kumar Gupta, "Design and Implementation of Hamming Code using VHDL & DSCH" International Journal of Latest Engineering Research and Applications(IJLERA),2017.
[9] Achmad Fauzi Nurhayati, Robbi Rahmin, "Bit Error Detection and Correction with Hamming CodeAlgorithm",IJSRET,2017.
[10] Dr. Sandeep Tayal, Dr. Nitin Gupta, Dr. Pankaj Gupta, Deepak Goyal, Monika Goyal, "A Review Paper on Network Security and Cryptography", Research India Publications, 2017.
[11] Deepika S S, Ashwin Kumar, Nisha, "A VHDL implementation of UART with Coding Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 2017.
[12] Abhishek Anand, Abhishek Raj, Rashi Kohli, "Proposed symmetric key cryptography algorithm for data security" IEEE, ICICCS, 2016.
[13] CemSahin, Brandon Katz, Kapil R. Dandekar ,"Secure and Robust symmetric key generation using physical layer techniques under various wireless environment", IEEE, 2016.
[14] Nabil Schear, "Cryptography for Big Data Security", Big Data, 2016.
[15] Adham Hadi Saleh, "Design of Hamming Encoder and Decoder Circuits For(64,7) Code and (128,8) Code using VHDL", Journal of Scientific and Engineering Research, 2015.
[16] Leena, Mr.Subham Gandhi, Mr, JItendra Khurana, "Implementing (7,4) Hamming Code Encoding and Decoding System Using CPLD", International Journal of Engineering Research and Technology(IJERT),2013.
[17] Brajesh Kumar Gupta, Rashmi Sinha, "Novel Hamming Code for correction and detection of higher data bits using VHDL", IJSER,VOL.4,2013.
[18] W. Stallings, "Cryptography and Network Security", Prentice hall, 2011.
[19] Douglas L. Perry "VHDL Programming by Examples", TMH, 2010.



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.122

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details