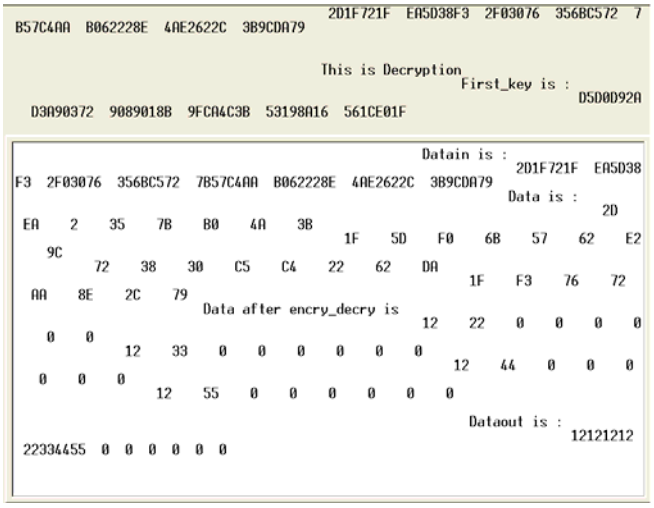

(b)

Figure 5.3: (a) encryption results and **(b)** decryption results

5. Conclusion

We have successfully implemented the AES encryption and decryption algorithm in the FPGA as shown from the results in figure 5.3 (a) and (b). The system C code was developed for the implementation of the encryption and decryption process. The microblaze processor uses a 5-stage pipeline which gives a high speed implementation of the AES algorithm. The synthesis report shows that space consumption is low, this permits the implementation of this method over inexpensive FPGAs.

6. Future Scope

I propose that this work be used as part of larger projects, including protecting sensitive data in the military and in the banks. This system can also be adopted in data terminal equipment with less demand on throughput.

References

[1] FIPS FIPS-197, Federal Information Processing Standards Publication FIPS-197,Advanced Encryption Standard(AES),http://csrc.nist.gov/publications/fips/fips 197/fips-197.pdf, 1999.
[2] Daemen, J. and Rijmen, V., The design of Rijndael: AES — The Advanced Encryption Standard. Springer-Verlag, 2002.
[3] SCHNEIER, B., Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, Inc. 2nd Ed, 1996.
[4] William Stallings, Cryptography and Network Security, Principles and Practices, 4th ed. Pearson Education, pp. 134-161, 2006
[5] [5] Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Private Communication in a Public World, 2nd ed. Pearson Education, pp. 41-114, 2006
[6] *on Circuits and Systems(LASCAS-2011),* February 201[6] Gomes, O. S. M.; Pimenta, T. C.; Moreno, R. l., "a highly efficient FPGA Implementation", *2nd Latin America Symposium* 1.
[7] Daemen, J. and Rijmen, V. A Specification for The AES Algorithm. NIST (National Institute of Standards and Technology).http://csrc.nist.gov/archive/aes/rijndael/wsd index.html, 2010.
[8] Ahmad, N.; Hasan, R.; Jubadi, W.M; "Design of AES S-Box using combinational logic optimization", IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.
[9] J. V. Dyken and J. G. Delgado-Frias, "FPGA schemes for minimizing the power-throughput trade-off in executing the Advanced Encryption Standard algorithm" School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164-2752, USA, Available online 16 December 2009 .
[10] K. Joarvinen, "Study on high-speed hardware implementation of cryptographic algorithms" Department of Signal processing and Acoustics, Helsinki of technology, 10 University Feb 2009.
[11] A. Hodjat and I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA", 12th IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM 2004), pages 308-309, IEEE Computer Society, 2005.
[12] Standaert et al, "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs. ches 2003, LNCS 2779, pp. 334-350, 2003.
[13] Saggese et al, "An FPGA-Based Performance Analysis of the Unrolling, Tiling, and Pipelining of the AES Algorithm", FPL 2003, LNCS 2778, pp. 292-302, 2003.
[14] Jarvinen et al, "A fully pipelined memory less 17.8 Gbps AES-128 encryptor", International Symposium on Field Programmable Gate Arrays, pp. 207-215. 2003.

Author Profile

Rudo Duri attained her B. Tech. Degree in ECE from the Harare Institute of Technology 2010, Zimbabwe. Currently she is studying towards M. Tech Digital Systems and Computer Electronics at JNTUH, India.. She is a Harare Institute of Technology staff development research fellow. Her research interests are in the area of Microcontroller Design, ADHoc and Wireless Sensor networks, VLSI Design, Advanced Data Communications, Real Time Operating Systems and Digital System Design.

Mrs.Thoomati Madhavi Kumari obtained B.Tech. in ECE and M.Tech. in Computer Science from JNT University. Presently Mrs. Madhavi is pursuing Ph.D. in Data security for natural languages using FPGA. Mrs. Madhavi joined the faculty of ECE Department of JNU College of Engineering, Kukatpally, Hyderabad as Assistant Professor and served the department for 13 years. Later she was appointed as Assistant Director, UGC-ASC, JNT University, and Hyderabad. She was associated with the implementation of AICTE sponsored project on computer networks.