RESEARCH ARTICLE OPEN ACCESS

Data Encryption and Decryption Algorithm Using Hamming Code and Arithmetic Operations

Kurapati Sundar Teja[1], Shanmukha Mallikarjuna Bandaru[2], Kurapati Pavan Teja[3], Fazal Noorbasha[4]
Department of ECE, K L University, Vaddeswaram, Guntur, AP, India-522502

ABSTRACT
This paper explains the implementation of data encryption and decryption algorithm using hamming code and arithmetic operations with the help of Verilog HDL. As the days are passing the old algorithms are not remained so strong cryptanalyst are familiar with them. Hamming code is one of forward error correcting code which has got many applications. In this paper hamming code algorithm was discussed and the implementation of it was done with arithmetic operations. For high security some arithmetic operations are added with hamming code process. A 3-bit data will be encrypted as 14-bit and using decryption process again we will receives 3-bit original data. The implemented design was tested on Spartan3A FPGA kit.
Keywords **–** Encryption, Decryption, Hamming Code, Arithmetic, Verilog HDL, FPGA.

I. INTRODUCTION

Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g., the Internet, e-Commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines [1].

The encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and EES (Escrowed Encryption Standard) are widely used to solve the problem of communication over an insecure channel [2]. First, the encryption and decryption procedures are much simpler, and consequently, much faster. Second, the security level is higher due to the inherent poly-alphabetic nature of the substitution mapping method used here, together with the translation and transposition operations performed in the algorithm [3].

In this paper, the encryption and decryption procedures are explained and the performance is compared with popular encryption algorithms. Recently, a reconfigurable FPGA design is efficient method to implement a digital logic, because FPGA provides a compromise between general-purpose processors and ASIC. The FPGA based design is also more flexible, programmable and can be re-programmed. FPGA based design can easily be modified by modifying design's software part [4]. Our proposed system is designed in FPGA design style and gate level modeling.

II. SYSTEM MODEL AND OPERATION

This encryption and decryption process is divided in to two parts. In first part the 3-bit data and key will be converted in to 4-bit data. For this we are using the arithmetic operation addition between 3-bit data and key. 3-bit key will be converted in to 4-bit key by performing ex-or operation between the key bits. In second step the 4-bit addition data and key data will be converted in to 7-bit data using the hamming code process. Finally these two 7-bit data will be clubbed to form a 14-bit data. This final encrypted 14-bit data will be transmitted. In this 14-bita 0 to 6 bits are key and 7 to 13 bits are data. Figure 1 shows the encryption process.

Figure 2 shows the decryption process. This system will receive total 14-bit encrypted data. First it will check the whether the received data is free of error or not. If there is not error in the data then next step will start. In first step total 14-bit data will be divided into two 7-bit data i.e. 7-bit information data and 7-bit key, by using hamming code technique we will get a 4-bit information data and 4-bit key. In second step 4-bit data will subtracted from 4-bit information data. Finally we will get a 3-bit original data. Figure 3 shows the FPGA RTL view.

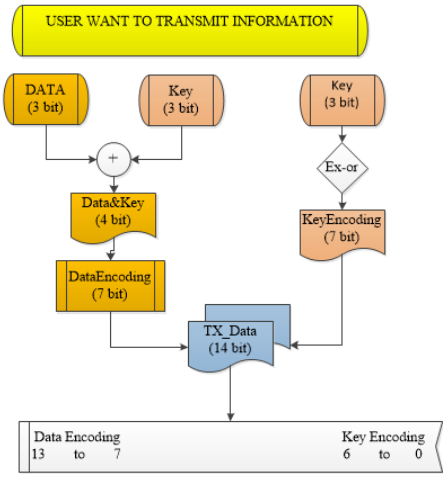

Figure 1: Data Encryption Process

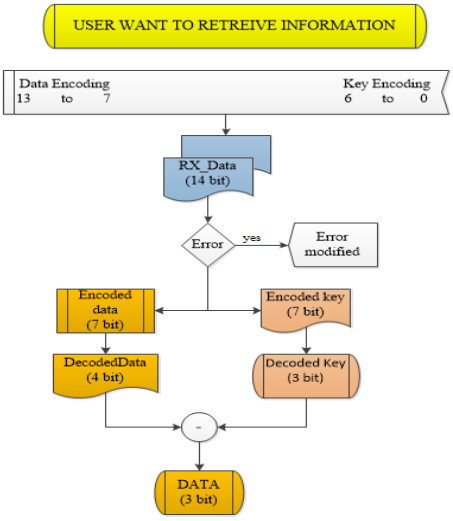

Figure 2: Data Decryption Process

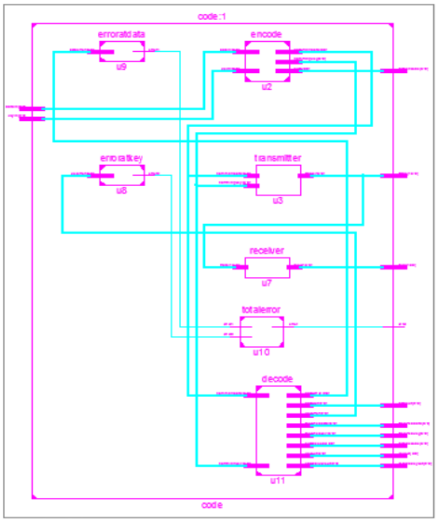

Figure 3: FPGA RTL View of Data Encryption and Decryption Process System

III. RESULTS

Figure 4 shows the Data Encryption and Decryption Process simulation results of No - error and Figure 5 shows Data Encryption and Decryption Process simulation results – Error. We have tested the results in Spartan3A FPGA kit.

Figure 4: Data Encryption and Decryption Process simulation results – NO Error

Figure 5: Data Encryption and Decryption Process simulation results – Error

IV. CONCLUSION

The present data encryption and decryption process is implemented using Verilog HDL with the help of Xilinx ISE Design Suite. The design is verified on Spartan 3A FPGA kit. FPGA increase productivity, reduces cost, and accelerates time to market. The designed system can be used for many applications and also security will be high.

REFERENCES

[1] Vinod Shokeen, Niranjan Yadav, "Encryption and Decryption Technique for Message Communication", International Journal of Electronics & Communication Technology, Vol. 2, Issue 2, June 2011, pp. 80-83.

[2] Obaida Mohammad Awad Al-Hazaimeh, "A New Approach For Complex Encrypting and Decrypting Data", International Journal Of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013, pp. 95-103.

[3] Prakash G L ,Dr. Manish Prateek and Dr. Inder Singh, "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science, Volume 3 Issue 4 April, 2014 Page No. 5215-5223