Vol 07, Article 05672; May 2016
http://ijves.com

International Journal of VLSI and Embedded Systems-IJVES
ISSN: 2249 – 6556

VHDL IMPLEMENTATION OF AN ENCRYPTED IMAGE TRANSMISSION SYSTEM

ADITHYA SABARISH S[1], KAUSHIK C A[2], PRADHEEP S[3], ARVIND P[4], PREMALATHA B[5]
[1,2,3,4]ECE Final year, Coimbatore Institute of Technology,Coimbatore-14
[5]Assistant Professor, Department of ECE, Coimbatore Institute of Technology,Coimbatore-14
[1]adithyasabarish94@gmail.com, [2] kaushikanguraj@gmail.com,
[3]pradheep444@gmail.com,[4]arvindprakash22@gmail.com, [5]premalathaece.cit@gmail.com

ABSTRACT

An image cannot be transmitted as such from one point to another as it would cause wastage in bandwidth and also prone to various security threats. In order to achieve maximum security and use optimal bandwidth usage, an efficient transmission system is used. The steps involved in the proposed system are image conversion, compression, encryption and decryption. Huffman based compression technique is applied to decrease file size. Pre-existing images or images captured using a camera can be given as input for the system. The compressed data is still prone to security hacks and other threats, to avoid that AES encryption is then performed on the compressed data. At the receiver side, the inverse of the operations done in the transmitter side are performed. The received data is decrypted and restored to its original state. The received image is exactly similar to that of the transmitted image as the process involves lossless compression of the data. The modelling of the above system is implemented using the Xilinx ModelSim software environment.

Keywords: *compression, encryption, decryption, VHDL*

1. INTRODUCTION

At present, security is a huge concern, in the confidential information transfer by means of wired and wireless media. The main objective of the project is to devise a secure, efficient and high speed system for long distance image transfer. Converting the image into binary data and performing compression and encryption operations on it at the bit level ensures efficiency of the system. Using an unallocated portion of the frequency spectrum ensures speed due to lack or presence of minimal traffic on the same bandwidth. Chip level implementation using an FPGA assures the above system at a much lower cost than using ASICs.The system consists of two sections, namely a transmitter and receiver section. The transmitter section converts the image into a compressed one and encrypted to obtain image in a secured form and then transmits the data after modulation. The receiver section involves blocks which help restore the image by means of demodulation, AES decryption and inverse Huffman Coding. Extremely high security due to the efficiency and reliability of the AES encryption standard can be achieved. Highly efficient transmission due to the Huffman compression technique is observed. Lossless image compression due to the Huffman compression technique is obtained. High speed and security due to the incorporation of efficient algorithms is done. It is cost efficient due to the implementation on an FPGA. It works on any image format and is scalable. Any form of data can be converted to binary and transmitted with appropriate implementations of upgrades. The main aim is to develop a high speed, efficient and secure long-range image transmission system using VHDL. This can be extended to any use where highly confidential image files are involved namely corporate, government and military applications. High security is required for transmitting images and videos for military application, thus we use AES encryption which is considered as one of the best encryption techniques present. Compression is a necessary evil, as high compression involves losses such that the original image cannot be regained. Compression affords optimal memory utilization at the cost of losses in the image recovery. But compression helps in removing redundant information. Huffman aims at providing a good compression ratio with minimal loss.

2. SYSTEM ARCHITECTURE

The image to be transmitted is captured by means of a camera or an uncompressed image is used. The image is then encoded into a binary file by means of a MATLAB program. The output of the program is stored as a text file containing the equivalent binary values of the pixel intensity values of the image. This text file is used and Huffman compression algorithm is incorporated on it in VHDL environment. Huffman encoding scheme is employed to encode the image and to assign binary symbols of varied lengths based on their probability of occurrence. These symbols and their lengths are obtained and a codebook is generated. Since varied symbol lengths are used it accounts for compression. The compressed binary data obtained is piled up in a new text file. The values in the file are accessed using file pointers and further security standard is appended using AES scheme and the result is again a text file containing compressed, encrypted data. The text file obtained as the output from encryption block is applied to decryption algorithm and decompression is also performed. The AES decryption is nothing but the exact reverse process of the encryption standard. Hence the data is decrypted and the output text file is given as input to next VHDL program which performs Huffman decompression algorithm

Vol 07, Article 05672; May 2016
http://ijves.com
International Journal of VLSI and Embedded Systems-IJVES
ISSN: 2249 – 6556

that uses the codebook previously generated. Finally the binary data obtained is plotted to corresponding pixels using image processing software. The complete system description of image processing is shown in Fig.2.1.

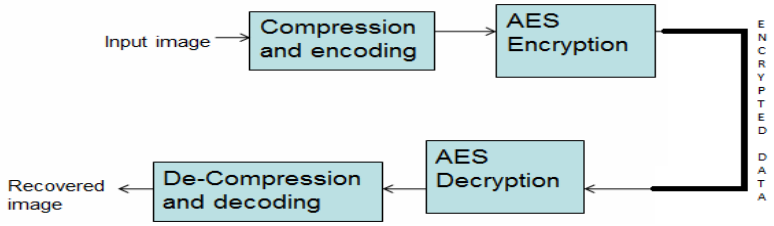

Fig. 2.1 System description

3. ALGORITHMS INCORPORATED

Huffman coding provides an efficient usage of bandwidth since word lengths for each symbol depends on the probability of occurrence of that particular pixel in the image. Huffman coding is used adaptively, accommodating unknown, changing, or context-dependent probabilities. Huffman coding is optimal when each input symbol is a known independent and identically distributed random variable having a probability that is an the inverse of a power of two.

3.1 Huffman algorithm

A Huffman code is obtained by constructing a Huffman tree. The path from the root to each leaf gives the code word for the binary string corresponding to the leaf. Huffman decoder uses a lookup table for retrieving the original or transmitted data from the encoder. This lookup table consists of all the unique words and their corresponding code vectors. Input is array of unique characters along with their frequency of occurrences and output is Huffman tree. Fig 3.1 explains the Huffman algorithm.

1. Create a leaf node for each unique character and build a min heap of all leaf nodes (Min Heap is used as a priority queue. The value of frequency field is used to compare two nodes in min heap. Initially, the least frequent character is at root).
2. Extract two nodes with the minimum frequency from the min heap.
3. Create a new internal node with frequency equal to the sum of the two nodes frequencies. Make the first extracted node as its left child and the other extracted node as its right child. Add this node to the min heap.
4. Repeat steps 2 and 3 until the heap contains only one node. The remaining node is the root node and the tree is complete.
5. Assign 0 and 1 for the final two existing nodes.
6. Follow the reverse traversal algorithm such that the word length increases by one bit when it finds a parent node.
7. Repeat the above till all symbols are assigned with a unique binary word such that each word has different word lengths based on their probabilities of occurrence.

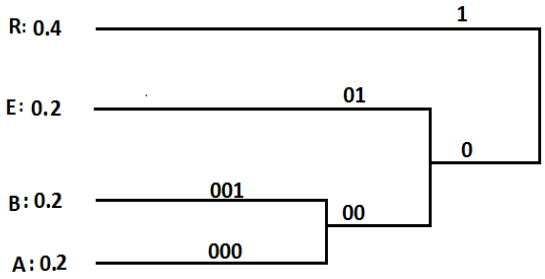

Fig.3.1 Huffman Algorithm

3.2 AES ENCRYPTION STANDARD

The Advanced Encryption System (AES), also known as Rijndael is a reliable encryption algorithm for the encryption of electronic data. The AES algorithm is a symmetrical block cipher that can encrypt (encipher), and decrypt, (decipher), information.AES is more secure (it is less susceptible to cryptanalysis than 3DES). It supports larger key sizes than 3DES's 112 or 168 bytes.AES is faster in both hardware and software. AES's 128-bit block size makes it less open to attacks via the birthday problem than 3DES with its 64-bit block size. The algorithm is required by the latest U.S. and international standards. The process of AES Encryption and decryption is as discussed in Fig. 3.2.

Vol 07, Article 05672; May 2016
http://ijves.com

International Journal of VLSI and Embedded Systems-IJVES
ISSN: 2249 – 6556

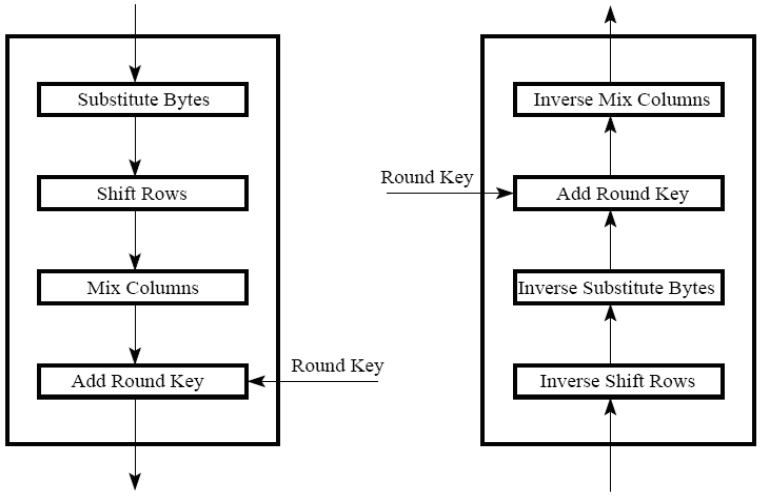

Fig.3.2 AES Algorithm

4. EXPERIMENTATION RESULTS

The experimental observation of the uncompressed image transmission involves the following steps: Uncompressed image is given as input. Huffman algorithm give text files as outputs. A text file stating codes assigned for all pixel symbols. A reference code book which will be used for decoding. A text file that contains the length values for each symbols. A text file containing binary values (assigned codes) for each pixel. The AES acts on these values so the data is encrypted. The reverse process (decryption and decoding) is done and the text files previously generated are used while decoding so as to obtain the original image.

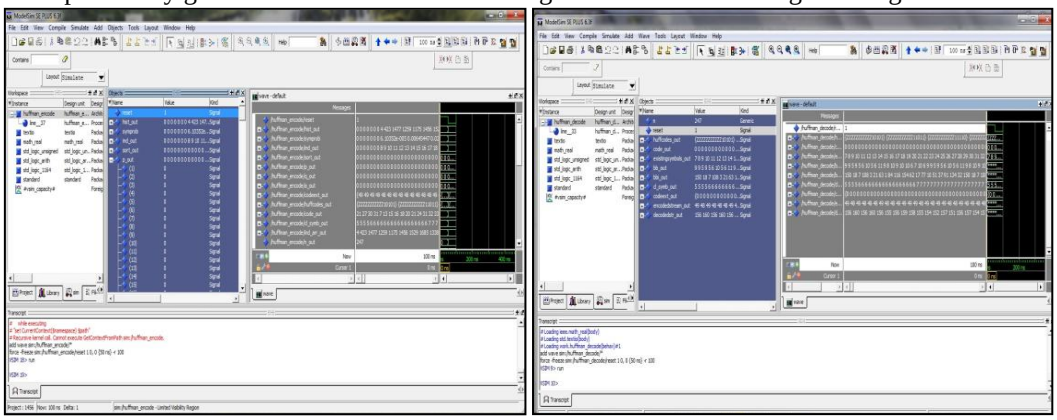

Fig. 4.1 Execution of Huffman Encoder and Decoder in VHDL Environment

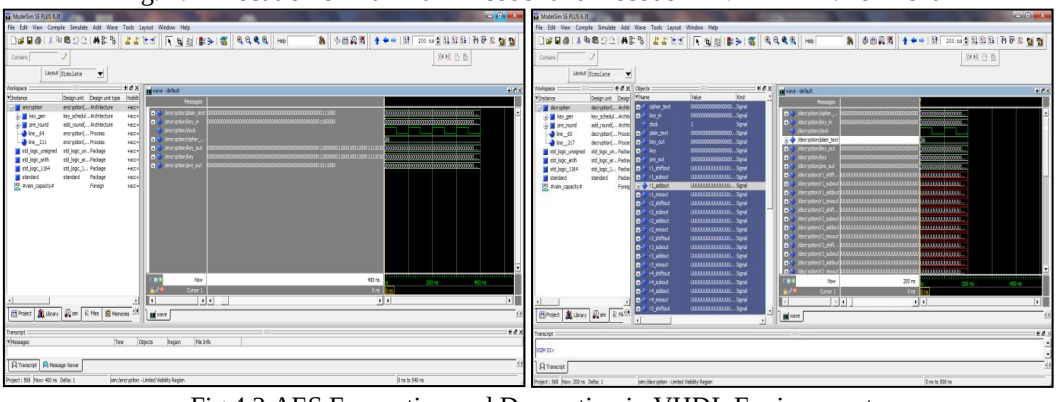

Fig.4.2 AES Encryption and Decryption in VHDL Environment

5. CONCLUSION

In any transmission system, bandwidth is considered as an important factor to establish an efficient communication. The compression is implemented using variable length Huffman Coding and the encryption technique used is 128 bit Advanced Encryption Standard. Implementation of a secured image transmission system is carried out and the results are noted.AES is extremely secure and has not been hacked as of now. It

Vol 07, Article 05672; May 2016
http://ijves.com
International Journal of VLSI and Embedded Systems-IJVES
ISSN: 2249 – 6556

takes 2^{128} attempts to crack using the brute force approach. Results are simulated using Xilinx ModelSim and the output waveforms help in verifying the results of encryption. A suitable modulation scheme combined with the project will make it a transmission-reception system completely dedicated for secured image transmission. This may find its application in several fields like military and government privacy information can be securely transmitted as an image with the allocation of separate bandwidth as per the choice and preference. As an upgrade for the project, efficient modulation schemes can be employed so as to design a complete image transmission system.

REFERENCES

[1] Ambika, Himanshu Yadav, Anurag Jain, "A Review: Image Encryption Techniques and its Terminologies", International Journal of Engineering and Advanced Technology (IJEAT), Vol.3, Issue 4, 2014.
[2] Amol Ananda Gore, V.V.Deotare, "FPGA Implementation of Area Optimized AES for Image Encryption/Decryption Process", International Journal of next generation computer applications, Vol. 4, pp.74-90, 2010.
[3] Babu, K.A. Kumar , "Implementation of data compression using Huffman coding", Methods and Models in Computer Science (ICM2CS), International Conference on Next Generation Computing Technologies (NGCT), Vol.7, pp.58-76, 2013.
[4] Dalakoti,N., Gaur,N. Mehra, "Hardware efficient AES for image processing with high throughput", 1st International conference on Next Generation Computing Technologies (NGCT), Vol.6, pp.94-120, 2015.
[5] Deshpande, H.S.; Karande, K.J. Mulani, "Efficient implementation of AES algorithm on FPGA", International Conference on Communications and Signal Processing (ICCSP), Vol.5, pp.79-102, 2014.
[6] Hashemian.R, "Memory efficient and high-speed search Huffman coding", IEEE Transactions on Communications. (43) ,2576- 2581, 1995.
[7] Hodjat, A., Verbauwhede , "A 21.54 Gbits/s fully pipelined AES processor on FPGA", IEEE International Symposium on Proceedings. Field-Programmable Custom Computing Machines, pp. 308–309, 2004.
[8] Huffman.D.A , "A Method for the Construction of Minimum-Redundancy Codes", Proceedings of the Institute of Radio Engineers, pp1098–1102, 1952.
[9] Hussain.U., Jamal.H., "An efficient high throughput FPGA implementation of AES for multi-gigabit protocols", Proceedings of International Conferences, Frontiers of Information Technology, pp. 215–218, 2012.
[10] Javed.M.Y and A. Nadeem , "Data compression through adaptive Huffman coding scheme", In Proceedings of TENCON, Vol.2, pp.187-190, 2000.
[11] Kawahara, M., "High-speed software implementation of Huffman coding", Data Compression Conference, 1998.
[12] Liu.Q., Xu.Z., Yuan "A 66.1 Gbps single-pipeline AES on FPGA", Proceedings of International Conferences, Field-Programmable Technology, pp. 378–381, 2013.
[13] MacKay, D.J.C , "Information Theory, Inference, and Learning Algorithms", Cambridge University Press, 2003.
[14] MamtaSharma,S.L. Bawa , "Compression using Huffman Coding", International Journal of Computer Science and Network Security (IJCSNS), Vol.10, No.5., 2010.
[15] Nagdeve, S.H. Ghodeswar, "U.S. Synthesis of Advanced Encryption Standards using Xilinx 13.4", Communications and Signal Processing (ICCSP), International Conference of security technology, Vol.2, pp.114-128,2015.