DESIGN AND VLSI IMPLEMENTATION OF MODIFIED AES WITH NEURAL NETWORKS FOR IMAGE CODING

Kanakatte A. Dattathreya
Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Hosur - 635109, Tamil Nadu, INDIA
kadatta2002@gmail.com

ABSTRACT
This paper is an attempt to address the security issue while transmitting the images over channel in an unprotected environment. Artificial neural networks have been used for image compression and AES is used for data encryption of compressed images. The feed forward network adopted compression of image up to a 97% and thus reducing the complexity in AES encryption. The compressor and encryption is modeled using HDL and synthesized using Xilinx ISE targeting Virtex2 and Virtex5 FPGA. The design consumes 9% of the slices and 1.128 W of power. The developed design is reconfigurable and hence used for real time applications.

KEY WORDS
Information security, encryption, decryption, FPGA, VLSI Design, image compression.

1. INTRODUCTION
The present scenario is that, the usage of autonomous vehicles such as UAV (unmanned aerial vehicle), Robots or unmanned military vehicles are growing especially in applications such as manufacturing, hazardous materials handling, surveillance, etc. The basic task in any such application is the perception of the environment through one or more sensors. Processing of the sensor input results in a particular representation of the unknown environment, which can then be used for navigating and controlling the vehicle. The general sensors used for autonomous vehicles include infra-red, sonar, laser, radar and so on [1]. For example, patent [2] discusses a navigation and control system including an emitter sensor configured to locate objects in a predetermined field of view from a vehicle and describe the techniques which make use of characteristics of infrared sensitive video data, in which heat emitting objects appear as hot spots. Compared to these types of sensors, vision sensors provide a whole new way for autonomous vehicles to create an image of the environment.

For the finding of better navigation these images will transmitted to the service base stations, for the military application these images should be transmitted very safely with high security algorithm for the captured image, which that no third person should not get what that image contained. Even from the captured images of UAV are high in memory; these images should not transmit easily, so the memory of the image should be reduced, those images required a good and better compression technique to reduce the memory of the image without altering the image content.

Image compression is a key technology in the development of various multimedia computer services and telecommunication applications such as teleconferencing; digital broadcast codec and video technology, etc. At present, the main core of image compression technology consists of three important Processing stages; pixel transforms quantization and entropy coding. In addition to these key techniques, new ideas are constantly appearing across different disciplines and new research fronts.

As image needs a huge amount of data to store it, there is pressing need to limit image data volume for fast transport along communication links. The goal of image compression techniques is to remove redundancy present in data in a way that enables image reconstruction. Statistical properties of the image are used in design an appropriate compression technique. The strong correlation between image data items enables reduction in the data contents without significant quality degradation. The Neural Networks (NN) has been used for solving many problems in image compression, in cases where the results are very difficult to achieve by traditional analytical methods. Possibly in the future this could have a great impact to the development of new technologies and algorithms in this area.

Encryption is a common technique to uphold image security. Image encryption has applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Here using AES (Advanced Encryption Standard) to protect the confidential image data from unauthorized access after compression from the Neural Networks.

1.1 Literature Survey
In paper [7], puts into perspective the performance of these by evaluating JPEG 2000 versus JPEG-LS and MPEG-4 VTC, as well as the older but widely used JPEG.
This paper compares JPEG 2000 to other coding standards on the basis of compression efficiency as well as functionality set, and provides an outlook on the future of image coding. In paper [10] they have proposed a new video security scheme, which includes two encryption methods DCEA and event Shuffling.

In paper [10], they have proposed a new video security scheme, which includes two encryption methods DCEA and event Shuffling.

Figure 1. The UAV sending an image of a particular location to the army base

In paper [3] they present some experience in using neural networks for image compression. The multilayer perception was used for direct image compression. The transform coding capabilities of neural network enable this compression. The network was trained with blocks of an image and tested with the same image. Another image was used in simulation purposes, where perception showed good generalization capabilities.

In paper [4] the nonlinear nature of neural networks can be exploited to design nonlinear predictors for predictive coding. Multilayer perceptions (Figure 2) trained via the back propagation algorithm have been shown to increase predictive gain relative to linear predictors. Other networks based on higher-order statistical models and recurrent models have similarly shown improvements over linear predictor.

Figure 2. General architecture of multilayer perception

In paper [8], they have discussed various up-to-date neural network architectures for image compression, which are classified into different categories based on the nature of their application and design. These include direct development of neural learning algorithms for image compression, and neural network implementation of traditional image compression algorithms.

In paper [6], they analyzed the Advanced Encryption Standard (AES), and they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance; mainly for images characterized by reduced entropy. In this paper, they analyze the Advanced Encryption Standard (AES), and add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance; mainly for images characterized by reduced entropy.

In paper [9], presents the AES algorithm with regard to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL). This paper proposes a method to integrate the AES encrypter and the AES decrypter. This method can make it a very low-complexity architecture, especially in saving the hardware resource in implementing the AES Sub Bytes module and Mix columns module etc. Most designed modules can be used for both AES encryption and decryption. The architecture can still deliver a high data rate in both encryption/decryption operations.

2. IMAGE COMPRESSION

Image compression research aims at reducing the number of bits needed to represent an image. Image compression algorithms take into account the psycho visual features both in space and frequency domain and exploit the spatial correlation along with the statistical redundancy. However, usages of the algorithms are dependent mostly on the information contained in images. A practical compression algorithm for image data should preserve most of the characteristics of the data while working in a lossy manner and maximize the gain and be of lesser algorithmic complexity. In general almost all the traditional approaches adopt a two-stage process; first, the data is transformed into some other domain and or represented.

There are number trials of using neural networks as signal processing tools for image compression. In this paper [3], a direct solution method is used for image compression using the neural networks. An experience of using multilayer perception for image compression is presented. The topology of neural network shown in fig 2.1, the multilayer perception is used for transform coding of the image. The network is trained for different number of hidden neurons with direct impact to compress ratio. It is experimented with different images that have been segmented in the blocks of various sizes for compression process. Reconstructed image is compared with original image using signal-to-noise ratio and number of bits per
pixel. The results show the possibility of using multilayer perceptions for image compression.

![Figure 3. Topology of the neural network](image)

![Figure 4. Feed-forward neural network architecture](image)

This paper [4] presents a tutorial overview of neural networks as signal processing tools for image compression. They are well suited to the problem of image compression due to their massively parallel and distributed architecture. Their characteristics are analogous to some of the features of our own visual system, which allow us to process visual information with much ease. The characteristics of artificial neural networks which include a massively parallel structure, a high degree of interconnection, the propensity for storing experiential knowledge, and the ability to self-organize, parallel many of the characteristics of our own visual system.

In contrast, standard approaches to the processing of image data have been based on a serial paradigm of information processing which is more suited to sequential information such as language. As a result, neural network approaches to image compression have been shown to perform as well as or better than other standard approaches. Image Compression using Artificial Neural Networks is a topic where research is being carried out in various directions towards achieving a generalized and economical network proposed in paper [5].

Feed forward networks using back propagation Algorithm adopting the method of steepest descent for error minimization is popular and widely adopted and is directly applied to image compression. Various research works are directed towards achieving quick convergence of the network without loss of quality of the restored image. In general the images used for compression are of different types like dark image, high intensity image etc. Artificial Neural Networks have been applied to image compression problems, due to their superiority over traditional methods when dealing with noisy or incomplete data.

The Feed-Forward Neural Network architecture shown in Figure 4 is capable of approximating most problems with high accuracy and generalization ability. This algorithm is based on the error correction learning rule. Error propagation consists of two passes through the different layers of the network, a forward pass and a backward pass. In the forward pass the input vector is applied to the sensory nodes of the network and its effect propagates through the network layer by layer. Finally a set of outputs is produced as the actual response of the network.

### 3. ENCRYPTION

Encryption is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access.

![Figure 5. AES algorithm- encryption Structure](image)

In October 2000, NIST (National Institute of Standards and Technology) selected Rijndael as the new Advanced Encryption Standard (AES), in order to replace the old Data Encryption Standard (DES) and triple DES.

Joan Daemen and Vincent Rijmen are invented AES to replace the Data Encryption Standard (DES) algorithm. The AES, also known as Rijndael, is a block cipher adopted as encryption standards by the US government.
which specifies an encryption algorithm capable of protecting sensitive information. Data Encryption Standard (DES) was the earlier technique which was used to code the image or video. Since 1990, many specific methods have been proposed, such as SCAN–based methods, chaos-based method, true structure-based methods, and other miscellaneous methods for image encryption physical systems, processes and scientific problems that involve local interactions, like image processing, data encryption and byte error correcting codes. Limitations of earlier technique are Performance, Speed, Security, Throughput, Low accuracy, High cost. The input and output for the AES algorithm each consist of sequences of 128 bits. These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The cipher key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and cipher key lengths are not permitted by this standard. The input, output and cipher key bit sequences are processed as arrays of bytes that are formed by dividing these sequences into groups of eight contiguous bits to form arrays of bytes.

The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. AES algorithm - Encryption Structure is shown in Figure 5. These blocks operate on array of bytes and organized as a 4x4 matrix that is called the state. For full encryption, the data is passed through number of rounds Nr (Nr = 10, 12, 14), AES Encryption and Decryption are shown in fig 3.2. These rounds are governed by the following transformations from [6]:

3.1 Subbyte Transformation
A non-linear substitution step where each byte is replaced with another according to a lookup table.

3.2 Shiftrows Transformation
A transposition step where each row of the state is shifted cyclically a certain number of steps.

3.3 Mix Columns Transformation
Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

3.4 Addroundkey Transformation
Is a simple XOR between the working state and the roundkey. The cipher transformation is inverted and implemented in reverse order to produce a straightforward inverse cipher for AES algorithm. Invshiftrows, invsubbyte, invmixcolumn and addroundkey are the transformation performed in decryption.

The encryption procedure consists of several steps as shown in above Figure 6. After an initial add round key, a round function is applied to the data block (consisting of byte sub, shift rows, mix columns and add round key transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv Shift rows, the Inv-Mix columns, and the Add round key allow the form of the key schedules to be identical for encryption and decryption.

4. SYSTEM DESIGN
4.1 Multi Layered Feed Forward NN
Neural Networks as signal processing tools for image compression, the application of neural networks to the problem of image compression have produced some promising results. By their very nature, neural networks are well suited to the task of processing image data. The
characteristics of artificial neural networks which include a massively parallel structure, a high degree of interconnection for image coding. It is constituted by predictions and updating steps. Feed forward Networks using Back propagation Algorithm adopting the method of steepest descent for error minimization is popular and widely adopted and is directly applied to image compression.

![Image Coding System Diagram](image)

Figure 7. Block diagram of the image coding system

4.2 Quantizer

The process of approximating the continuous set of values in the image data with a finite (preferably small) set of values. The input to a quantizer is the original data, and the output is always one among a finite number of levels. The design of the quantizer has a significant impact on the amount of compression obtained and loss incurred in a compression scheme.

4.3 Advanced Encryption Standard (AES)

AES is a block cipher with variable key length (128-bit, 192-bit, and 256-bit respectively) and block size of 128-bit. AES need very low memory requirements to make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES can be programmed in software or built with pure hardware.

4.4 Huffman Coding

Huffman coding is a form of encoding that creates the most efficient set of prefix codes for a given text. The principle is to use a lower number of bits to encode the data that occurs more frequently. The ease with which Huffman codes can be created and used makes this still an extremely popular tool for compression code.

4.5 Controller

The controller is a module needed for optimizing applications security requirements based on a variable system resources. Users can define their security requirements for a particular security service by specifying a security range. The most important abstraction in controller module is security levels, which is used to indicate how strength is a particular security service. The control AES identify the encryption or decryption scheme.

4.6 HDL Modeling and Verification

The feed forward neural network architecture designed for image compression consists of 16 inputs in the input layer, and is compressed to 4 outputs in the hidden layer. The hidden layer has 4 neurons, 64 multipliers, 4 bias elements, 4 adders and 4 network functions. The output layer is also designed according to the requirements of hidden layer. The HDL model developed is verified for its functionality using testbench. Various test vectors are used to test the network functionality. The AES algorithms is also modeled using HDL and is verified with different test vectors using test bench. The verified model is synthesized and performances are estimated for comparison.

5. RESULTS AND DISCUSSION

The sum of encryption results shown in the Table 1 and 2 of different Families of FPGA

<table>
<thead>
<tr>
<th>Table 1: Encryption results on Virtex2p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Utilization</td>
</tr>
<tr>
<td>Number of Slices</td>
</tr>
<tr>
<td>Number of Slice Flip Flops</td>
</tr>
<tr>
<td>Number of 4 input LUTs</td>
</tr>
<tr>
<td>Number of bonded IOBs</td>
</tr>
<tr>
<td>Number of BRAMs</td>
</tr>
<tr>
<td>Number of GCLKs</td>
</tr>
<tr>
<td>Total Power(w)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Encryption results on Virtex5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Utilization</td>
</tr>
<tr>
<td>Number of Slice Registers</td>
</tr>
<tr>
<td>Number used as Flip Flops</td>
</tr>
<tr>
<td>Number of Slice LUTs</td>
</tr>
<tr>
<td>Number used as logic</td>
</tr>
<tr>
<td>Number used as Memory</td>
</tr>
<tr>
<td>Number used as Shift Registers</td>
</tr>
<tr>
<td>Number using O6 output only</td>
</tr>
<tr>
<td>Total Power(w)</td>
</tr>
</tbody>
</table>
6. CONCLUSION

With security of information being given priority during data transmission, channel noise being considered as another major constraint in data transmission, in this work we have used neural network architecture for image compression and AES for data encryption. Neural network architecture is trained to learn the features of input image and compresses the information; noise in the channel does not affect the compressed data as the decompression architecture is immune to noise. The complexity in AES is reduced as the compressed data is smaller in size compared with original image thus improving the speed of processing. The Neural Network architecture with AES algorithm is modeled and implemented on FPGA. Performances such as area, power and speed complexities are compared. The architecture occupies 9% of slices on Virtex-5 FPGA and consumes power less than 1.128W. The design is suitable for real time applications on FPGA platform. Further the processing speed and power consumption can be optimized using pipelined architecture and low power techniques respectively.

REFERENCES