An Efficient Memristor based Image Encryption Algorithm

V. Parthasarathy, *G. Saravana Kumar, #S. Sivasaravana Babu, *S. BanuPriya

Address For Correspondence:
V. Parthasarathy, Dean and Professor, Department of Computer Science and Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, AVADI, Chennai, TAMILNADU, INDIA.

ABSTRACT

Contemporary inquisition on numerous schemas of FPGA endeavoring curtailment of power consumption effectuates the inference that one of the utmost expansively used contexts is Static Random Access Memory (SRAM) based structures. This paper addresses the limitations associated with SRAM such as bw density longer routing path, increased propagation delay, increased peak power consumption rate as well as high value of average power consumption and proposes an alternative methodology for image encryption schemes. This paper proposes Neuotropic Memristor based FPGA design to achieve high degree of correlation measure. A comparison study between conventional encryption algorithm and the results attained by this proposed corroborates the efficacy of the suggested method.

KEY WORDS: Image Encryption, Field-Programmable Gate Arrays (FPGA), Memristor, Low Power Consumption, SRAM, Very Large Scale Integrated Circuits

INTRODUCTION

Many digital services require reliable security in storage and transmission of digital images. Due to the rapid growth of the internet in the digital world today, the security of digital images has become more important and attracted much attention. The prevalence of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users’ privacy for all applications. Encryption techniques of digital images are very important and should be used to frustrate opponent attacks from unauthorized access (Mitra et al, 2006). (Shujun et al, 2002), (Lee et al, 2003). Digital images are exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data (Hossam El-din et al, 2006). There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types (Shujun and Zheng, 2002), (Mohammed Husainy, 2006). In general, most of the available encryption algorithms are used for text data. However, due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for...
multimedia data (Yas A. Alsultanny, 2008), (Droogenbroeck and Benedett, 2002), (Fong and Singh, 2002). According to Xun (2001) and Wang (2005), even though triple-data encryption standard (T-DES) and international data encryption algorithm (IDEA) can achieve high security, they may not be suitable for multimedia applications (Xun et al, 2001), (Wang et al, 2005). Therefore, encryption algorithms such as data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA) were built for textual data (Lee et al., 2003), (Syed, 2002), (Xun et al., 2001). Although we can use the traditional encryption algorithms to encrypt images directly, this may not be a good idea for two reasons. First, the image size is often larger than text. Consequently, the traditional encryption algorithms need a longer time to directly encrypt the image data. Second, the decrypted text must be equal to the original text but this requirement is not necessary for image data. According to Chang (2001), due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable (Chang et al., 2001), (Jiri Jan, 2005), (David Salomon, 2005). The intelligible information present in an image is due to the

*Journal of Applied Science and Agriculture*, s(x) Month 2014, Pages:X-X:
correlation among the image elements in a given arrangement. According to Mitra (2006), Most of the algorithms specifically designed to encrypt digital images were proposed in the mid-1990s. According to the Maniccam and Bourbakis (2004), there are two major groups of image encryption algorithms: (a) Non-chaos selective methods, and (b) Chaos-based selective or non-selective methods (Maniccam and Bourbakis, 2004). However, most of these algorithms are designed for a specific image format, either compressed or uncompressed. There are methods that offer light encryption (degradation), while others offer strong form of encryption. Some of the algorithms are scalable and have different modes ranging from degradation to strong encryption. According to Borko (2005), the user is expected to choose a method based on its properties, which will be best for image security (Borko Furht et al, 2005). Image encryption has applications in internet communication, multimedia systems, medical and military imaging systems. Each type of multimedia data has its own characteristics such as high correlation among pixels and high redundancy. Thus, different techniques should be used to protect confidential image data from unauthorized access (Hossam El-din et al., 2006), (Ozturk and Sogukpinar, 2004).

The rationale behind the proposed algorithm is the ever-increasing need for harder-to-break encryption and decryption algorithms as the computer and network technologies evolve. VLSI implementation of efficient image cryptography should satisfy the following main parameters: less area, less power consumption, less propagation delay, less execution time, reduction in the relationship among image elements by increase in the entropy value of the encrypted images as well as reduction in the correlation also the key space analysis should be more.

2. Power Consumption in FPGA:

2.1. Structure of Conventional FPGA:

Power Consumption in FPGA is mainly due to the static and dynamic power consumption, which in turn is due to the conventional structure of the FPGA. It is made of several arrays of blocks and each block consists of one logic block (LB), two connection blocks (CB) and one switch block (SB). Each logic block contains a cluster of basic logic elements (BLE’s); the lookup tables (LUT’s) for providing the logic functions. LB’s are connected to the routing channels through CB’s and the routing channels are connected with each other through the SB’s. The selector pins of each multiplexer are connected to the SRAM cell made of 6-transistors for their connectivity with much larger area and higher complexity compared to the direct interconnects of the ASIC. The programming technology for the logic and interconnect resources are the SRAM. The SRAM based FPGA’s offer in-circuit re configurability though being volatile

2.2. Sources of Power Dissipation:

All The main sources of the power dissipation in the FPGA are the static, dynamic and the memory cell power consumption. FPGA’s consume more power than the ASIC because of the presence of a large number of transistors which though provides flexibility causes both the static and dynamic power dissipation. The SRAM cells have to be slowed down and their leakage have to be reduced in order to reduce the total power consumption of FPGA. Furthermore, SRAM cells constitute a large space of the FPGA’s total area which makes the wire lengths in FPGA’s longer. These interconnects thus increases the high capacitive load in FPGAs, making it as the primary source of dynamic power dissipation. The earlier techniques that are commonly used to reduce the power consumption of the conventional FPGA are as follows:

1) Architectural level power reduction techniques:

The architectural level power reduction techniques are fine grained-VDD, leakage reduction in FPGA routing multiplexers, low power programmable FPGA routing circuitry, clock gating power reduction technique, power gating and sub threshold FPGA.
2) Circuit level power reduction techniques:
The circuit level power reduction techniques are a dual-threshold FPGA routing design, programmability of VDD, input vector reordering, FPGA leakage power reduction using CLB- clustering and dual threshold transistor stacking (DTTS).

3) Device level power reduction techniques:
The device level power reduction techniques are leakage power reductions from Tunnel FETs (TFETs) and carbonnano tube SRAM design.
The key problems in the related works are mainly due to the presence of the SRAM based interconnects in the FPGAs architecture which results in high power consumption. These related works are mainly focused on reducing the number of transistors in the SRAM. However almost the same amount of power is being consumed once again, because of the access time, density and power dissipation of the SRAM.

2.3. Conventional SRAM based FPGA:
The Conventional FPGA’s are made of SRAM based programmable interconnects. The major power consumption in
FPGA is due to its programmable routing structure made of SRAM. The energy consumption in the SRAM includes two components: dynamic energy consumption and static energy consumption. Static energy consumption, consumed due to leakage current in SRAM, and dynamic energy consumption consumed due to the charging and de-charging of capacitance during read and write operation. It is been found that the programmable interconnects in FPGA accounts for about 90% of the total area, about 80% of the total delay and about 85% of the total power consumption.

2.4. Memristor based FPGA:
In this paper the proposed methodology is aimed to reduce the power consumption of FPGA by using the Memristor-based FPGA architecture.
The methodology used here is the neoteric Memristor based FPGA architecture. Memristor based FPGA uses Memristor interconnects rather than programmable interconnects made of SRAM memory cells. Proposed methodology is made of 3-D crossbar-based memory architecture with the 3D die-stacking process and also provides capacitance shielding from unused routing path. The programmable interconnects of Memristor based FPGA architecture uses the newly found circuit element, i.e. Memristors instead of the SRAM based interconnects as in the usual FPGA architecture, resulting in significant reduction of overall area power consumption, area, interconnect delay and increases the speed of the FPGA. Compared to the existing system, it does not occupy more area because Memristor is a nano device. The main highlight of this approach is that it employs the Resistive Random Access Memory (RRAM) instead of the SRAM.

![Fig. 1: Structure of Memristor](image)

Memristor is a fourth fundamental passive 2 terminal linear resistor with memory (RRAM). Memristor is a semiconductor thin film sandwiched between two metal contacts with a total length of D of TiO2 film and it consists of doped low resistance and undoped high resistance regions. The physical structure of Memristor is shown in Fig 1. Resistance can be changed by changing the direction of applied voltage or current. Resistance increases when current flows in one direction and decreases when it flows in the other direction. When applied external potential is removed, Memristor remains in the last state. Memristor is capable of memorizing its own resistance, different resistance values can be used to represent different values of data.
The Memristive systems [15] can be described as follows:
\[ M(x) = R_{ON} x + R_{OFF}(1-x) \]
Where, \( x \) is the state variable which has to satisfy the boundary conditions of 0 and 1 and ‘\( M(x) \)’ is the Memristance

A. Memristor:
M depends on the history of current passing through the Memristor element, which makes the Memristor act like a
resistor with memory. The non linear Memristance (M) is a function of charge (q).

B. Main Features of the Memristor:
The following are the main features of the Memristor:
i. Has resistive Random Access memory (RRAM).
ii. Small size (<10 nm, two terminals) and scalable below 5x5nm. iii. Can be programmed within 5ns at 180nm.
iv. Saves power consumption
v. Long lifetime
vi. Needs a very low biasing voltage and ultrafast switching - up to six orders of magnitude due to the highly non-linear rate of switching.

Fig. 2: Structure of 1 Transistor 1 Memristor Model

3. Implementation:
The proposed algorithm flow consists of following steps,
i. Conversion of image into hexadecimal value using MATLAB.
ii. Implementation of Memristor based user logic using VERILOG.
iii. Implementation of APC-OMS technique using VERILOG.
iv. Implementation of AES encryption using MODELSIM.
v. Conversion of AES encrypted hexadecimal data into cipher image using MATLAB.
vi. Implementation of AES decryption using MODELSIM.
vii. Conversion of hexadecimal data into image using MATLAB.

Fig. 3: Image Encryption
The plain image taken for both the conventional and the proposed MEMRISTOR based logic is the Lena, grey image of size 256x256 as shown in Fig. 4
Fig. 4: Input Lena grey image

The Overall Block diagram of the proposed scheme where the comparison of both the proposed and the existing techniques are shown in Fig.4. The Fig. 6 shows the generalized output of the Memristor based image cryptography which is obtained via Matlab. First the input image is fed, then it is converted into hex value, then it is converted into cipher image, then it is again converted as plain image.

Fig. 5: Overall Block diagram

Fig. 6: Generalized output of the MEMRISTOR based image cryptography
Since an image itself cannot be used protected directly, it is being converted to a hex data and then that data is being encrypted first. A digital image is defined as a 2-D rectangular array. The elements of this array are called as pixels. Each pixel has an intensity value as digital number and a location address as row and column. Each pixel in an image is represented by 8 bits which are nothing but 1 byte. Using MATLAB, the pixel values can be converted into bytes. These byte values can be indicated as hexadecimal values. This hex data value is given as the input to encryption algorithm block. The encryption technique used in this project is Advanced Encryption Standard (AES) and the resultant images are shown in Fig. 7 and Fig. 8.
For protecting the data in the image they must be converted into one-dimensional arrays before using any encryption technique. The sequence of data in the image can be encrypted into blocks or streams by using block cipher and stream cipher. This paper utilizes AES algorithm. A product cipher can also be used to encrypt a file of image data. Compression techniques can be used for encryption in order to reduce computational effort and increase the speed of processing. The hexadecimal values got from the image by using MATLAB are generally stored in RAM.

The Fig.9 shows the conversion of decrypted Hexadecimal data into decrypted image of the existing system using Matlab software. After the hex data of the plain image is been encrypted with the key in the encryption block, the cipher image (or) the encrypted image is being obtained from the Matlab. Then again this cipher image and the same key which is being extracted from the plain image before the AES encryption are given as the input to the decryption block of the AES. The images shown in Fig. 10, Fig. 11 and Fig. 12 reveals the effectiveness of the proposed scheme.
Correlation is a measure that computes degree of similarity between two variables. Any image cryptosystem is said to be good, if encryption algorithm hides all attributes of a plaintext image, and encrypted image is totally random and highly uncorrelated. If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero.
The above table shows the coefficient values randomly in all the three positions of the plain image and the cipher image. Here the values of encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero.

Table 2: Correlation coefficient of Existing system

<table>
<thead>
<tr>
<th>POSITION</th>
<th>PLAIN IMAGE</th>
<th>CIPHER IMAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vertical</td>
<td>0.965432</td>
<td>-0.002674</td>
</tr>
<tr>
<td>Horizontal</td>
<td>0.947654</td>
<td>-0.003598</td>
</tr>
<tr>
<td>Diagonal</td>
<td>0.964999</td>
<td>-0.005693</td>
</tr>
</tbody>
</table>

The Table 2 shows the coefficient values randomly in all the three positions of the plain image and the cipher image. Here the values of encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. Thus the proposed Memristor based system is a better system in terms of less correlation coefficient parameter.

**Conclusion:**

By implementing the proposed methodology of image cryptography, the Memristor is replaced instead of the normal memory in order to achieve reduction in overall area and power consumption and propagation delay and also it satisfies the usual image cryptography parameters like less correlation coefficient, high entropy value, better randomly distributed histogram, more key sensitive with high key space analysis value and avalanche effect value, less simulation time and less memory for implementation. These are the main features for a better image cryptography technique. This shows that the proposed Memristor based image cryptography method is the better option than the conventional RAM based image cryptography method. The future enhancement that can be done in extending this project is to implement the Memristor based hardware security and Neuromorphic application circuits in FPGA.

**REFERENCES**


Zhe Zhang and Jose G. Delgado-Frias, 2012. “Carbon Nano tube SRAM Design with Metallic CNT or Removed Metallic CNT Tolerant Approaches”, IEEE.


Peter J. Grossmann et al, 2012.“Minimum Energy Analysis and Experimental Verification of a Latch-Based Sub threshold FPGA”

Assem, A.M. Boul and Steven J.E. Wilton, 2010.”An FPGA architecture supporting dynamically controlled power gating.

