International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5715-5721

Efficient Implementation of Selective Image Encryption Technique on Multi-core Reconfigurable System

Rahul K. Hiware[1], Dr. Dinesh V. Padole[2]

[1]Research Scholar, [2]Professor,
Department of Electronics Engineering, G.H. Raisoni College of Engineering,
Digdoh Hills, Nagpur, Maharashtra 440016, India.

Abstract

Advances of microprocessor design has been putting multiple cores on a single chip giving ways to internal parallel computing an exodus from increase in single clock frequency to provide remarkable growth in speed. What's significant is that each configuration presents itself to developer as a set of two or more cores capable of executing multiple tasks concurrently. Current advancements in industry highlight reconfigurable architectures as the new trend capable of conquering complexity of design, computational time and cost the primary research aspect of our paper. Researcher to conquer these complexity constraints looks up to CGRA's (Course Grained Reconfigurable Architectures) for application specific optimization. This paper highlights the amendments/advancements in the implemented VHDL reconfigurable multi-core processor and its architecture for demonstrating its capability via application specific optimization. Due to abundant amount of data, Image encryption imposes heavy resource requirements on the hardware platform. To test complexity and accountability of structure, a Selective Image Encryption technique using base calculation of 2D-DCT is implemented. The paper also covers the mathematical apparatus utilized to explore the implemented structures accountability and testability.

Keywords: Multi-core, CGRA, Reconfiguration, Image Processing, Optimization, VHDL, Encryption

INTRODUCTION

Computational tasks are derived sets of rules combined together to form an application requiring certain time for computation. This computational time also known as running time is the most important efficiency characteristic of a system. Computer science domain studies the character of computation among other things to largely dictate its uses. A set of rules used to carry out a computation is known as an algorithm. Computation could be the least amount of requirement not just limited to algorithm but also needs to take into account the structure and the attributes of a processing unit. Description with respect to class of algorithm that we study, compare, utilize and modify requires mathematical apparatus that can test/explore structures to provide their capabilities. These capabilities provide for multi core computer architectures optimally tailored for specific algorithms demanding faster parallel commuting or rather greater order of computing. Multi-core processors are preferred over single core as single core processors hastily reach the physical limits of possible complexity and speed. To achieve high performance without increasing power consumption and heat has become a critical concern. That's why a strong demand for high performance and flexible application is pushing designers to move to multi-core systems. Multi-core architectures provide a new dimension to scale up the number of processing elements (cores) and, therefore, the potential computing capacity [1][2][3][15]. The potential capacity of such Multi-core architectures is explored and demonstrated with the help of this research paper.

Image a major acquisition and representation form of data over the past years is utilized by numerous applications as their integral part. Latest trends in embedded systems concentrate on the evolving role of security and its impact in communication. Real time imaging and its seamless video transmission imposes heavy pre as well as computational requirements on encryption and decryption blocks [4]. Efficient encryption and decryption on FPGAs have been implemented in the past, with the goal of conquering security measures with fewer overheads of communication prerequisites. Few techniques have sponsored low power and area efficient architectures [5], while others deployed area efficient shuffling schemes [6] for implementation on FPGAs bringing us to our main area of exploration and optimization. Many techniques have been brought in mainly to increase the throughput of such encryption & decryption techniques by deploying multi-core architecture [7]. For embedded applications utilizing complex architecture designed and implemented on FPGA, area is the central optimizing parameter for such encryption and decryption algorithms [16].

With development communication is more demanding because of faster computational possibilities. For such vigorous computation, utilization of power management techniques for performance enhancement in various applications plays a key role. Encryption of image puts heavy load on processing engine in terms of size of data. To reduce such burden techniques utilizing selective image encryption are becoming regular in research. Selective area encryption with permuted un-encrypted area consequences in good achievement of the mean square error and peak signal to noise ratio [8][9][10]. Some selective encryption methods suggest no regulation over the quantity of encryption making their parameter extraction and optimization very challenging when it comes down to soft computing [11][12][13]. To overcome such challenges FPGA's serve as a great platform to implement a new design for analysis of performance

parameters with the goal of computational optimization. Selective image encryption when implemented on FPGA should use minimum hardware resources while taking less time which might cater many applications [14][15][16]. One such technique based on discrete cosine compression modified with selective encryption utilizing a multi core reconfigurable 4x4 architecture area requiring architecture having multi core processing along with preemptive reconfiguring capacity for the fixed architecture is implemented and presented in this paper.

The image of fixed size (256 x 256) is first divided into blocks of constant size (8 x 8). A mask following the base calculation of 2D-DCT (discrete cosine transform) comprising of selective pixel encryption option is also formed which is overlapped along with the image and computed specifying the encrypted pixels to achieve an enhanced, compressed and encrypted image. This encrypted image can only be decrypted with the decryption algorithm and the created mask to generate the original image providing an additional security. Computational analysis of MATLAB vs FPGA performance has been carried out to highlight the optimizing parameters conquered in the research. The paper is structured as follows: Section 2 presents the concept of the proposed reconfigurable system and algorithm and for a gray scale image. Section 3 discusses the VHDL modeling and Simulation for selective image encryption based on 2D-DCT compression. Section 4 presents FPGA performance and MATLAB computational results in details followed by experimental results in Section 5. Conclusion is presented thereafter.

ANTICIPATED ALGORITHM

In the algorithm the image is firstly divided into blocks. A selective mask overlapping utilizing 2D-DCT as in equation 1 is carried out on each of such block. Selective Pixels based on masking considerations are encrypted and others are left unencrypted. This is carried out for all the blocks of the image to achieve a partially encrypted image which is equal to the size of input image. This mask is the user variable security key on the decryption side to generate the original image. This selective encryption reduces the compression ratio but also adds up an additional security feature utilized for demonstrating the computational capabilities of our multi core reconfigurable system rather than concentrating on the image encryption and decryption.

$$Z = A \; x \; I \; x \; A' \qquad (1)$$

Where Z = Output image (Encrypted and 2-d cosine Transposed)

A = Selective pixel mask

I = Input image block

A' = Transpose of Selective pixel mask

A. PROPOSED SYSTEM

The proposed system, shown in fig.1 [17], consists of an array of 8 Processors having simple ALUs (Arithmetic & Logical units) called as Processing Element (PE) shared memory, configuration memory, bus management unit (BMU), main processor and external memory (not show in fig.1) where input/output image will be stored .

1) Main Processor

Main Processor will control and monitor all operations of proposed system like process management, memory management and scheduling.

2) BMU

Bus management unit (BMU) manages operations of data bus and configuration bus.

3) Processing Elements

4) Processing Elements (PE), also referred as core in this paper, are processing blocks which will be activated during applications. In Proposed system, all cores are homogeneous, and it could be any processing system like simple ALU to High-end Processors. For effortlessness, here we have taken simple 16 bit processor core to form 8 PEs.

5) Configuration Memory

Configuration memory is key block of the system. Configuration codes in form of Data flow graph (DFG) for different applications are stored in memory. As per DFG particular core will perform instructed operation. The data which is to be processed will be provide by BMU as per the scheduling algorithm [17].

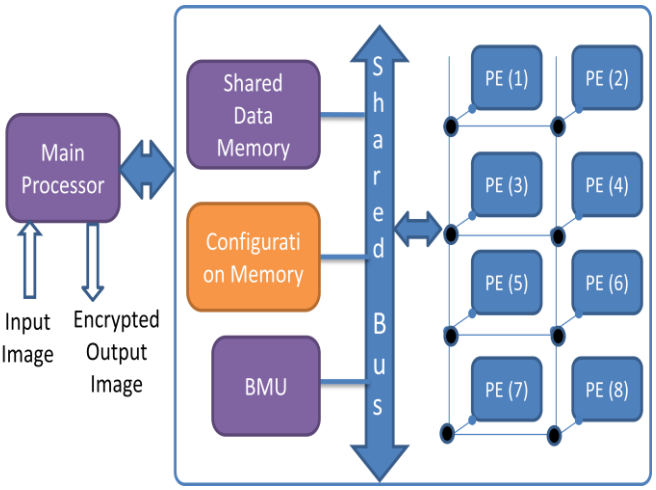

Figure 1. Multi-core Reconfigurable System

Text I/O is used for simulation, where the image converted to text file is accessed and divided into a number of blocks for parallel operations of processing elements. The selective encryption mask is utilized and combined based on the pixels to be encrypted following the algorithm. The partially encrypted and compressed data is then achieved ready for transmission. For testing the VHDL code, a 256 x 256 image is accessed and divided with 8 x 8 block size. For processing such small blocks on the basis of 2D-DCT we have register bank of 8 registers in each processing core. At a time 8 cores

work parallel to process our 8 x 8 block size. The processed block is then transferred to the 8 other cores for data recording and next step of transformation is carried out. Once the complete blocks are processed the encrypted blocks are combined to form our complete encrypted 256 x 256 image/block and written out with the help of Text I/O operation the process can be better understood with the help of a data flow diagram as in fig 2 below. Number in node represents that particular PE is active and performing operation mention on top of it (shown in fig. 2).

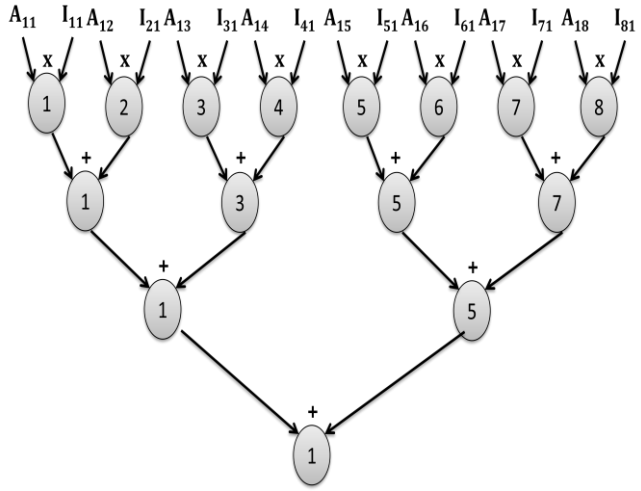

Figure 2. Data Flow Diagram (DFG) of Matrix multiplication

Data flow diagram shows that at the first state all the values are loaded which are to be operated upon i.e first row of Selective pixel mask A and first column of Input image I of the first 8 x 8 block of data. An 8 x 8 matrix multiplication needs to be carried out which is configured in terms of multiplication and addition operations. In the data flow graph second state shows the multiplication of cross bars which is then followed by reconfiguration of elements to perform addition of few as well as loading of the remaining others. Next step is then combination of all the three steps depending on the requirement be it addition of previous step, multiplication of last loaded elements or loading of next set of data in the free processing elements. These steps provide us the output of the first 8x8 block which is then stored for further processing. These steps are reconfigured again and again with the help of data flow instructions providing us re-configurability. Such reconfiguration allows utilization of the multi core processor for other applications required by the user an indomitable advantage of our design.

VHDL MODELLING & SIMULATION

Sample image chosen to be encrypted is shown in figure 4(a). The image is converted to its pixel values for performing selective encryption with the help of our 16 core reconfigurable processor. The text values along with the operation codes [15] are read by the top processor using text I/O from the text input file and distributed to the specified processing elements hidden in the operation codes to perform our selective encryption and compression operation. Simulation is done to demonstrate the capability of our developed multi core processor so that one can correlate, compare and highlight the advantages of our multi core processor on comparison with general purpose platform generic processor.

Figure 3(a) shows the selective encryption mask (Element A) following the principles of 2D-DCT evaluation, a part of the input i.e. first block of 8x8 text integer values (Element I); transpose of encryption mask (Element A') and finally the integer values of compressed encryption process. Figure 3(b) shows the hex values of the first block after encryption. Hexadecimal values can be easily depicted during VHDL simulation as shown in figure 3(c); making sure that the output can be correlated and verified by the user. This operation performed on the first 8x8 block of data is repeated until the complete image is encrypted as shown in figure 4(b),(d). The chosen selective encryption configuration is further analyzed and evaluated in section IV that highlights the advantages offered by our designed multi core processor.

FPGA PERFORMANCE & MATLAB COMPUTATION RESULT

An important attribute which is utilized for our architectural optimization is the correlation. Moreover power requirements for programmable logic devices are highly dependent on the logic and functionality of your design, especially when we are trying to compare a hard processor with a soft core. Hence one needs to evaluate power implications and identify the cost trade-offs for different implementations in our design. Soft Core Processors - 250MHz and less (usually less than 200MHz) can be easily modified and tuned to specific requirements, more features, custom instructions, etc. In soft core processors multiple cores may be used at the cost of resource yet we implement a multi core processor having an additional overpowering feature that is reconfiguration with the help of custom instructions [15].

Hence choosing an FPGA platform that can help us reduce this trade-offs and helps us optimize our architecture is of prime importance. In our research a FGPA platform of modern technology "Artix 7" Xc7a100t is chosen for calculating the performance of the FPGA system. For a first block of 8x8 the time required for commutation is 3,77,360ns with the consideration of a 40ns clock cycle. Hence the complete block of image is processed in 96,226,800ns i.e. 96.28ms for the clock speed of mere 250 MHz. For processing the complete image as indicated by synthesis, we observe a variable cost on the area as in figure 5. Hence for selective encryption timing optimization at the cost of area depends on the selection of FPGA chip. Figure 6 shows that 0.169W of power is recorded by the Xilinx XPower Analysis. Hence our VHDL modeling can be further optimized in the aspects of power consumed by utilizing Memory Ram blocks instead of LUTs.

11	11	11	11	11	11	11	11
15	12	8	3	1	3	4	5
14	6	2	5	5	2	6	14
12	1	5	3	8	15	3	4
11	4	4	11	11	4	4	11
8	5	3	12	4	1	15	3
6	5	14	2	2	14	5	6
3	3	12	5	15	4	8	1
A							
11	15	14	12	11	8	6	3
11	12	6	1	4	5	5	3
11	8	2	5	4	3	14	12
11	3	5	3	11	12	2	5
11	1	5	8	11	4	2	15
11	3	2	15	4	1	14	4
11	4	6	3	4	15	5	8
11	5	14	4	11	3	6	1
A'							

246	245	242	242	242	244	245	245
246	246	245	245	243	243	243	244
245	246	246	246	243	242	242	242
244	245	244	244	242	241	241	241
244	243	242	242	241	241	241	241
245	244	242	242	240	241	241	240
244	244	243	242	240	241	241	242
242	242	243	243	241	241	242	243
I (First Block)							
1880824	1093202	1155154	1089286	1282380	1090452	1153999	1088659
1092740	635068	671345	632911	745036	633548	670453	632287
1154373	670615	709235	668616	787083	669284	708298	667989
1089187	633256	669179	631086	742568	631578	668293	630201
1281841	744826	787339	742429	874007	743196	786450	741956
1089924	633592	669473	631198	743088	631819	668779	630776
1154560	671216	709002	668645	787158	669452	708404	668312
1089550	633413	669029	631017	742889	631665	668493	630804
Z = A X I X A'							

Figure 3(a). Text I/O - First Block Encryption Process

1CB2F8	10AE52	11A052	109F06	13914C	10A394	119BCF	109C93
10AC84	09B0BC	0A3E71	09A84F	0B5E4C	09AACC	0A3AF5	09A5DF
119D45	0A3B97	0AD273	0A33C8	0C028B	0A3664	0ACECA	0A3155
109EA3	09A9A8	0A35FB	09A12E	0B54A8	09A31A	0A3285	099DB9
138F31	0B5D7A	0C038B	0B541D	0D5617	0B571C	0C0012	0B5244
10A184	09AAF8	0A3721	09A19E	0B56B0	09A40B	0A346B	099FF8
119E00	0A3DF0	0AD18A	0A33E5	0C02D6	0A370C	0ACF34	0A3298
10A00E	09AA45	0A3565	09A0E9	0B55E9	09A371	0A334D	09A014

Figure 3(b). First Block Encryption Output (Hex Values)

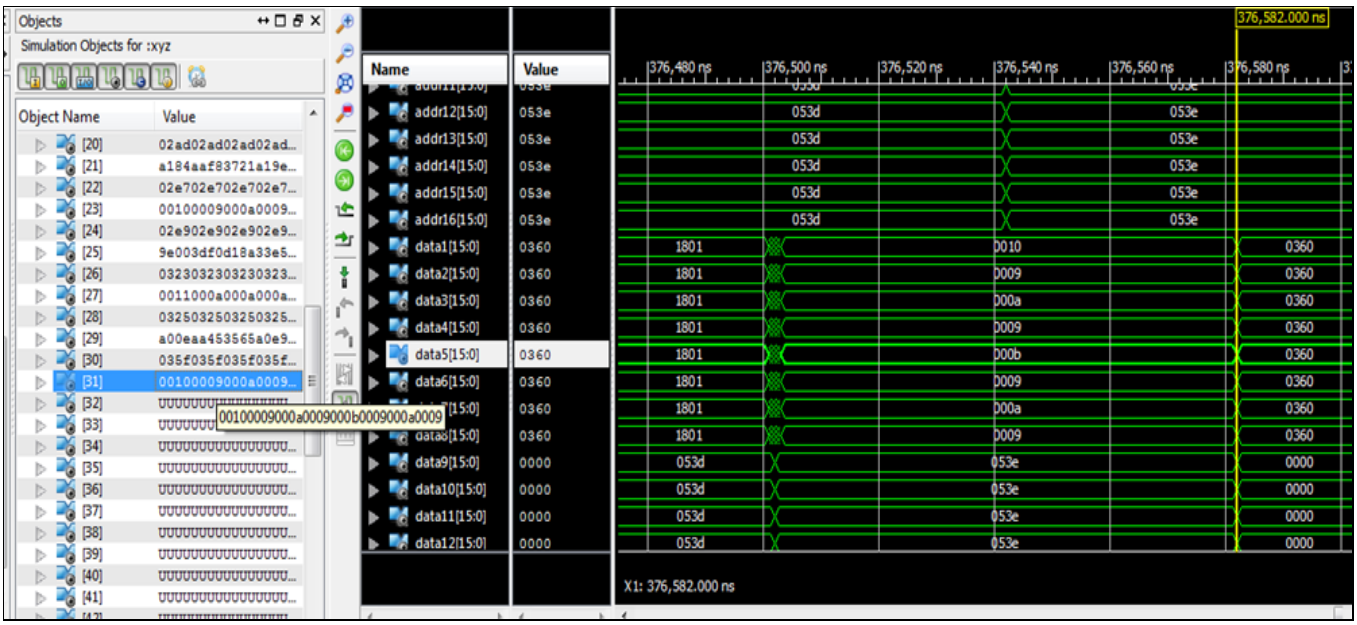

Figure 3(c). VHDL Simulation Waveform

Figure 4(a). Input Image - penguins

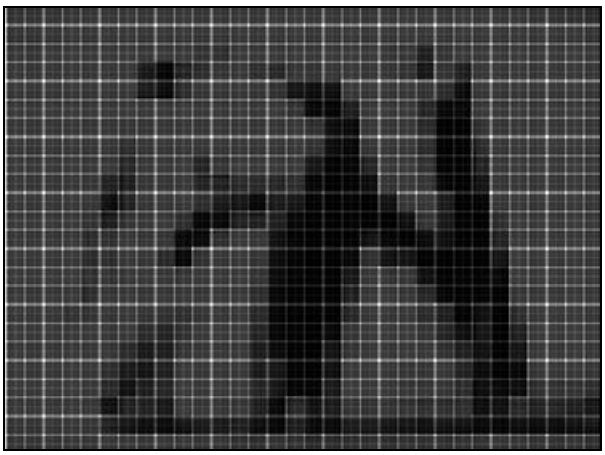

Figure 4(b). Selective Encrypted & Compressed penguins Image

Figure 4(c). Input Image - cameraman

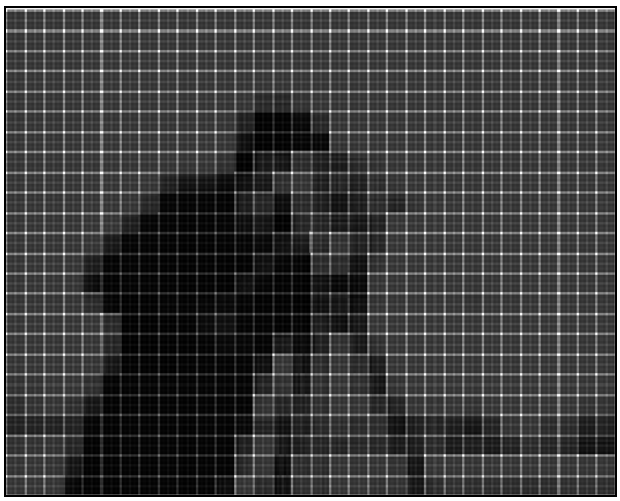

Figure 4(d). Selective Encrypted & Compressed Cameraman Image

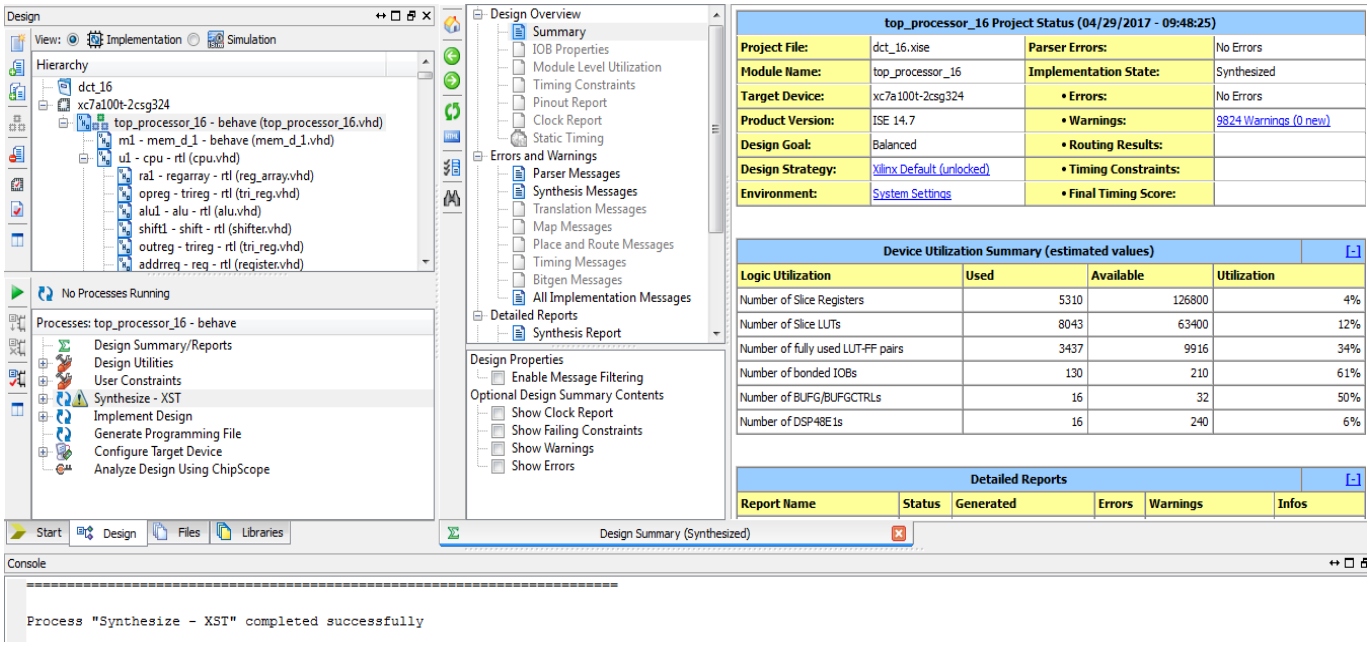

Figure 5. Xilinx Synthesis Report.

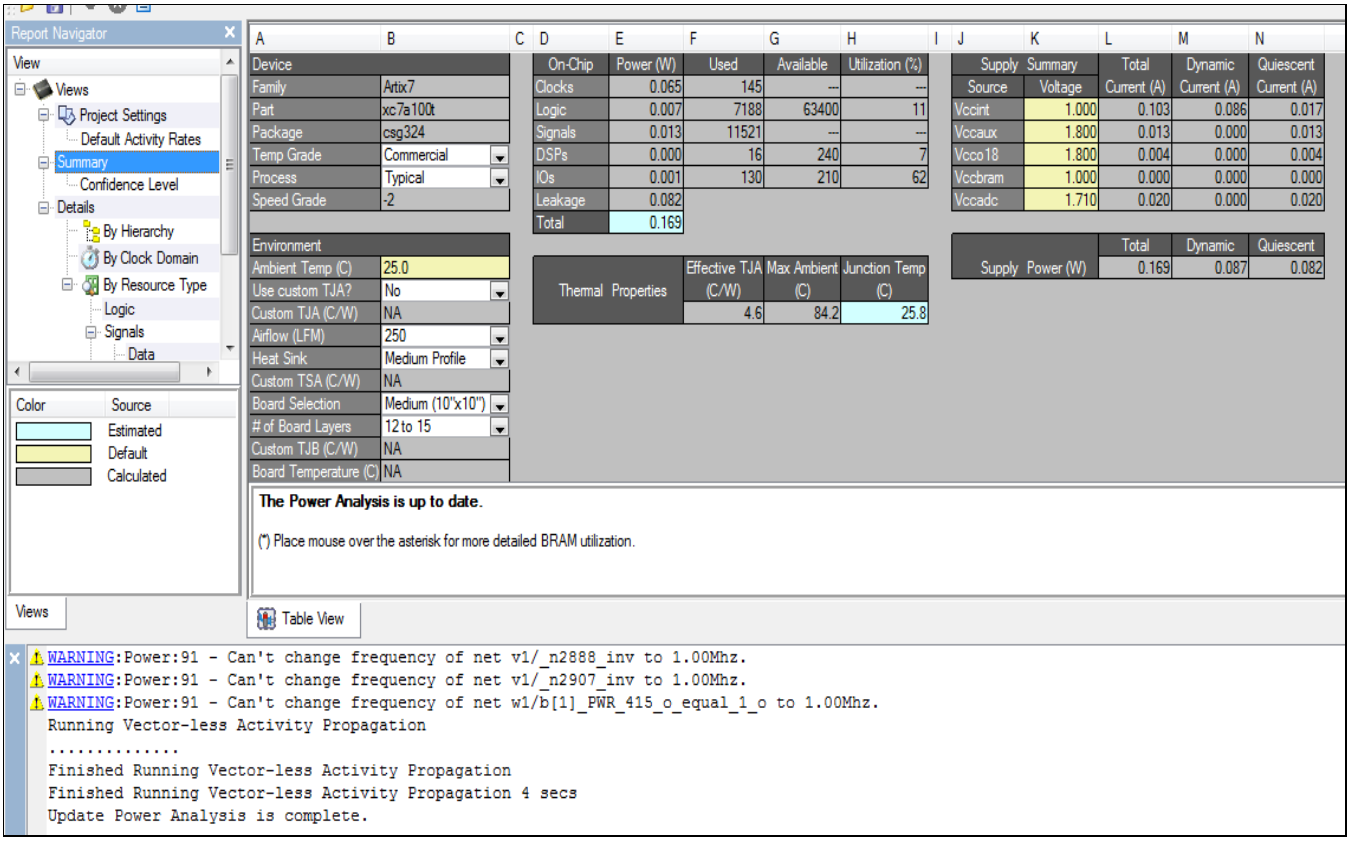

Figure 6. Xilinx Xpower Analyzer.

Similar computation is done on MATLAB to evaluate and understand the need of FPGA implementation over computational visualization. Profile viewer in-build function in MATLAB helps us evaluate the timing constraints of our script/code as shown in figure 7(a) & 7(b) . Figure 7(a) shows that 2.5Ghz is the operating system, utilizing that MATLAB requires total computational time of 1.071 seconds as highlighted in figure 7(b). Leaving the internal command "self time" of 0.350 seconds MATLAB requires 0.720 seconds i.e. 720ms to selectively encrypt and compress the image.

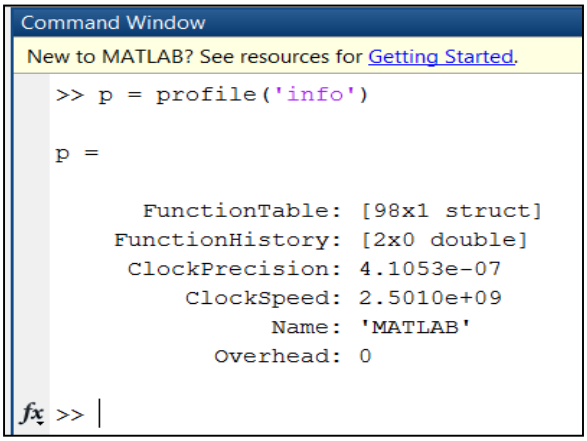

Figure 7(a). MATLAB system profile info

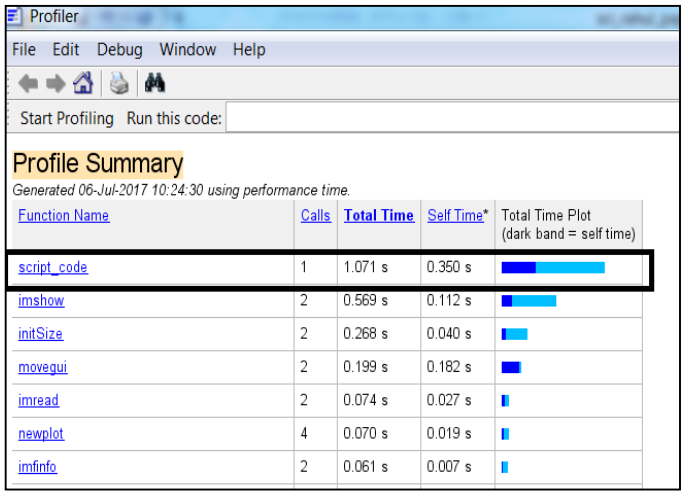

Figure 7(b). MATLAB Profile viewer for our code

CONCLUSION

Selective encryption of image is utilized in this paper which is relatively simple as compared to the other techniques used for selective image encryption earlier. The technique is randomly utilized where optimization of this technique was not our goal but computational analysis of our FPGA architecture was the prime objective. Optimization of performance parameters is a must in all domains of research. Sequencing and time analysis is one parameter that is covered in this paper. The research

here reveals considerable savings in time required for selective image encryption i.e. approximately 96ms when we evaluate with the help of FPGA compared to 720ms on a simulating platform "MATLAB". In spite of overhead on area when it comes down to programming our reconfigurable multiple-cores processor; it's possible utilization for different applications brings about new dimensions and possibilities. Still optimization for a successful and fruitful output requires us to cover all aspects, hence we need to modify our architecture and utilize FPGA block memory compared to LUTs to further reduce power constraints. The advantage of speed via reduction in time due to parallel processing has been achieved but the offset of area is a tradeoff that requires vigorous analysis covering various applications.

REFERENCES

[1] X.-H. Sun, Y. Chen , "Reevaluating Amdahl's law multi-core era",‖ J. Parallel Distribution Computing. 70 (2010) 183-188

[2] M. Hill, M. R. Marty, "Amdahl's law in the multicore era", IEEE Computer 41 (7)(2008) 33_38.

[3] Nikolaos S. Voros and Konstantinos Masselos, "System Level Design of Reconfigurable Systems-on-Chip", 1 ed, Springer, 2005.

[4] M. B. I. Reaz, F. Mohd-Yasin, S. L. Tan, H. Y. Tan and M. l. Tbrahimy, "Partial Encryption of Compressed Images Employing FPGA," Circuits and Systems. 2005. ISCAS 2005. iEEE international Symposium on, IEEE, pp. 2385-2388 Vol. 3,23-26 May 2005.

[5] Habibullah Jamal, Sheikh. M. Farhan and Shoab A Khan, "Low Power Area Efficient High Data Rate 16-bit ABS Crypto Processor," Microelectronics. 2006. ICM '06. International Cotiference on, IEEE, Dhahran, pp. 186-189, 16-19 Dec. 2006.

[6] Yi Wang and Yajun Ha, "An Area-Efficient Shuffling Scheme for AES Implementation on FPGA," Circuits and Systems (ISCAS). 2013 IEEE international Symposium on, IEEE, Beijing, pp. 2577-2580, 1923 May 2013.

[7] Angelo Barnes, Ryan Fernando, Kasuni Mettananda and Roshan Ragei, "Improving the Throughput of the AES Algorithm with Multicore Processors," Industrial and ltiformation Systems (ICIIS). 2012 7th iEEE International Conference on, IEEE, Chennai, pp. 1-6, 6-9 Aug. 2012.

[8] M. S. Azzaz, C. Tanougast, S. Sadoudi, A. Bouridane and A. Dandache, "FPGA implementation of new Real-time Image Encryption based switching chaotic systems," Signals and Systems Cotiference (ISSC 2009), lET Irish, TET, Dublin, pp. 1-6, 10-11 June 2009.

[9] Anurag Gupta, A.fandi Ahmad, Mhd Saeed Sharif, and Abbes Amira, "Rapid Prototyping of AES Encryption for Wireless Communication System on FPGA," Consumer Electronics (ISCE), 2011 IEEE 15th international Symposium on, IEEE, Singapore, pp. 571-575, 14-17 June 2011.

[10] Kuo-Huang Chang, Yi-Cheng Chen, Chung-Cheng Hsieh, Chi-Wu Huang and Chi-Jeng Chang, "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application," Circuits and Systems, 2009. ISCAS 2009. iEEE international Symposium on, IEEE, Taipei, pp. 1922-1925,24-27 May 2009.

[11] M. Lombardo, J. Carnarero, J. Valverde, J. Portilla, E. de la Torre, T. Riesgo, "Power Management Techniques in an FPGA-Based WSN Node for High Performance Applications," Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2012 7th international Workshop on, IEEE, York, pp. 1-8,9-11 July 2012.

[12] M.T. Ramirez-Torres, J. S. Murguia, and M. Mejia-Carlos, "FPGA implementation of a reconfigurable image encryption system," ReConFigurable Computing and FPGAs (ReConFig), 2014 International Cotiference on, IEEE, Cancun, pp. 1-4,8-10 Dec. 2014.

[13] Irfan Ullah, Waseem Tqbal, Dr. Asif Masood, "Selective Region Based Images Encryption," information Assurance (NCiA), 2013 2nd National Cotiference on, IEEE, Rawalpindi, pp. 125-128, 11-12 Dec. 2013.

[14] Dr. Naveenkumar S K, Panduranga H T, Kiran, "Partial Image Encryption for Smart Camera," International Conference on Recent Trends in Information Technology (lCRTlT), 2013, IEEE, Chennai, pp. 126-132,25-27 July 2013.

[15] R. K. Hiware, D. Padole, "Application Mapping Methodology for Reconfigurable Architecture", Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 1, Smart Innovation, Systems and Technologies 50, DOI 10.1007/978-3-319-30933-0_2.

[16] Anish Goel, Kaustabh Chaudhari, " FPGA implementation of a novel technique for selective image encryption", 2016, 2nd International Conference on Frontiers of Signal Processing (ICESP), 2016.

[17] R. K. Hiware, D. Padole, "Configuration Memory Based Dynamic Coarse Grained Reconfigurable Multicore Architecture for 8 Point FFT", 2015, IEEE, 7th International Conference on Emerging Trends in Engineering & Technology, IEEEDOI 10.1109/ICETET.2015.37