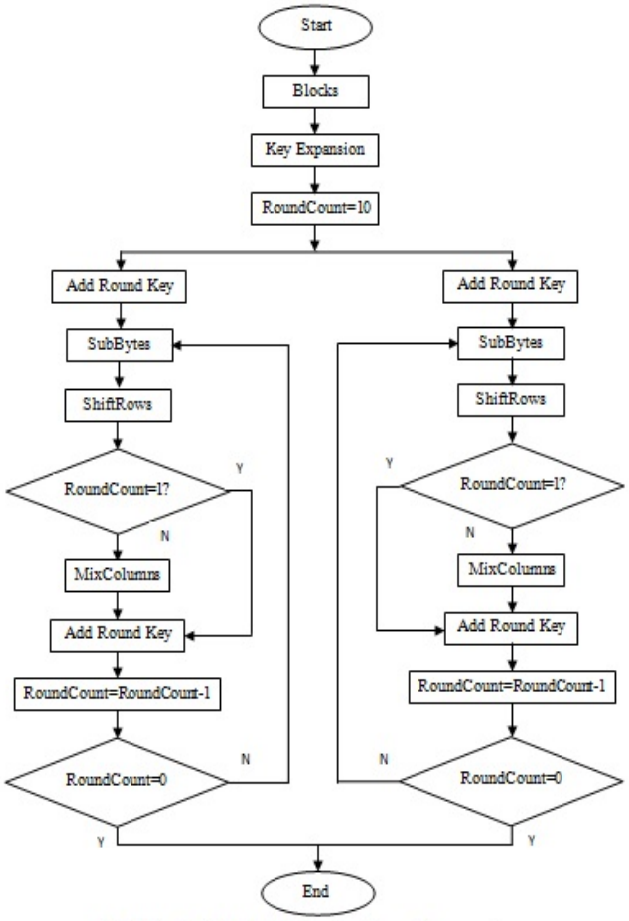

Figure 6: Flowchart of AES for Parallel Computing

According to the proposed AES algorithm for parallel computing in figure 6, we firstly store the plaintext and expanded key in the global memory space. The plaintext is then divided in blocks of 16 bytes which are encrypted completely in parallel. There are two general methods of AES computation [17]. One is the matrix computation, namely the 128-bit block is mapped into a 4*4 matrix. Then, the matrix is computed in a sequence of four stages: AddRoundKey, SubBytes, ShiftRows and MixColumns in each round. The other is the table lookup.

According to the proposed parallel AES algorithm, we firstly store the plaintext and expanded key in the global memory space. The plaintext is then divided in blocks of 16 bytes which are encrypted completely in parallel.

9. Performance Analysis and Evaluation

In this sub-section, we evaluate the performance of new AES algorithm for parallel computing that is used in a cipher system for data encryption. In our cipher system, the hardware is equipped with CPU of Intel Core 2 Duo E8200, the memory of 1GB. The software is our implementation of AES algorithm for parallel computing which runs in Windows XP. Tool used to achieve the goal is eclipse, and the language used is core java and swing.

A. Procedure Followed

Here we are showing the steps followed in order to achieve the better performance of parallel computing with the help of new AES algorithm. Figure 7 shows the window to select and compare the execution time between AES algorithm for parallel computing and sequential AES algorithm. The window contains two sections first one is for sequential AES algorithm and the second one is for AES algorithm for parallel computing. Left most column is to select file middle column will show the file size in kilobyte and after clicking the second right button of encrypt, the algorithm will encrypt the data and the time taken is shown in the rightmost column in millisecond.

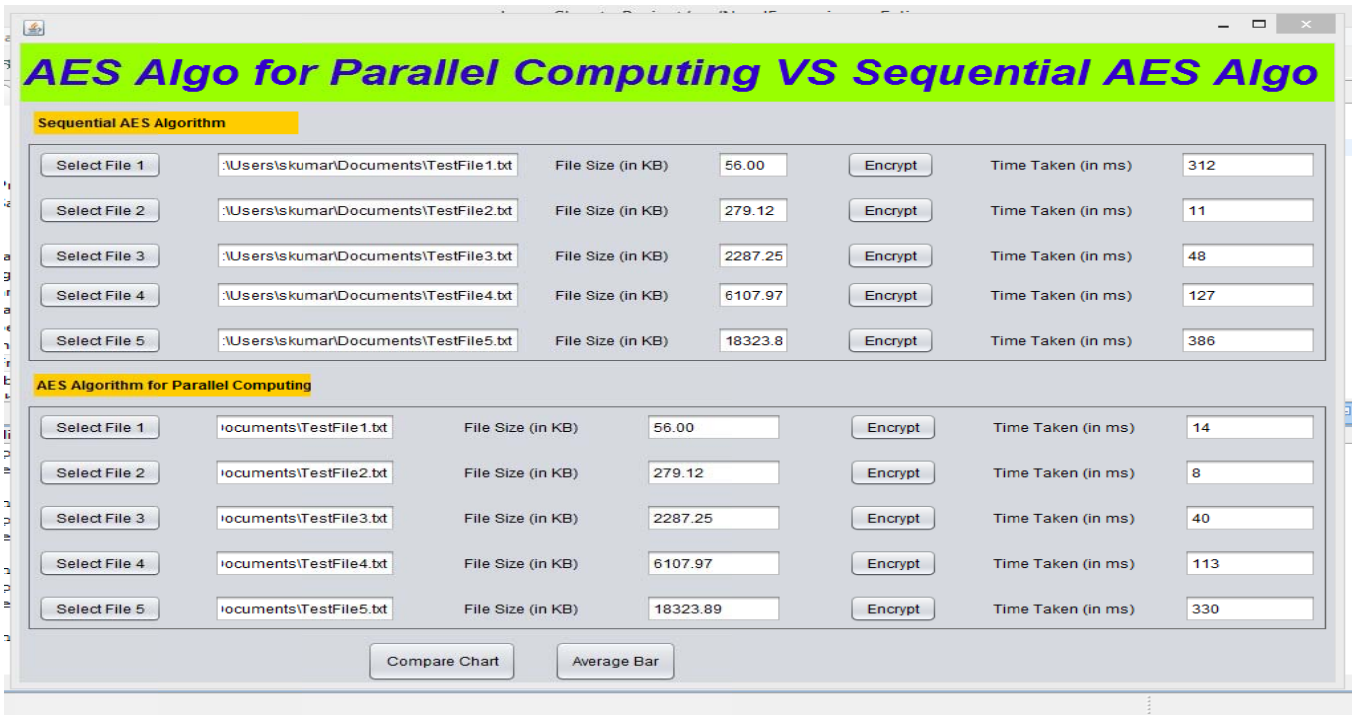

Figure 7: Time Taken for Encryption by AES for Sequential and Parallel Computing

After selecting the file and clicking the encrypt button we get the execution time, we will repeat same procedure for as much as file we want to select. Here we are selecting five files and the encryption time taken for all the five files are shown above, now the same process get repeated for AES algorithm for parallel computing.

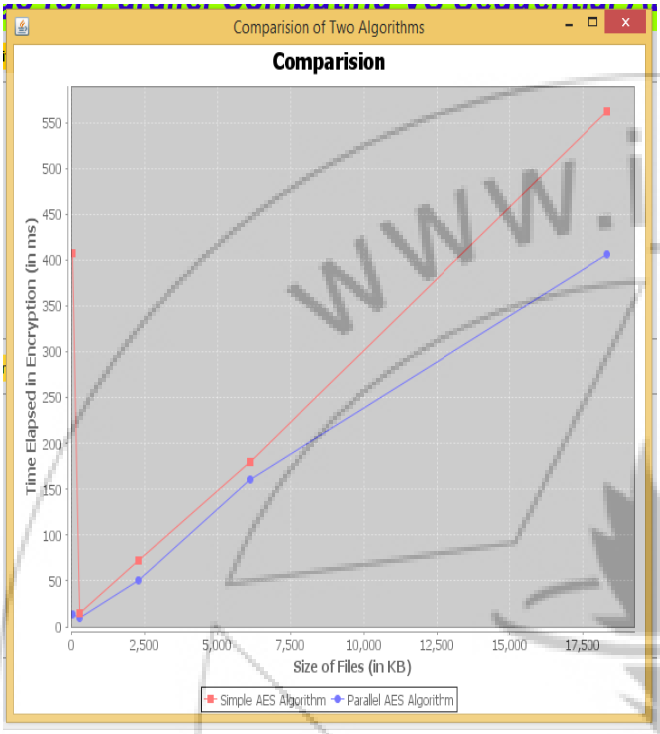

Figure 8: Comparison of Time Taken by Both Algorithms

Figure 8 illustrates the comparisons of AES encryption in terms of encryption time. In this figure, the horizontal axis indicates the size of files in terms of kilobyte (kb), the left vertical axis indicates the time in which the plaintext are encrypted into the ciphertext through AES algorithm in terms of millisecond (ms). Figure 9 is a bar graph of the overall comparison of both the algorithms for the five selected files:

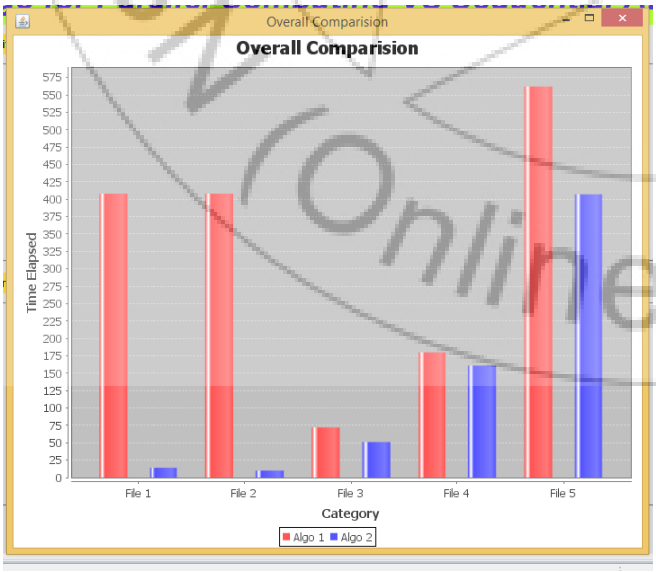

Figure 9: Overall Comparison of Both Algorithms

References

[1] N. Dunstan, "Semaphores for fair scheduling monitor conditions," SIGOPS Oper. Syst. Rev., 25(3):27–31,May 1991.
[2] M. Cole, "Algorithmic skeletons: structured management of parallel computation," MIT Press, Cambridge, MA, USA, 1991.
[3] L. Marziale, G. G. Richard III, and V. Roussev. Massive Threading: Using GPUs to Increase The Performance of Digital Forensics Tools. Digital Investigation, pp. S73-S81, 2007.
[4] Sarita V. Adve and Kourosh Gharachorloo, "Shared Memory Consistency Models: a Tutorial," IEEE Comput.,29(12):66-76, 1996.
[5] Ian Foster, "Designing and Building Parallel Programs," Addison Wesley, 1995.
[6] Murray I. Cole, "Algorithmic Skeletons: Structured Management of Parallel Computation," Pitman and MIT Press, 1989.
[7] Susanna Pelagatti, "Structured Development of Parallel Programs," Taylor & Francis, 1998.
[8] Kai Hong, "Advance Computer Architecture: Parallelism, Scalability and Programming," TMH, Edition 2001.
[9] J. Darlington, A. J. Field, P. G. Harrison, P. H. B. Kelly, D. W. N. Sharp, and Q. Wu, "Parallel Programming Using Skeleton Functions," In Proc. Conf. Parallel Architectures and Languages Europe, pages 146-160. Springer LNCS 694, 1993.
[10] National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard,", U.S. Department of Commerce, January 1977.
[11] J. Daemen, V. Rijmen. The Design of Rijndael: AES The Advanced Encryption Standard. New York, USA: Springer-Verlag, 2002.
[12] Daemon, J. and Rijmen, V. "The Rijndael Block Cipher: AES Proposal", NIST, Version 2, March 1999.
[13] Stallings, W. "Cryptography and Network Security: Principles and Practices." Third Edition, Pearson Education, Inc. 2003.
[14] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. In Proc. 2nd AES candidate conference, pp 15–34, NIST, 1999.
[15] J D. Owens, D. Luebke, N. Govindaraju et al. A Survey of General- Purpose Computation on Graphics Hardware. Computer Graphics Forum, Vol. 26, No. 1, pp. 80-113, 2007.
[16] RSA Laboratories, "The RSA Laboratories Secret-key Challenge: Cryptographic Challenges."
[17] Jaspal Subhlok, James M. Stichnoth, David R O'Hallaron, Thomas Gross, "Exploiting task and data parallelism on multicomputer," PPOPP '93 Proceedings of the fourth ACM SIGPLAN symposium on Principles and practice of parallel programming, ACM, NY, USA, 1993.