Abstract

The more rapid development in information technology, the process of exchanging images, either via internet or intranet, becomes higher and easier. On the other hand, the security in the process of exchanging images become very vital in maintaining the image confidentiality from unauthorized access. The need for confidentiality and copyright aspects that must be met. One way to protect the images from unauthorized access which may occur when delivery is by apply encryption to the images that will be transmitted. Encryption changes the content of the images become can not be read by using specific encryption algorithm. Advanced Encryption Standard (AES) is one of encryption algorithm that is quite widely used today. However, with the increasing exchange of images, is needed a way to be able to encrypt images in a relatively short time. Parallel computing is used to address the needs of high computing.

There are several things in parallelize the image encryption process, which is part of the process can be parallelized, which section is requires the longest time in the execution, and the data-cutting strategy. Part of the encryption process that can be parallelized is the part to be executed repeatedly and takes a long time. because the AES is sequential in nature, the core of AES algorithm is not parallelized, but the data is partitioned to be processed in the slave. While the master is
only in charge of sending the job that contains the task-task to be
sent to the slave and reassembling the result of each slave. In the
implementation, is used Java Parallel Programming Framework
(JPPF) and applications built on the Java programming language. In use, JPPF can run on various operating systems that
support Java.

Testing performed on several images with different
resolutions. Based on the results of testing the implementation of
parallel computing in image encryption, obtained speedup in the
image encryption process with size over 500 x 500 pixel.

Keywords: AES, job, JPPF, master, parallel, partition, slave,
task.