Uchenna Onukwue (Feb 2015)

Thesis Title: Investigating the Effects of Wavelet Filters on a Mean-Reversion Strategy

Abstract

This thesis examines the implementation of a simple mean reversion trading strategy. It further applies wavelet filters to the price data and then investigates the collective results. The closing price of high frequency and daily equity data of constituent stocks of the Dow Jones Industrial Average (DJIA) is used in our models to compare the profit potential of selected pairs at the respective sampling frequencies. The high frequency data is sampled at one minute intervals and include data for after-hours trades on all stocks. Mean reversion models are structural relationship models that rely on correction of price movements towards equilibrium.

We first implement a function to determine the underlying correlation structure of the input data and select the most correlated pair of stock. This data is then transformed using various wavelet filters to three levels of decomposition. The now transformed signals are used as input into our mean reversion model to investigate the effects of the filters at each level on the performance of the model to which they are applied. We compare our performance results to those generated by an adapted MACD based mean reversion model as well as a selection of stock market benchmark indices. We also briefly compare these performances to the performances of models based on unfiltered price data to see if any of the filter based models backtested outperformed or performed as good as the unfiltered models.

Conclusive observations show that wavelet filtered mean reversion models might be useful for practical trading as in scenarios where the wavelet filters applied generated statistically significant results as per our tests. Results of our tests indicate the potential to save on transaction costs as a result of the wavelet filter effects. The 200 period backtests generally outperform the 50 period backtests. The coiflet 1 based models generate the most statistically significant results from our backtests using daily data while the Haar based models generated the most returns on average in all sample datasets. Hence, the coiflet 1 based models are best applied for the best risk adjusted returns using daily data. The Haar based models, despite their risk profile, are the most flexible models to trade using either low or high frequency datasets or optimal model parameters; i.e. significantly profitable model parameters such as the rebalancing period (lookback) and the level of decomposition of the input signal applied to such models as per our tests.

Sandilya Narahari (expected completion: April 2017)

Thesis Title: Performance Analysis of CrypDB and Assessment of Its Readiness for Real-life Applications

Abstract

Data security breaches pose a serious threat. In recent years, an increasing number of high-profile data security breaches have made headlines. Accessibility of Internet has made online applications vulnerable to theft of sensitive information exposing the business to devastating legal ramifications. CryptDB is a Database Management System (DBMS) that claims to provide a practical solution in the face of compromised sensitive information or data leaks. It works on a number of aspects of online data protection. It allows standard SQL queries to process over encrypted database through a range of encryption schemes. These schemes by encrypting both data and queries are well suited with SQL standards and in theory are very effective in shielding the data.

There are three fundamental concepts embedded into CryptDB: an *SQL-aware encryption strategy* that maps SQL queries to appropriate encryption schemes, *adjustable query-based encryption* which allows to adjust the encryption level of each data item based on input queries and lastly "*onion layer" based encryption* which efficiently encrypts data items using different encryption schemes.

While its concept to improve database security looks fresh and interesting from an academic standpoint, this dissertation examines the usability of CryptDB in practical applications. We have therefore benchmarked the performance of CryptDB and examined how well practical applications can be adapted for the use with a CryptDB setup. Our evaluation results show that CryptDB has high overhead of about 61% and 50% for queries running from web applications and TPC-C respectively, compared to unmodified MySQL, which is two to three times more than what has been claimed by the original CryptDB promoters. Our study indicates that CryptDB has not yet been developed into an effective security technology for real-life applications. At the same time, the dissertation acknowledge the contribution by CryptDB to the research and development in seeking better and more secured solutions for large databases with sensitive data.