Correlating Time-Domain Noise to Detect Fraudulent Credit Cards

Andrew Wiens, Wenyuan Liu, Robert Morley (Advisor)

Department of Electrical and Systems Engineering

Washington University in St. Louis

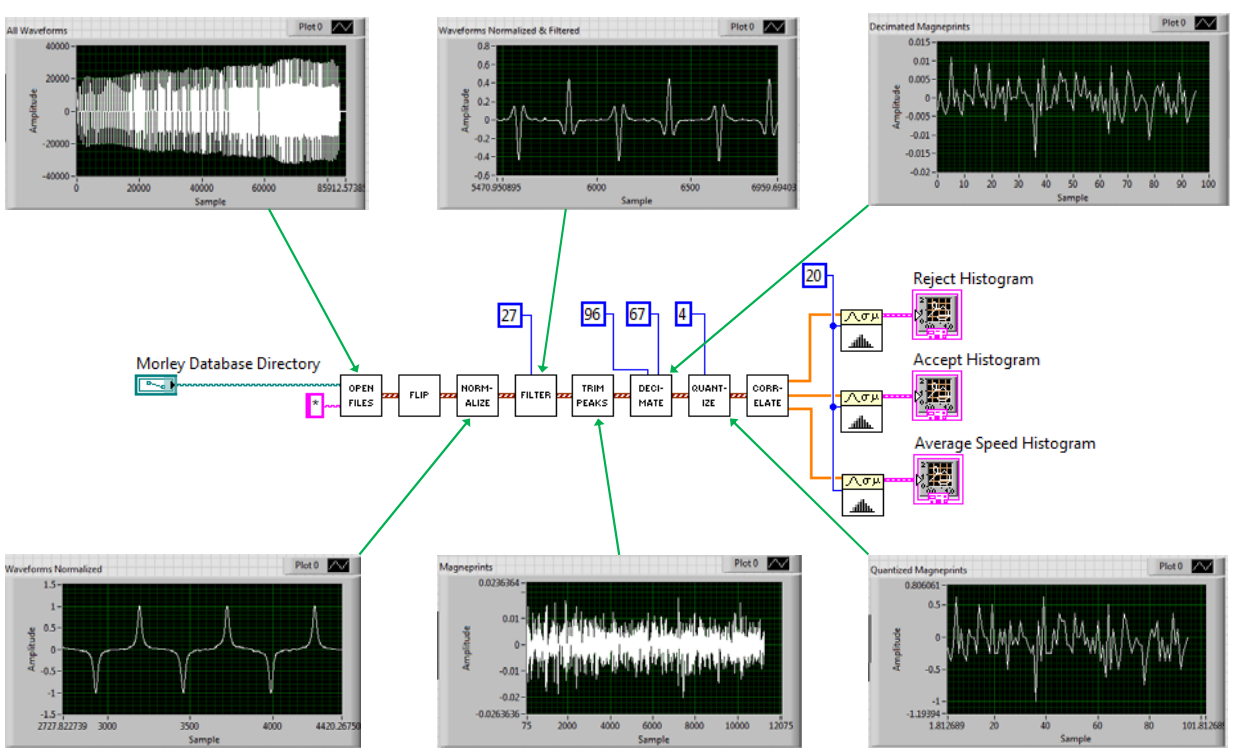
Abstract

In this project, we developed using Labview a system that detects fraudulent credit cards using the noise in-between the data on the credit cards. First, we determined the direction of the card swipe and normalized all swipes to be forwards. Then the amplitudes of the peaks were normalized to one, as well as the number of samples between adjacent data peaks to 266(zeros) and 133(ones). The normalized waveform is then high pass filtered with a FIR moving average filter and then broken up from peak to peak. 64 samples were taken in-between the peaks among the 266 samples (only from zeroes). Then we formed a Magneprint™ of the card by decimating, quantizing, and choosing a subset of the samples. We found that for a small Magneprint™ size of 384 bits in an effort minimize cost, we achieved excellent results in determining fraudulent cards.

Problem

- Need a system to create a fingerprint profile of each individual card.
- The fingerprint must be unique for each card, even for cards with identical data.
- Fraudulent counterfeits can then be identified when their Magneprints™ are compared to the authentic card.
- System must be robust, consistent, and reliable, with minimal rates of false positives and false negatives.

Design



Results

Iterated through various values of:
•Filter Length
•Delta, distance between samples
•M, number of samples taken
•B, quantization of samples
to get the best separation, S, between accept and reject distributions in order to minimize the rate of false positives and false negatives.

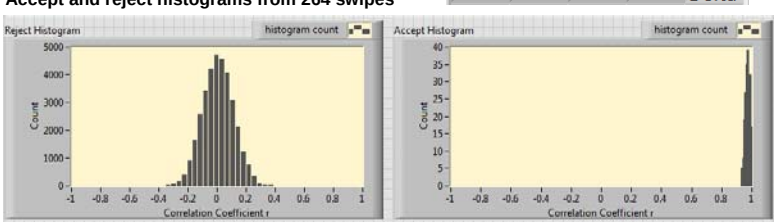
$$S = \mu_A - 3\sigma_A - 3\sigma_R$$

Best parameters, as determined from a database of 264 swipes

Results

384	768	1024	2048	Total
96	192	256	512	M
4	4	4	4	B
0.642227	0.725985	0.751830	0.799264	S
17	17	17	17	Filter
89	52	35	20	Delta

Accept and reject histograms from 264 swipes



Conclusions and Future Work

- For a Magneprint™ size of 384 bits, the best parameters were: Filter length=17, M=96, Delta=89, B=4 in order to eliminate false positives and false negatives.
- Our system achieved a maximum separation of 0.799
- Live swiping of cards confirmed working system, which was able to identify authentic and fraudulent cards.
- The system is very robust and reliable.
- Future areas of exploration include hardware implementation of the system, optimizing cost vs robustness for commercial use, and commercial testing.
- Our design is an accurate way to distinguish authentic cards from copied cards.
- Our implementation could use less computing time and memory by processing the cards on the fly.

References

- "Method and apparatus for authenticating a magnetic fingerprint signal using a filter capable of isolating a remanent noise related signal component," with R. E. Morley, R. S. DeLand, E. C. Limtao, E. J. Richter, and S. R. Wood U.S. Patent No. 7,478,751, January 20, 2009
- "Magnetic stripe card verification system," with T. C. McGeary and R. S. DeLand, Jr. U.S. Patent No. 6,098,881, August 8, 2000.