Designing a System For Authenticating a Magnetic Fingerprint Signal

Andrew Cowley and Jason Binder

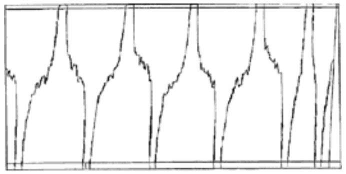
Abstract

A large amount of credit card fraud that occurs every year results from the copying of an authentic card's data to a skim card. One method for preventing this fraud is to design a system with the ability to dynamically differentiate between two unique cards regardless of the binary information encoded on them. Due to the imperfect alignment of ferromagnetic particles in a magnetic stripe, each magnetic strip card contains a unique, data-independent fingerprint (MagnePrint™) that may be detected with a card reader and used for authentication. We successfully designed a system to store card swipes in a database, extract the MagnePrint™ from each swipe, and correlate these MagnePrints™ together in order to determine the authenticity of a given swipe.

Introduction

Magnetic Stripe Card Swipe Basics

The stripes on cards are composed of ferromagnetic rods fixed in a resin. Data is encoded on the card by changing the polarity of the rods at specific points along the card. During a swipe, the time-varying magnetic field from the polarity shifting of the rods at an inductive read head yields an electric signal with an amplitude proportional to the density of the rods and to the swipe speed. Ideally, all of these rods are perfectly aligned with the length of the magnetic stripe, meaning a switch in polarity would yield an electrical data signal with maximum amplitude. However, the rods are not perfectly aligned with the length of the magnetic stripe, yielding a small signal embedded within the data signal. This small signal causes the amplitude of the data signal to vary from ideal at a greater frequency than the data signal. From the literature, we know that this small signal is at about -40dB relative to the data signal, and has an amplitude of about 20μV$_{pk}$/IPS. This small signal is unique to each magnetic stripe and is independent of the encoded data, thus it may be used for card authentication. Any given card may be authenticated by correlating the small signal, extracted at the point of sale, with its MagnePrint™, extracted by the card manufacturer and stored in a secure database.



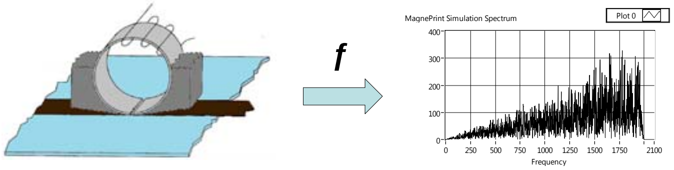
Electric data signal with embedded MagnePrint™

The Software and Hardware Used

The simulations and data collection were all coded using LabVIEW. The swipe signals were collected using a magnetic stripe card reader, and amplifier circuit, and the Elvis II Prototyping Board.

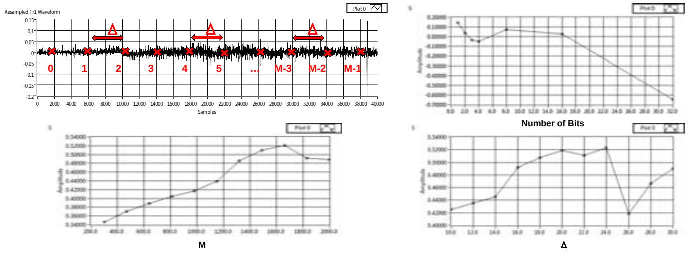
Methods

MagnePrint™ Simulations

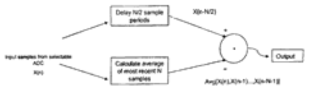


Spatial sensitivity of read head yields band-limited, high-pass filter

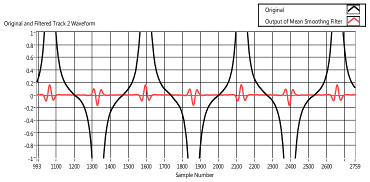
Track 1 Data MagnePrint™ Collection and Analysis

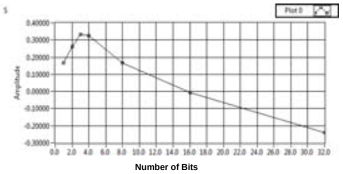


Track 2 Data MagnePrint™ Collection and Analysis

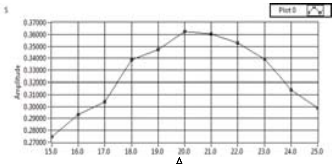

Delay N/2 sample periods
X(n-N/2)
Input samples from selectable ADC
X(n)
Calculate average of most recent N samples
+
-
Avg[X(n),X(n-1)...X(n-N-1)]
Output

Mean Smoothing Filter used to extract MagnePrint from center of zero bits (N = 33)

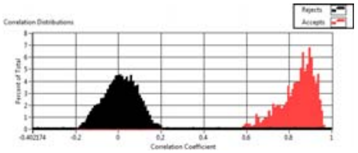




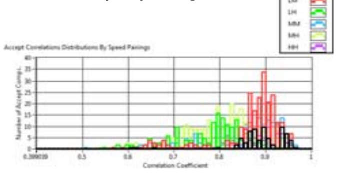
The Separation with a Δ of 20 and 384 total bits per MagnePrint™



The Separation with 3 bits per sample and 128 total samples per MagnePrint™



Correlation distributions for M = 128, Delta = 20, and 3 bits per sample



Accept correlation distributions based on the swipe speeds of the correlated MagnePrints™

Results

We ran a variety of tests to determine the optimal value of the following parameters when generating and analyzing MagnePrints™: The number of bits per sample (numBits), the spacing between samples (Δ), and the total number of samples per MagnePrint™ (M). The separation (S) is defined as $\mu_A - 3\sigma_A - 3\sigma_R$. The results are summarized in the table below:

Parameter	Track 1 (384 bits)	Track 1 (No Constraints)	Track 2 (384 bits)	Track 2 (No Constraints)
Δ	20	24	20	20
M (# of Samples)	384	1650	128	300
numBits	1	8	3	32
μ_A	0.734	0.910	0.834	0.857
σ_A	0.131	0.07	0.086	0.104
σ_R	0.004	0.059	0.082	0.054
Separation (S)	0.15	0.423	0.331	0.37

Future Directions

Other modifications should be done to make the system commercially viable. To help test the system, we treated the forward and backward swipes of each card as two different cards. This was possible because the MagnePrint™ of a backward swipe is flipped, and therefore correlates with the corresponding forward swipe to zero, as would two different cards. In a real-world application, the MagnePrint™ for a backward swipe should be flipped in time so that the swipe direction has no effect on the authentication process. Another necessity to implement the system commercially is to create a server to store the MagnePrints™ associated with each card, as opposed to storing the data locally. Finally, the sampling speed of card reader ADC should be increased to allow for swipes with speeds greater than 40 IPS to be accurately recorded and processed.

Literature Cited

1. Morley, Jr. et al. Method and Apparatus For Authentication a Magnetic Fingerprint Signal Using a Filter Capable of Isolating a Remnant Noise Related Signal Component. U.S. Patent 7,478,751 B2, filed December 17, 2004, and issued January 20, 2009.

Acknowledgements

We would like to both acknowledge and thank Professor Morley for assisting us with this research project by providing both the necessary equipment, as well as guidance.