

Washington University in St. Louis
School of Engineering and Applied Science
Electrical and Systems Engineering Department

ESE498

Authentication of Magnetic Media

By

Calvin Murdock
Saroj Hyoju

Supervisor

Dr. Robert Morley

*Submitted in Partial Fulfillment of the Requirement for the BSEE
Degree,
Electrical and Systems Engineering Department, School of
Engineering and Applied Science,
Washington University in St. Louis*

May 2013

ABSTRACT

The main objective of the project is to design a system that authenticates magnetic media, namely credit cards. During the design process, we simulated magnetic remnant noise as band limited, differentiated white Gaussian noise and investigated the effect on the correlation distributions of both legitimate and counterfeit card swipes of various parameters, including sample size, sample spacing and sample quantization: the number of bits allocated to each measurement. In general, we found that the standard deviation of reject correlations is a function of sample size and sample spacing, but is largely unaffected by quantization. We then constructed a database of real magnetic card swipes and analyzed the correlations for a variety of parameters under varying memory constraints. By comparing the Gaussian separations and the areas under Receiver Operating Characteristic (ROC) curves of the resulting accept and reject correlation distributions, we justified engineering choices that optimize system performance. Specifically, the best performance was found to occur using the maximum memory size of 256 bytes with a sample quantization of 7 bits per sample, a total of 292 samples, and a sample separation of 35.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude and humble appreciation to Prof. Robert Morley for providing the opportunity to work on this design and his supervision, guidance, and helpful feedback through the project process.

Table of Contents

Abstract	2
Acknowledgement	2
Introduction.....	4
Concept Synthesis	5
Project Specifications	9
Engineering Analysis and presentation.....	10
Results.....	18
Conclusion.....	26
References	27

INTRODUCTION

In this modern commercial era, identity theft and counterfeiting of magnetic stripe credit and debit cards have been prominent and critical issues. Despite their convenience and various means of protection and usage monitoring, consumers have been regular victims of such fraudulent activities. Credit/debit card information can be unknowingly stolen by waiters/waitress, clerks, and even from ATMs and gas pumps. Most importantly, counterfeit cards using this information can be created resulting into great monetary loss in financial sectors. Tremendous sums of money have been stolen around the world, creating financial instability among various banks and institutions.

In this situation, there is an urgency to help eliminate such fraudulent activities. In order to provide safe and reliable means of transaction to consumers, we propose a long-term solution for this problem through a robust card authentication system. Our design is economically feasible since it would only require a simple verification during the transaction process. This is accomplished through a “magnetic fingerprint” that is uniquely inherent in all magnetic media. By comparing this information with legitimate data stored in a secure database, merchants can simply detect and decline counterfeit card charges, thus wiping out this form of fraud around the world.

All magnetic media have properties that depend only on unique abnormalities in the microstructure of the material, and can thus be compared to a human fingerprint. This “magnetic fingerprint” (or “MagneprintTM”) can be modeled as band-limited, differentiated white noise. Although personal information can be easily stolen through available card copying devices, the magnetic fingerprint cannot. This provides a deterministic method for differentiating between authentic and counterfeit cards. In the following sections, we describe the design considerations and experiments that we performed to evaluate the feasibility and effectiveness of this approach.

CONCEPT SYNTHESIS

Previous Work:

Our current design of “card authentication system” drew upon our analyses and reviews of patent documents as suggested by Prof. Morley covering areas of signal processing, probability theory and modern electronics. From one of the patents, we identified that “relatively flat” portion located between magnetic flux reversals, as shown in Figure 1, serves as a basis to authenticate various magnetic media since they are virtually unique for each magnetic stripe [1]. The magnified portion of this signal is shown in Figure 2.

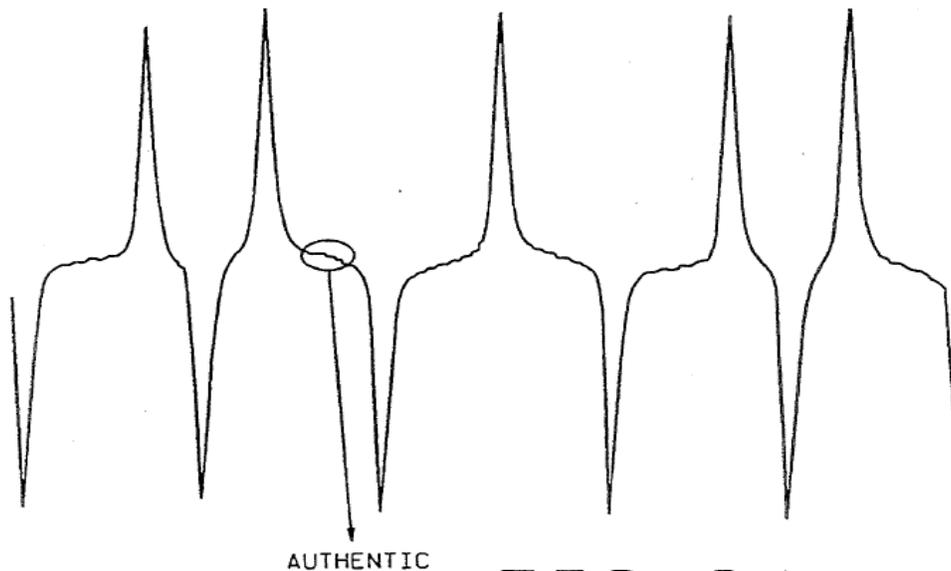


Figure 1: Signal representation of magnetic data transition [2]

As justified from one of the patents, these noise components are instead deterministic and repeatable, depending entirely on the head-medium position and physical microstructure of the card itself [1]. The card could be DC saturated to measure its remanent/remaining noise. As referred to Figure 1, two adjacent peaks represent magnetic flux reversals (N to S or vice-versa) and may represent a data. Data in the form of bits are encoded in magnetic stripes bearing card such a way that a bit “0” contains two peaks whereas bit “1” contains three peaks if we considering equal time intervals of a normalized waveform, i.e., waveform taken at a constant

speed. This type of data encoding is performed in magnetic stripe bearing medium/card by the process known as “F2F” encoding.

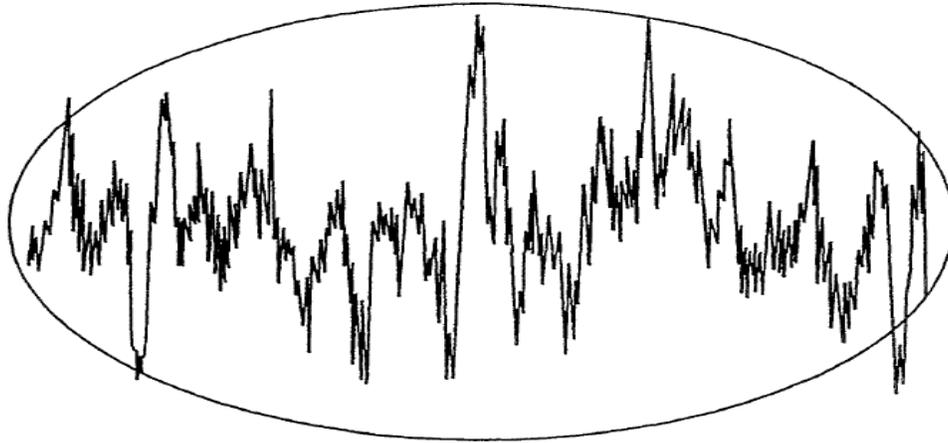


Figure 2: Magnified view of the noise signal between flux reversals [2]

For a typical inductive readhead, data-bearing signal has amplitude of 2 mV per IPS, whereas the remanent noise signal ranges from 1 μ V to 40 μ V per IPS [3]. The remanent noise signal between data transition is amplified by compressive amplifier such that data-bearing signal and remanent noise signal becomes more or less similar in amplitude, helping to analyze noise signal for authenticity of the medium. The repeatable remanent noise characteristic signals for the magnetic medium are selected from defined areas of a digitally recorded magnetic stripe. Figure 3 represents the top-level block diagram of an actual invention of authentication system as referenced from U.S. patent 7,478,751 B2. The system includes a sensing unit in the form of read head, which reads the magnetic stripe of a card producing analog signals containing signal indicative of a card data and remanent noise characteristic signal. The analog signals are then amplified by above discussed compressive amplifier, passed to a selectable ADC for digital conversion process. The ADC output is then fed to the data extraction circuit, where swipe speed and peak locations are determined. This information is provided to the controller and then to high-pass filter.

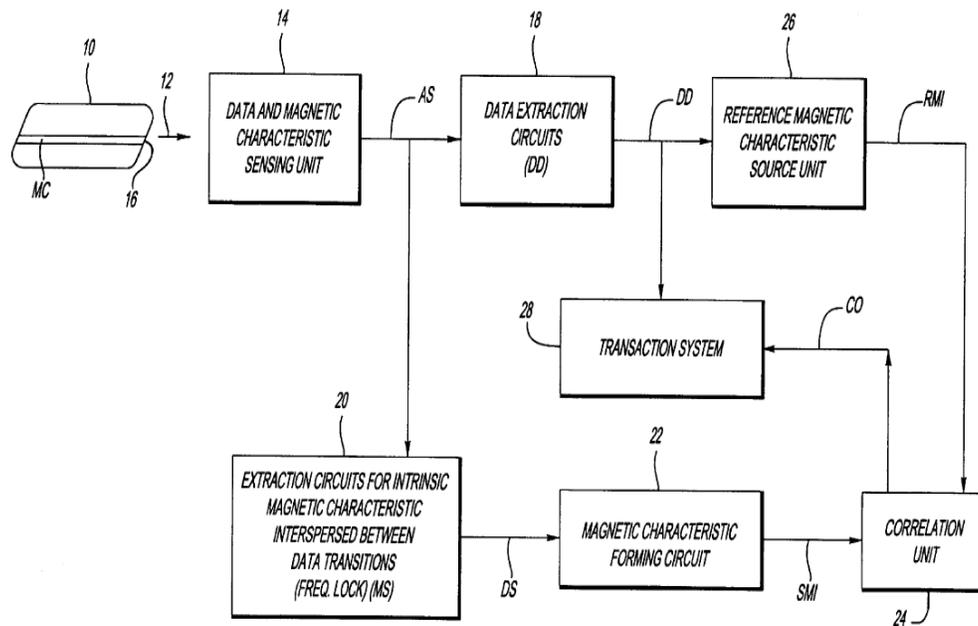


Figure 3: Block diagram of a card authentication system of an actual invention [3]

The filter passes relatively flat portions indicative of remanent noise components so that its output is received by authentication extraction unit. Here, the selected samples group of noise components are scaled, encrypted and then combined with card data with the help of data combiner for later transmitting to a transaction unit. The transaction unit which can be in the bank receives the encrypted samples and card data, then compares samples of the remanent noise characteristic with reference Magneprint™. The reference Magneprint™ is obtained at the time of card issuance. The transaction unit internally performs comparison between the card data with the reference Magneprint™ by correlation function. The resulting correlation is compared with the correlation threshold to either approve or reject the transaction and thereby indicate if the card is authentic.

Concept Generation and Reduction:

The key concept behind the current system design was to understand the relationship between the waveform expressed in time domain and spatial domain as shown below:

$$\frac{\text{Samples}}{\text{inch}} * \frac{\text{inch}}{\text{seconds}} = \frac{\text{Samples}}{\text{seconds}}$$

The relationship shown above allows us to express the sampling frequency (time domain) in the form of spatial sampling density (spatial domain) under normalized swipe speed, i.e. 1 inch per second. Since the spatial sampling frequency is fixed for a card, sampling frequency is directly related to the swipe speed. In addition, amplitude of the analog signal is directly related to the swipe speed from Faraday's law.

As discussed during the lecture, transfer characteristic of the system's read head is associated with its air gap, assumed to be 0.0005 inches. In spatial domain, the air gap of the read head can be modeled as a rectangular waveform with window equal to its aperture size. The frequency response is a Sinc function, where zero averages occurs at integer multiples of 0.0005" . The first null occurs at 0.0005"=2000 cycles/inch, indicating system's bandwidth to be 2000 cycles/inch. However, we observed that there are approximately 8-10 cycles per bit that can be distinguished from the electrical noise in the signal. Since there are 75 bits per inch, we employed a low-pass filter with a corner frequency of 750 cycles/inch.

Similar to the patent discussed above, our design method comprised methodology to evaluate relationship between different swipes of a same card and for different cards. According to preliminary analysis of sinusoidal waves, we found that even a small amount of phase discrepancy results in a significant decrease in correlation. More specifically, a phase difference of only 7% of signal wavelength results in a correlation of less than 0.9. This accentuates the need for an extremely accurate method of localizing samples. We chose to equate forward and reverse swipes of the same card by reversing and negating every reverse swipe signal. This causes slight discrepancies in the sample localizations, which result in small phase shifts and cause the accept correlations between forward and reverse swipes to be somewhat lower, as described in the results sections.

Because we normalize the sample values before computing their correlation and the signal voltages are approximately 50 times greater than the remnant magnetic noise, the data could

significantly affect the correlation results. Thus, a method for removing this dependency is necessary. We explored thresholding in order to extract samples only from low-voltage regions. However, because the voltage levels depend on swipe speed, this region of interest can change and results in inconsistent sample localization. Instead, we don't consider samples within a fixed range around each data peak location. Since these are independent of swipe speed, this is a much more reliable method. Even within this restricted region, there is still some data dependence, so we extract the residuals from a simple linear fit to remove any data bias.

PROJECT SPECIFICATIONS

In order to make use of this magnetic remnant noise for authentication purposes, the following criteria were taken into consideration.

1. Information extracted from authentic card swipes should be highly correlated while counterfeit swipes should have low correlation with a mean of zero. This allows for a deterministic threshold in correlation with a single reference for accurately distinguishing between authentic and counterfeit card swipes.
2. The accept (authentic) and reject (counterfeit) swipe correlation distributions should have low variance in order to maximize the margin around the decision threshold. This can be evaluated quantitatively by computing the Gaussian separation of the two distributions, which is defined to be $S = \mu_A - 3 * \sigma_A - 3 * \sigma_R$.
3. The probability of correctly accepting legitimate card swipes is high and the probability of incorrectly accepting counterfeit card swipes is low. This can be evaluated quantitatively by comparing the area under Receiver Operating Characteristic (ROC) curves.
4. MagneprintTM samples should be consistently taken from the same location on the card and the extracted information should be unaffected by swipe acceleration and card data. This will ensure consistent correlation results.
5. Memory usage should be as low as possible.

There are three independent variables that influence the performance of our system: B , the number of bits that we allocate to each MagneprintTM sample, Δ , the physical spacing of the

samples along the magnetic strip, and M , the total number of samples that are retained. The total memory requirement is thus $B \cdot M$. In the results section, we compare the system performance (as measured by the distribution separation and area under the ROC curve) for a variety of values under different memory restrictions. Other design choices are described in detail in the next section.

ENGINEERING ANALYSIS AND PRESENTATION

The initial approach in designing our system included modeling and simulation of random and repeatable magnetic noise in LabVIEW. We generated high-density random samples represented by band-limited, differentiated white Gaussian noise in order to model the characteristic of system's read head. This simulated the magnetic remnant noise of a card with a sample density of 20K samples per inch. The simulated MagneprintTM was then obtained by selecting M samples, each separated by Δ samples, quantized to B bits. To analyze the expected effects of these independent variables, we computed the MagneprintTM correlations between C randomly generated cards. The standard deviation of the resulting reject distribution was obtained for different Δ values to investigate the effect of sample spacing towards the distribution. In addition, effects of varying M and B (number of bits to represent a MagneprintTM sample) to the standard deviation of the reject distribution were examined. Simulation results are shown in the following section.

The block diagram in Figure 4 below summarizes our experimental authentication system. The input is a magnetic stripe bearing analog signals which are sampled and digitized by the ELVIS II ADC. Using the locations of the data peaks as landmarks, this signal is resampled to a constant swipe speed of 266 samples per bit, or approximately 1 inch per second, and warped so that it can be represented in spatial coordinates independent of swipe direction, speed, and acceleration. A low-pass filter extracts approximately 10 cycles per bit of characteristic magnetic remnant noise. We exclude data within 100 samples of peaks, resulting in 65 total samples at the center of each "0" bit. Within this small region, we assume that the underlying data trend is linear and extract unbiased samples from the residuals of a linear fit, which aligns them horizontally removing any additional data dependence. To avoid any spikes in voltage that could affect the

correlation normalization, we clip the resulting signal between -0.4 and 0.4 volts. Finally, we extract M samples each quantized to B bits and separated by Δ samples to form an authentic “Magneprint™” identifier, which is stored in the database. Successive swipes are correlated with this reference and an acceptance decision is made based on a predetermined threshold. Experimental results are shown in the following section.

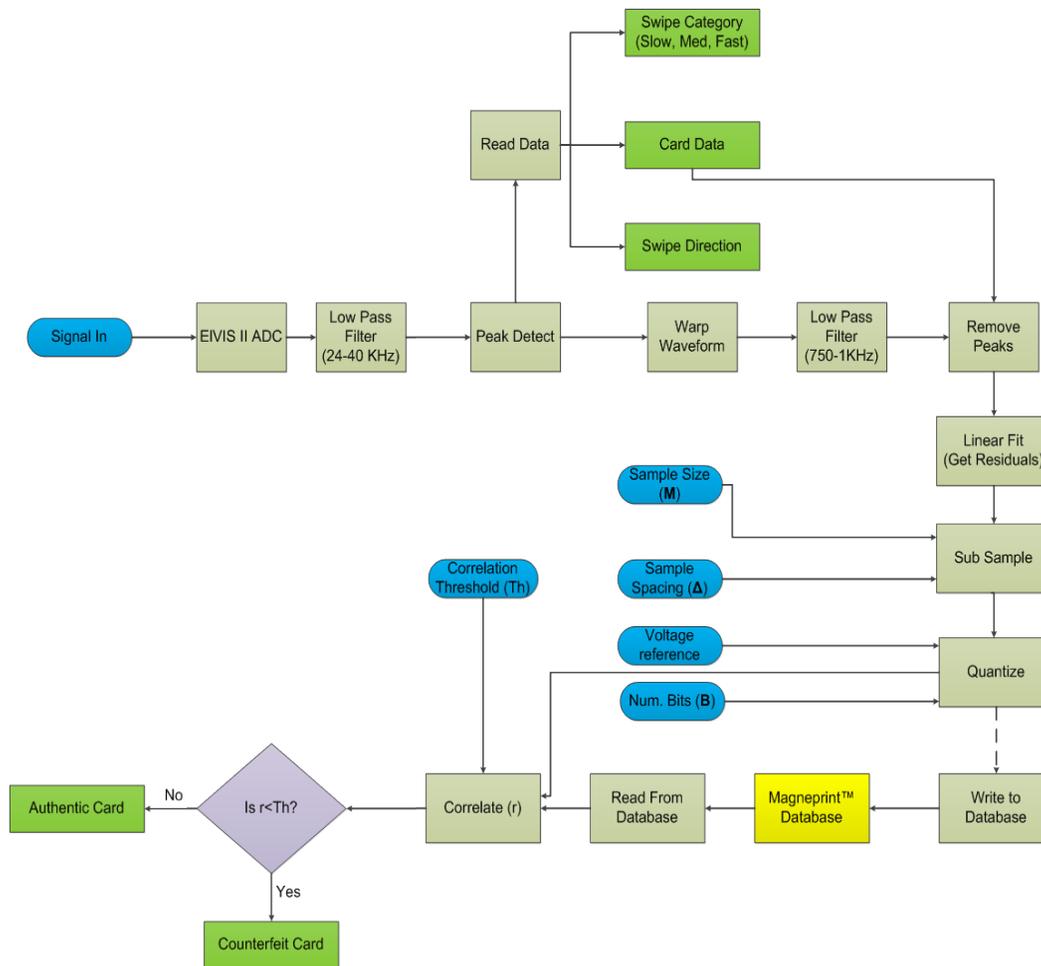


Figure 4: Block diagram of our card authentication system

Figure 5 and 6 combined show the top level of our LabVIEW wiring diagram. First, if the “Database Initialize” mode is selected, the correlation distributions and the Magneprint™ storage array is automatically populated from saved swipes using either track 1 or 2. Then, if “Live Mode” is selected, new swipes will be acquired, which are subsequently processed and

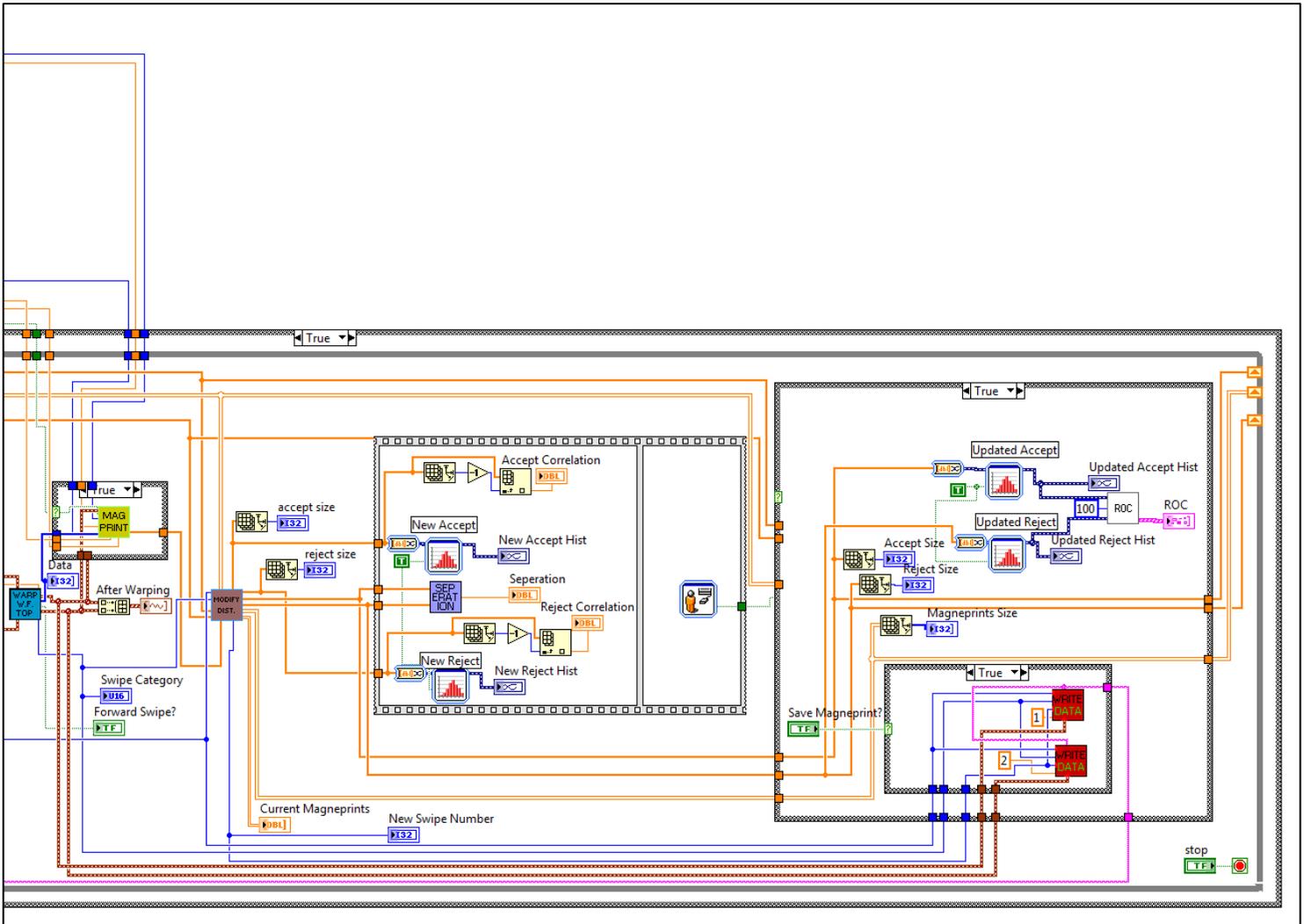


Figure 6: Wiring diagram of the top level VI (continued from Figure 5)

The majority of processing is done in the “Warp” and “Create Magneprint” VI’s, as shown in Figures 9, 10 and 11. In order to ensure that forward and reverse swipes are as consistent as possible, we detect the swipe direction and, if necessary, flip the reversed waveform (shown in Figure 7) and then warp it again. This is shown in Figure 8. The process to actually warp the waveform is performed in a sub VI as shown in Figure 9 and 10 combined. First, we detect peak locations using the built-in VI from the absolute value of the input waveform. Then, we use the distance between these peaks to determine if they belong to a “0” or “1” bit. In order to initialize the expected bit sizes, we assume that the data starts with a certain number of “0” bits. To account for swipe acceleration, we repeatedly update the expected bit

size. We then resample each bit to contain 266 samples and concatenate them, beginning two “0” bits before the first “1” bit, and adjust the sample spacing to be in physical units. Finally, the data is read and the swipe detection is determined based on magnetic strip data specifications.

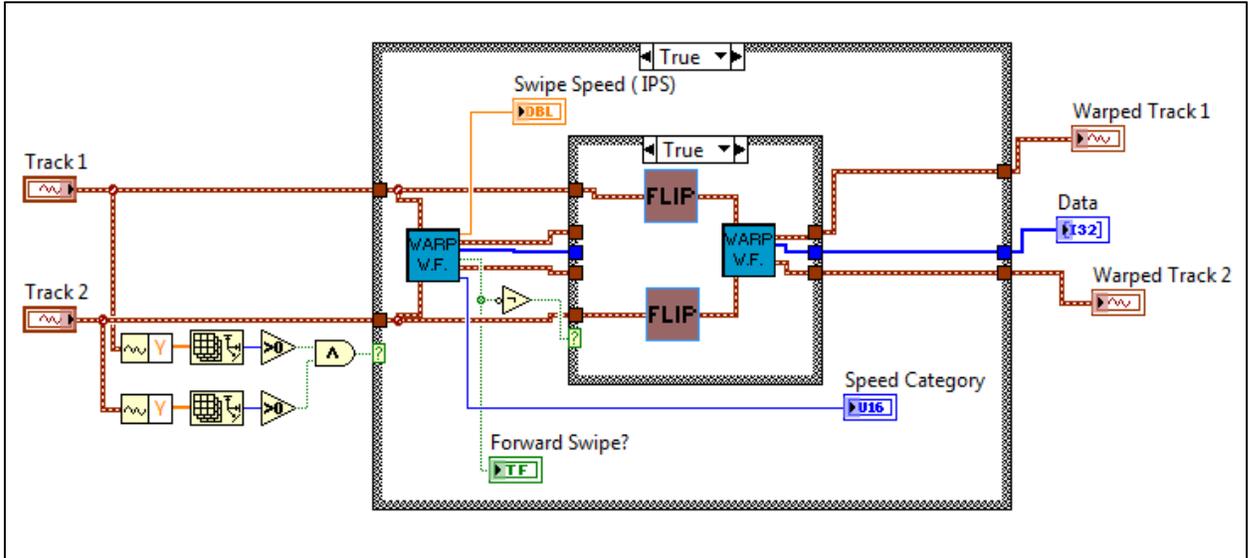


Figure 7: Wiring diagram showing top level Warp Waveform compensating for swipe direction

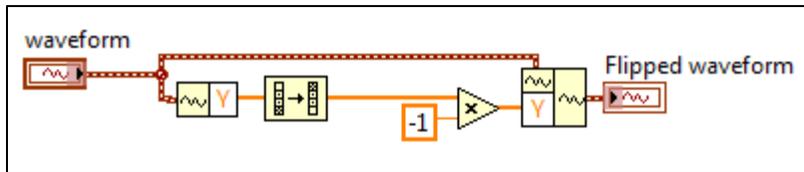


Figure 8: Functional code running behind FLIP sub VI

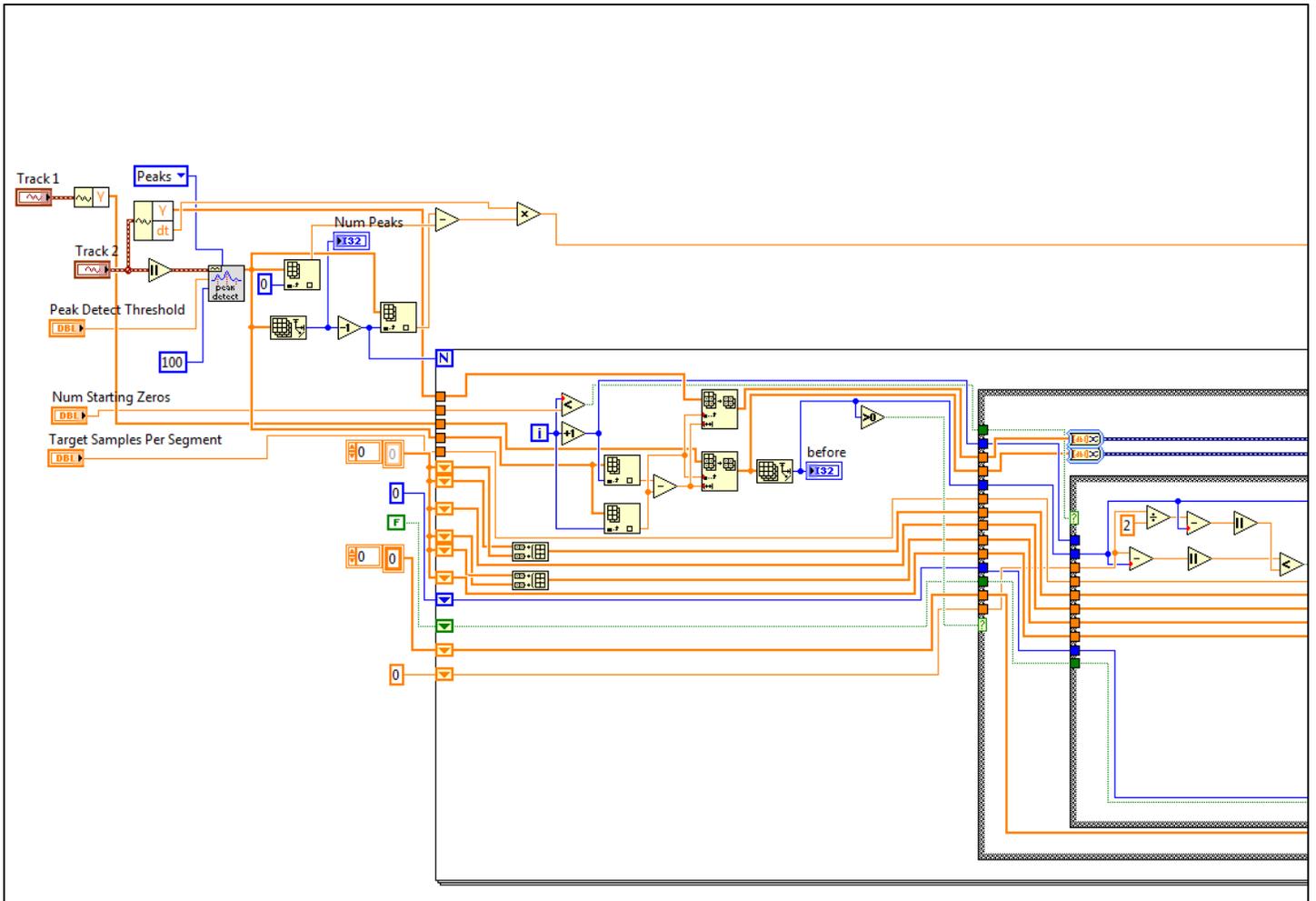


Figure 9: Wiring diagram of Warp Waveform subVI (continued in Figure 10)

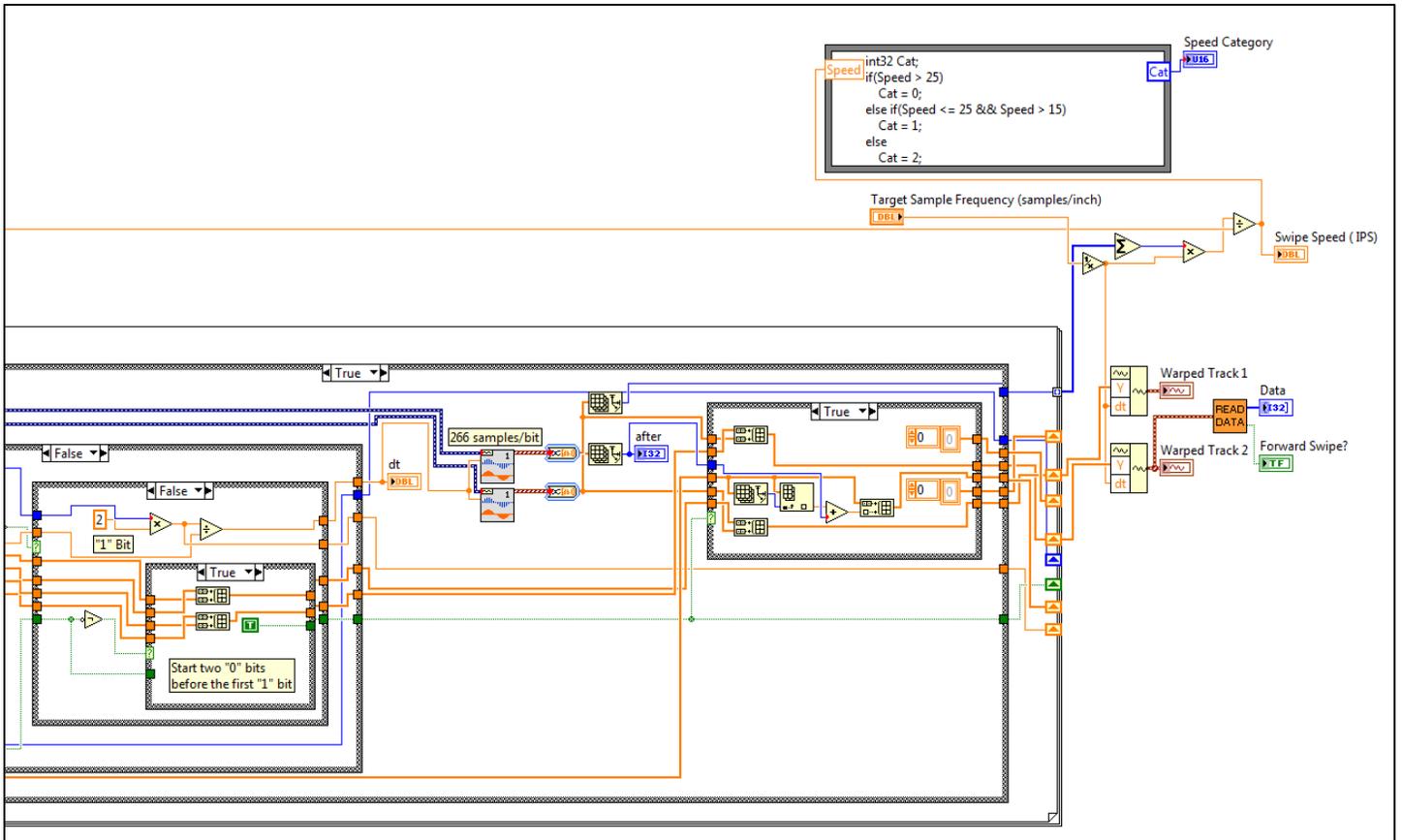


Figure 10: Wiring diagram of Warp Waveform subVI (continued from Figure 9)

The warped waveform is then passed to “Create Waveform,” as shown in Figure 11. If the Magneprint™ is to be extracted from track 2, the waveform is adjusted to remove data dependence (Figure 12) by removing samples around the peak locations, which are recalculated from the extracted data, and extracting residuals from a linear fit of the remaining data sections. Then, the data is subsampled to M total samples with a spacing of Δ and quantized to B bits after to the maximum reference voltage, which was set to be 0.4.

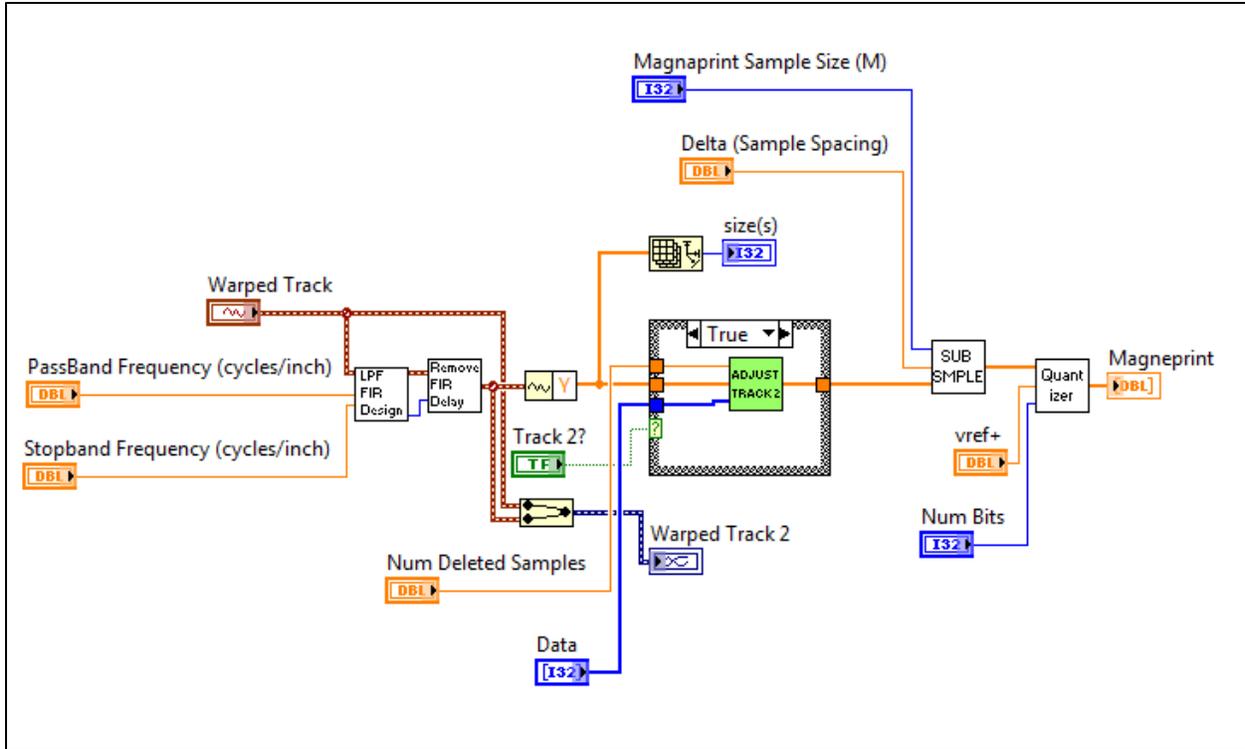


Figure 11: Wiring diagram of Create Magneprint VI

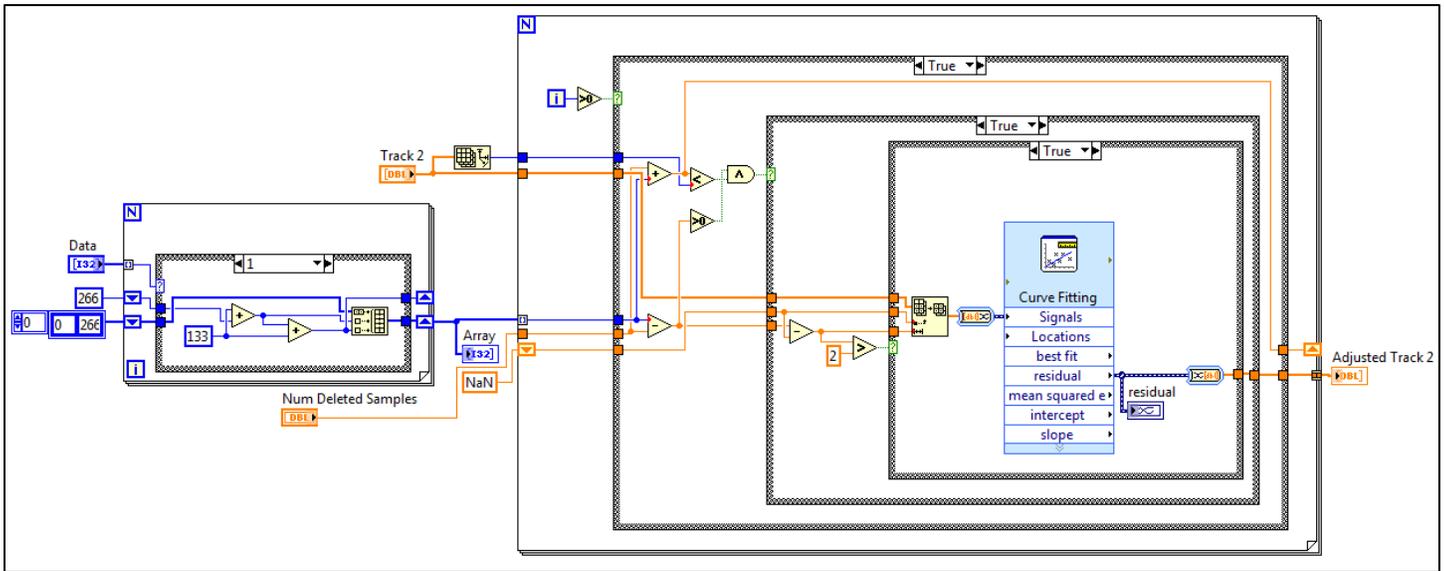


Figure 12: Functional code running behind Adjust Track 2 subVI

Bill of Materials:

S.No	Component Name	Part Number	Manufacturer	Price per 1000 units	URL
1	5-15 V Bi-directional Swipe Card Reader	21088061	Magtek Corp., CA	\$ 125,000	https://www.magtek.com/shop/fullSize.aspx#w=700

Hazards and Failure Analysis:

Since the system operates at low voltage DC (5-15 VDC), the system is less likely to cause any electrical shocks or hazards. It complies with Part 15 of FCC rules; therefore, operation of the device may not cause harmful interference and may accept any interference. Lastly, the device is plastic insulated; therefore, it is less likely to catch fire. However, we suggest not recycling the product because it cannot be decomposed.

RESULTS

Figures 13 through 15 show results from our simulation of a band-limited magnetic noise that we performed before actually taking real card swipes. Since the simulation involved generating different random cards, it was wise for us to examine standard deviation of reject distribution as a function of Magneprint™ sample size (M), samples spacing (delta) and bits per sample (B). From our analysis of the simulation results, we concluded that standard deviation reduces with increase in sample size (by factor of square root of n) but does not have any effect with bits per sample. In addition, as from the Figure 13, standard deviation decreases with increase in sample spacing but saturates after certain delta. For a fixed sample size, samples that are far apart from each other can be well distinguish from each other compared to when they closer. This analogy convinced us that far apart samples will more likely to be distinguished as different cards, thus results in tighter reject distribution, decrease in standard deviation of reject distribution.

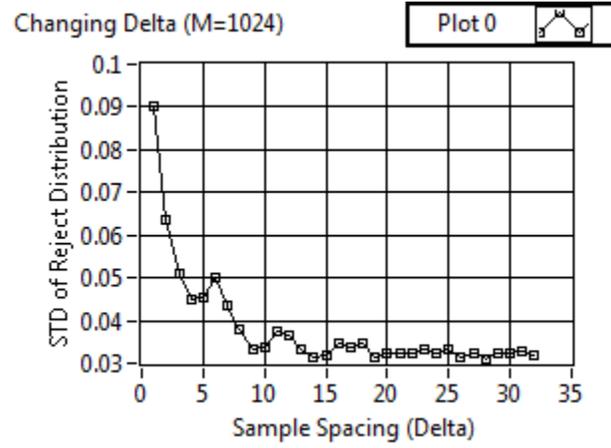


Figure 13: Reject. STD Dev as a function of Sample Spacing

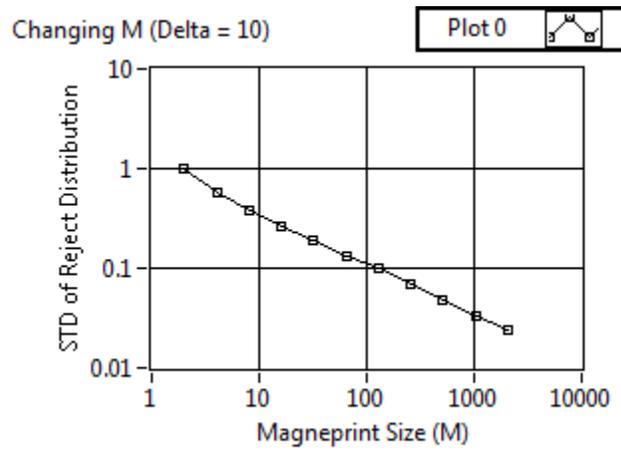


Figure 14: Reject. STD Dev as a function of Sample Size (M)

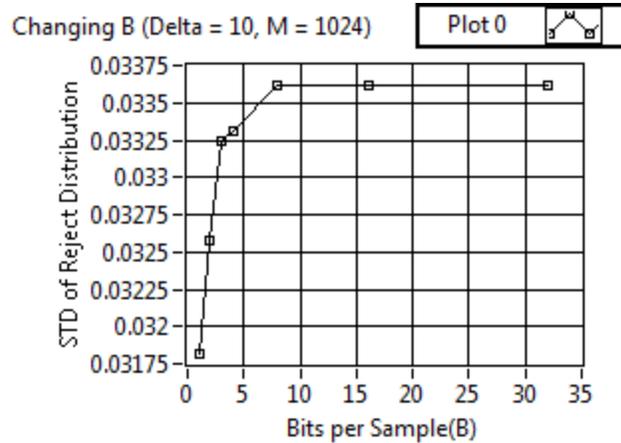


Figure 15: Reject standard deviation as a function of quantization bits per Sample

In order to evaluate effectiveness of our system, we began by creating a database to record all the swipes, which consists of approximately 20 swipes (10 forward and 10 reverse) from 11 cards, including credit cards and campus cards. Various cards were used to investigate real model of our system performance. We plotted accept and reject histograms of correlation coefficient for four different memory sizes which potentially could represent MagneprintTM size in database ($M*B$). Our choice of Δ maximized sample spacing between samples on MagneprintTM. Bit size was varied from 2 to 12 bits per sample for each MagneprintTM size so as to evaluate its effect on correlation histograms.

Figure 16 represents the graph of our system's performance, measured by the area under ROC curve and Gaussian separation (Figure 17) for varying Bits per Sample representation. However, since the only overlap in the accept and reject histograms was due to rare swipe error outliers, the ROC performance was nearly perfect for all variable choices. The separation graph, however, allows the selection of the bits per sample, B , for a fixed MagneprintTM size so as to maximize the system performance. For instance, considering a 96 byte (768 bit) MagneprintTM memory restriction, the maximum Gaussian separation occurs at 6 bits, which means that representing each sample by 6 bits, system can achieve its maximum performance such that MagneprintTM will have 128 samples. A very interesting yet unexpected behavior was noticed with an increase in B . Especially if we look at Figure, we notice that performance of the system increases as B increases and decreases after some value of B . We expected to have maximum system performance at approximately 3 bits per sample according to previous design experiments. This

would indicate that an increased resolution would no longer be beneficial at the cost of fewer samples. Instead, our maximum separation shifted to right, occurring at around 6 bits per sample. This may be because of the bimodal characteristic of our correlation distributions, considering forward and reverse swipes together. Though fewer measurements are included with higher bit quantization, increased sample resolution and spacing tightens the accept distributions, and the discrepancy between forward and reverse swipes is reduced, while the reject distributions remain largely unaffected.

The choice of selecting M and B can be further explained in Figures 22 and 23. Figure 22 shows accept and reject correlation histogram for MagneprintTM size of 768 bits, $B=2$, with separation of 0.2781 resulting from our experiment. Similarly, Figure 23 shows accept and reject correlation histogram for $B=12$, $M*B=768$, resulting separation of 0.2383.

In addition, we analyzed the choice of M , delta and B for a specific MagneprintTM sizes, 768 and 2048 as shown in the below Figure 24 and 25. We can observe that the separation is maximum for the choice of taking 109 samples, each spaced by 93 and representing 7 bits per sample to get 768 bits of MagneprintTM. Similarly from Figure 25, for a fixed MagneprintTM of 2048 bits, the system achieves maximum performance with 292 samples, each spaced by 35, represented by 7 bits per sample.

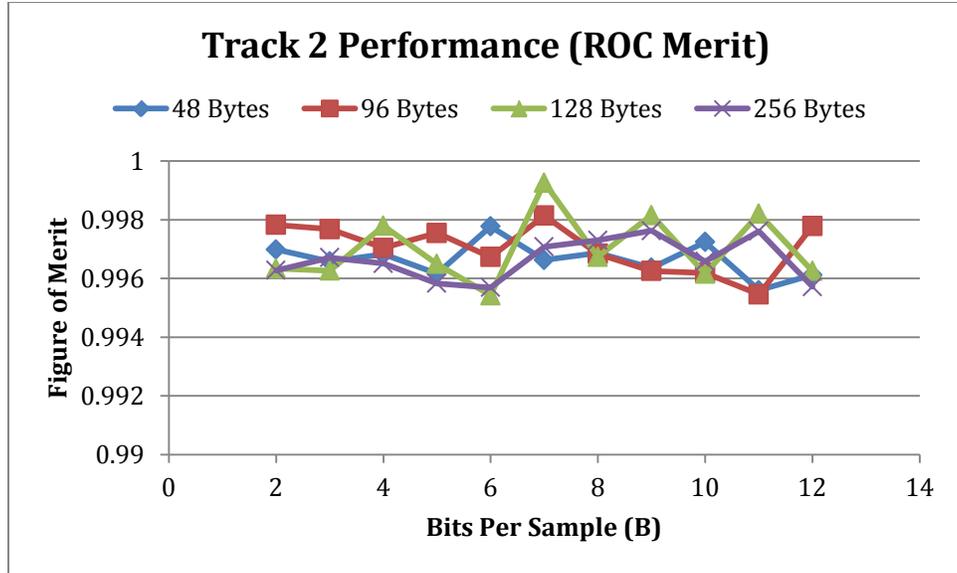


Figure 16: Figure of Merit vs. Bits per Sample

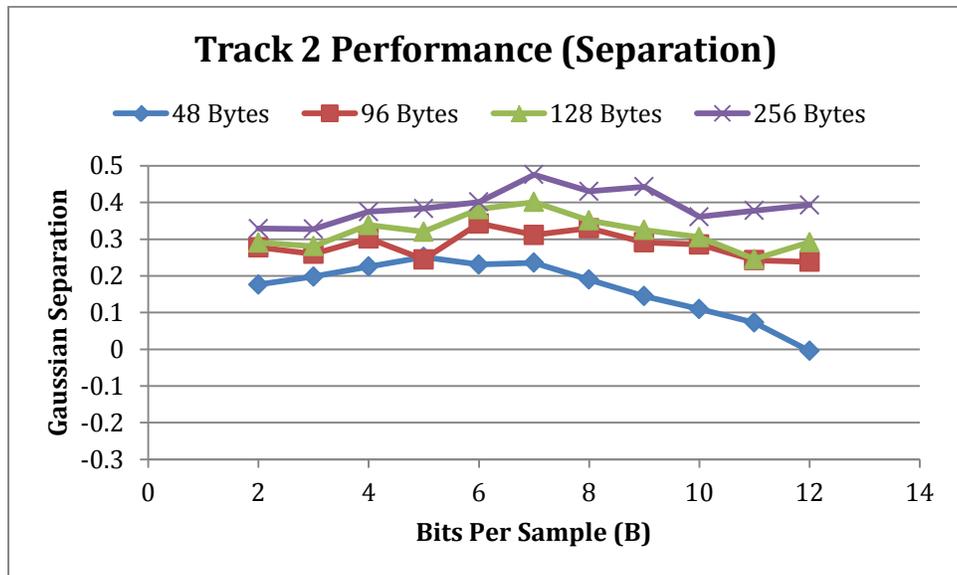


Figure 17: Separation vs. Bits per Sample

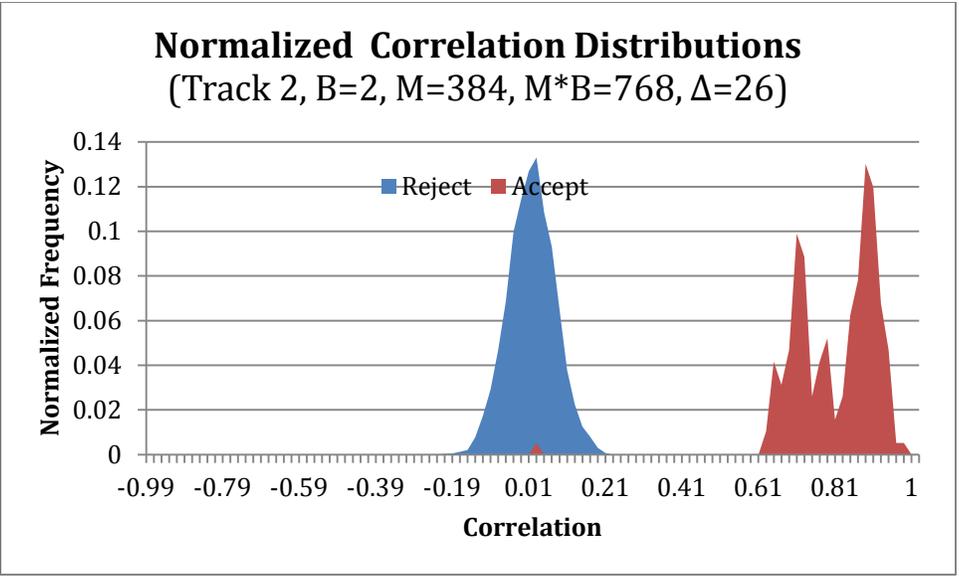


Figure 18: Accept and Reject Histograms for B=2, M*B=768

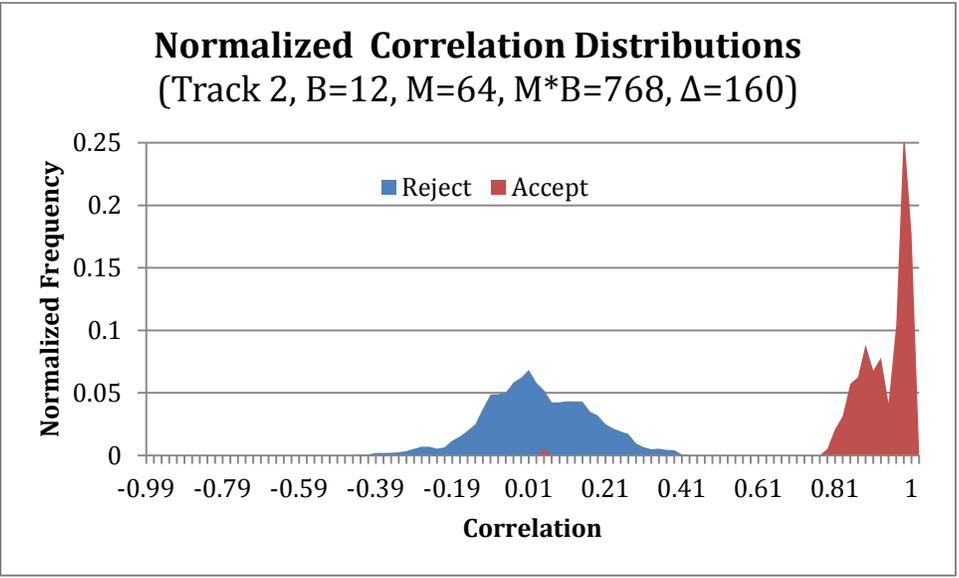


Figure 19: Accept and Reject Histograms for B=12, M*B=768

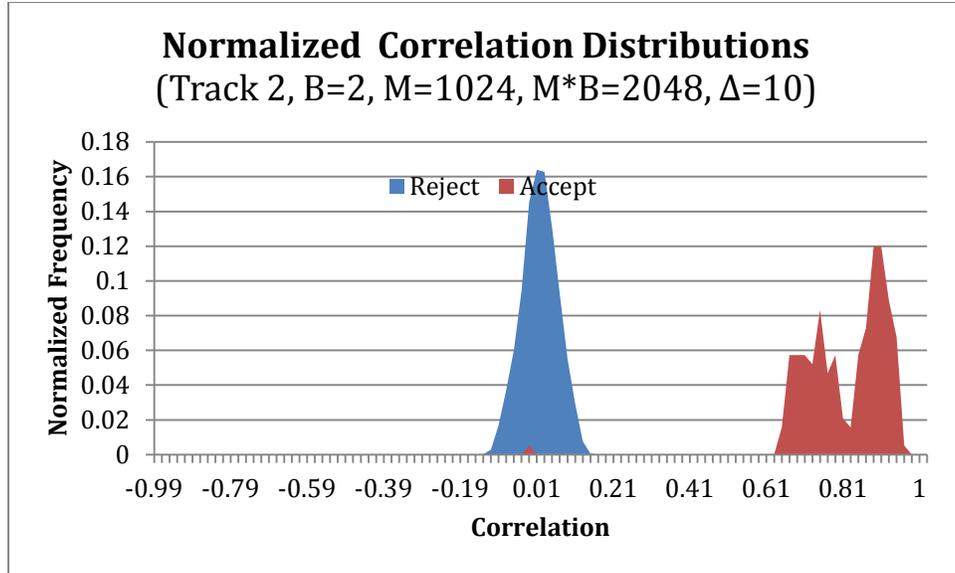


Figure 20: Accept and Reject Histograms for B=2, M*B=2048

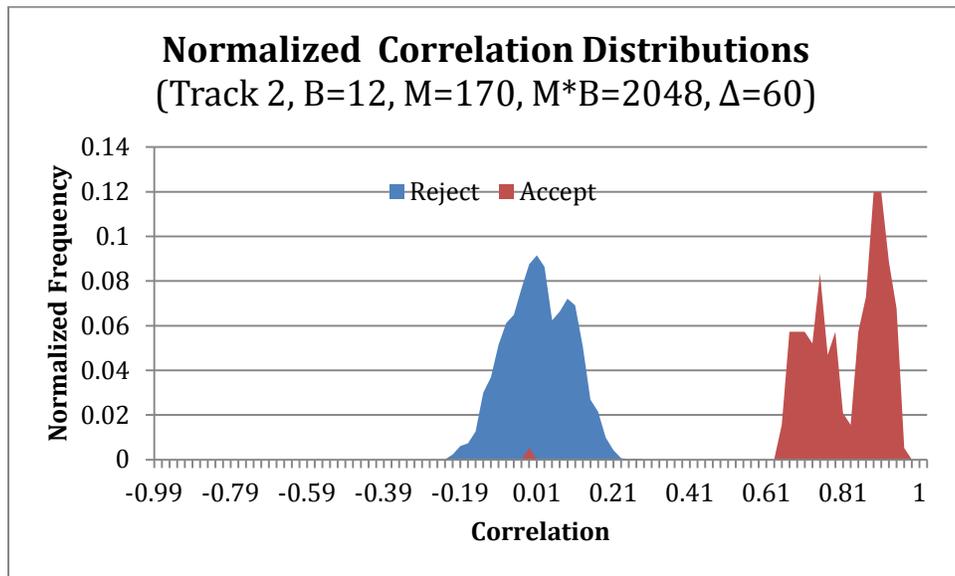


Figure 21: Accept and Reject Histograms for B=12, M*B=2048

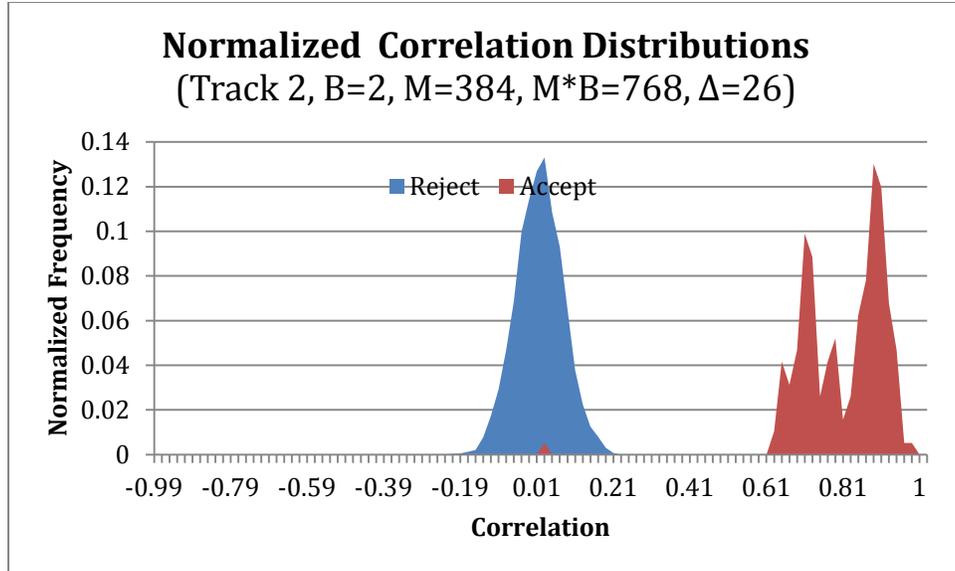


Figure 22: Accept and Reject Histograms for B=2, M*B= 768

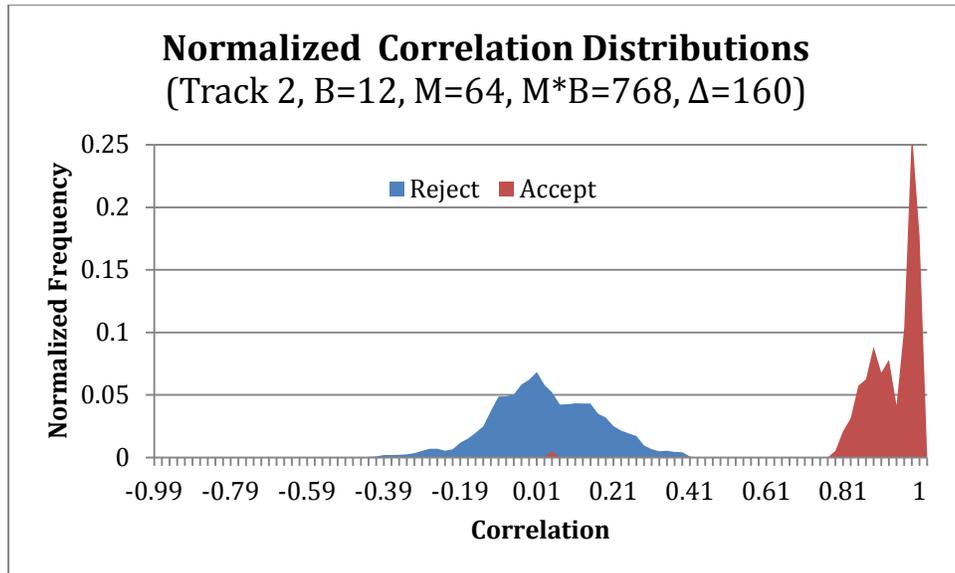


Figure 23: Accept and Reject Histograms for B=12, M*B= 768

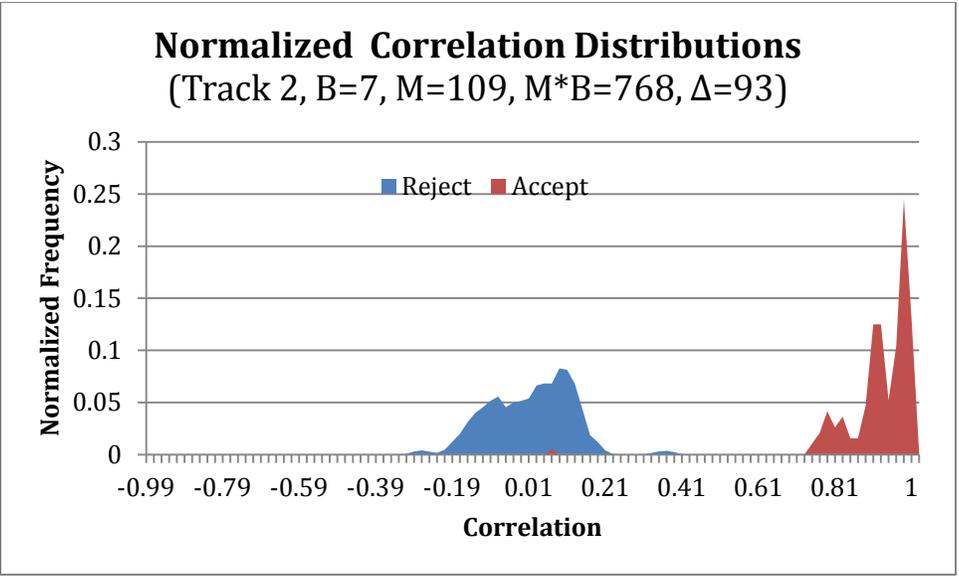


Figure 24: Histograms for Maximum Separation for M*B=768 bytes

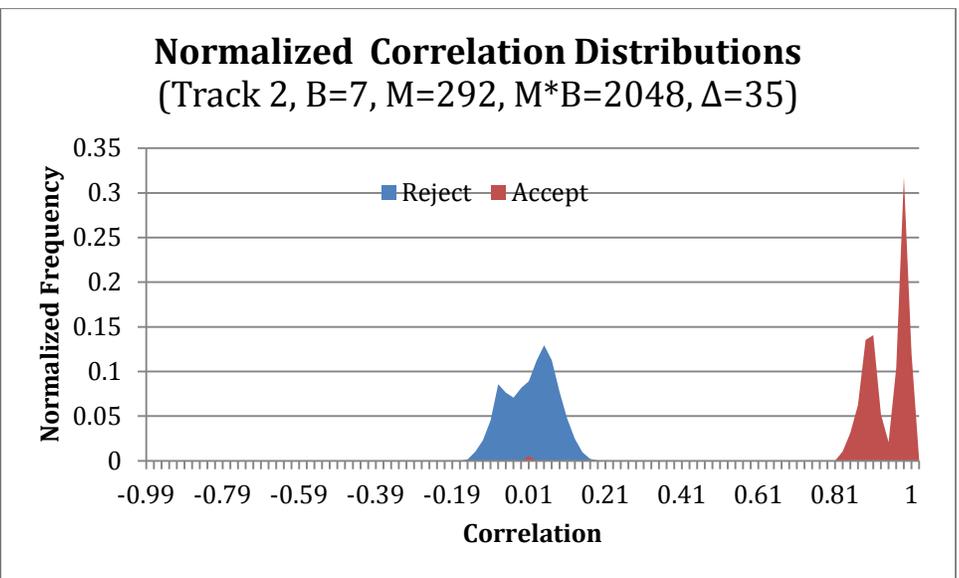


Figure 25 Histogram for Maximum Separation for M*B= 2048

CONCLUSION

Our authentication system performed as expected since we did not observe any overlap between two histogram plots. As our results show, we were able to achieve high system performance for different choices of M, Δ, and B to represent Magneprint™ in our database. An interesting feature of our design is that it can authenticate cards regardless of swipe speed, acceleration and

direction. Even though we observed bimodal distributions due to slight inconsistencies in the detected peak locations of forward and reverse swipes, they were within an acceptable range of correlation coefficients. We speculate that this occurred due to the discrepancy of taking samples at same location for either direction or may be because of peak detection scheme we implemented might have shifted sample locations. For future work, we would like to observe this bimodal behavior, study its significance, and find possible methods to reduce its effects on the correlation. In addition, we could explore how the physical characteristics of the system hardware affect the performance by testing multiple card readers. To sum up, with our design, cards could be authenticated with higher security and reliability, preventing from forged copying and huge monetary loss.

REFERENCES

- [1] R. S. Indeck, M. W. Muller, G. L. Engel and A. L. Hege, "Method and apparatus for fingerprinting and authenticating magnetic media," U.S. Patent 5,428,683, Jun. 27, 1995.
- [2] R. S. Deland, Jr., T. C. McGeary, "Magnetic Stripe Card Verification System," U.S. Patent 6,098,881, Aug. 8, 2000.
- [3] R. E. Morley, Jr., R. S. Deland, Jr., E. C. Limtao, E. J. Richter and S. R. Wood, "Method and apparatus for authenticating a magnetic fingerprint signal using filter capable of isolating a remanent noise related signal component," U.S. Patent 7,478,751 B2, Jan. 20, 2009.