Jurnal Nasional Teknik Elektro, Vol. 9, No. 3, November 2020
p-ISSN: 2302-2949, e-ISSN: 2407 - 7267

Design of a GSM-Based Skimming Reporting System for Automated Teller Machines

Robert Agyare Ofosu[*]**, Fuseini Mumuni and Ernest Nii Atuquaye Quaye**
Department of Electrical and Electronic Engineering, University of Mines and Technology, Ghana
[*]Corresponding author, e-mail: raofosu@umat.edu.gh

Abstract— In recent years, there has been the unpleasant advent of a new type of credit card fraud called Automated Teller Machine (ATM) skimming. This type of fraud poses a substantial threat to the banking sector because its modus operandi is quite subtler than other known types of ATM fraud. It consists of a criminal implanting a disguised dummy card reader very similar to the ATM's original card reader at the ATM. This is done to intercept the ATM card data of any unsuspecting customer who tries to withdraw cash. This paper seeks to design a system which will be able to detect and report such devices before they cause harm. The objective of this research was achieved by designing a skimmer incorporating the use of a metal detector for detecting new electronic components within the ATMs card slot region, an ultrasonic sensor for detecting unfamiliar skimmer overlays and the processing power of a microcontroller to coordinate theses sensors which monitor the status of the ATM terminal's original card reader and send a Short Message Service (SMS) text message whenever the system detects that a skimmer has been attached to the ATM terminal. This concept of skimming detection was designed, tested and simulated under several operating conditions in Proteus 8.0 simulation software to prove the detection method's efficacy. The simulation results showed that the proposed system provided a decent theoretical skimmer detection technique. However, other factors such as metal detector oscillator instability and the difficulty in accurately modelling the composition of ATM skimmers served as this design's major drawbacks.

Keywords : ATM, Skimming, GSM, Microcontroller

1. Introduction

The Automated Teller Machine (ATM) has become an integral part of modern-day banking systems worldwide. It is really patronized by customers of banks because of its ability to save customers lots of time spent in bank queues. This is evident because it is available for use all the time. It is also simple and user-friendly.

Due to the sensitive nature of these machines, security systems such as cameras and biometric fingerprint devices are put in place to make transactions more authentic and secure. However, criminals have updated their mode of operation to beat these systems and have now resorted to using even more sophisticated devices called ATM skimmers to steal ATM card data from customers of banks. These criminals later use the stolen data to conduct illicit bank transactions at the expense of the average man on the street [1].

These skimmer devices which are mostly installed in the night-time usually consist of a counterfeit device resembling an original card slot of an ATM with a magnetic card reader having storage capacity and a hidden pinhole camera. The skimming device is used to cover the original ATM card slot to primarily read and store ATM card data whenever there is a card inserted into the ATM. The pinhole camera attached to the skimmer then records the keystrokes of the customers ATM pin code. Finally, the data stolen through this method is used to create duplicate cards which give the criminals the unlawful access to the compromised bank accounts. Fig. 1 shows a skimmer found on an ATM.

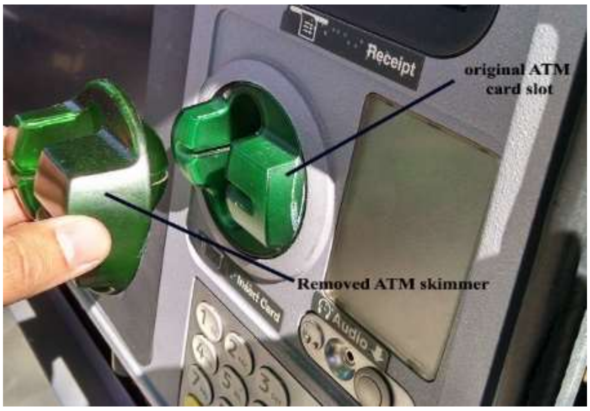


Fig. 1 Skimming device found on an ATM [2]

Received date 2020-04-06, Revised date 2020-08-10, Accepted date 2020-08-12
https://doi.org/10.25077/jnte.v9n3.770.2020

The composition of ATM skimmers is shrouded in mystery. However, [3] upon finding a skimmer at an ATM discovered that the ATM skimmer was made up of a mobile phone battery which powered the device, electronic circuitry, a flash storage device for storing data, a pinhole camera for recording the customers PIN keystrokes and finally a USB port which was to be a means of later retrieving the stolen information on the flash memory device.

ATM fraud can refer to an illegal transaction that is committed by using an ATM, including fraudulent deposits or skimming card information [4]. ATM fraud is perpetrated in many different forms. These include cash traps, transaction reversal fraud, internal fraud, Cybercrime and the use of Skimming devices.

In connection with ATM fraud statistics worldwide, in the second quarter of 2012, the ATM Industry Association (ATMIA) conducted a survey to determine the biggest threats to the ATM. The bar chart in Fig. 2 provides the results of the survey. From the survey results it can be seen that skimming tops the charts with the highest number of responses proving that card skimming is becoming a major security concern amongst the public.

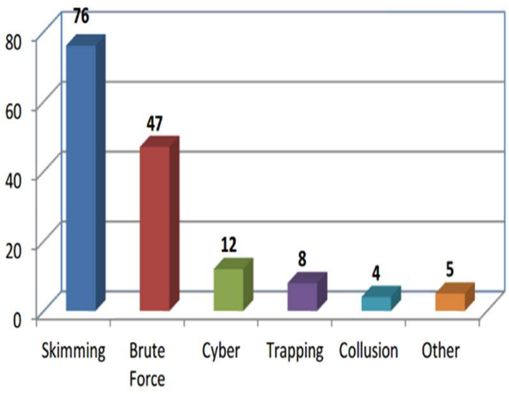


Fig. 2 ATM fraud report survey 2012 [5]

In Europe, a European firm called European ATM Security Team (EAST)'s 2014 fraud report elucidated the facts that during 2014 alone, losses amounting to € 279.86 million were accrued in European ATMs due to ATM related fraud attacks which was 13% increase compared to the losses of € 248.33 million reported for 2013 [6]. Further research by EAST established that in 2015 losses of € 327.48 million were reported which was a further 17% increase when compared to the total losses of € 279.86 million reported for 2014 [7]. The figures and trends from the EAST report as shown in Fig. 3 prove that ATM fraud losses are steadily rising over the years.

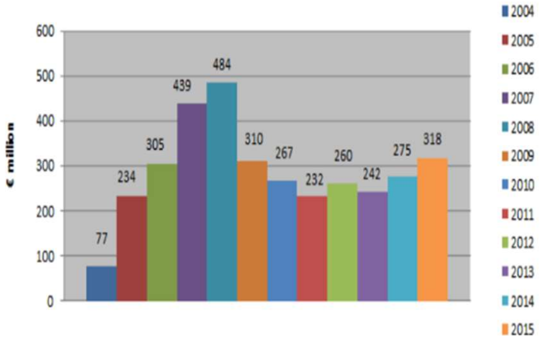


Fig. 3 ATM fraud losses from 2004-2015 [7]

A further perusal of the EAST report of 2014 revealed that the ATM fraud losses were broken down in further detail with credit card skimming being responsible for a greater part of these losses. The pie chart in Fig. 4 presents their findings.

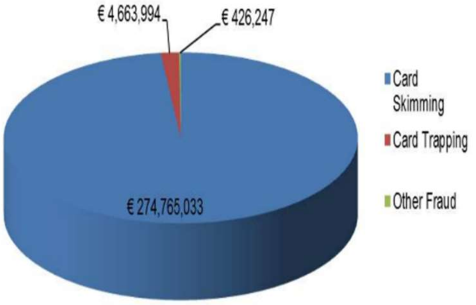


Fig. 4 Breakdown of ATM fraud attacks in 2014 [6]

The local scene is also not devoid of ATM card skimming fraud incidents. Notable among them is when in 2014, three Nigerians alleged to be members of a gang that manufactures and uses cloned ATM cards to withdraw various sums of money from the accounts of bank customers were arrested by the police. It was reported that they allegedly transferred an amount of GH¢ 3 million from accounts of customers [8]. Another is the incident in 2016 when two Bulgarians were arrested for allegedly making series of illegal transactions using cloned cards holding ATM card data that was skillfully and illegally retrieved at an ATM farm at Korle-Bu teaching hospital [9]. This trend shows an alarming rate of ATM card skimming worldwide hence the need to avert this canker.

Several research works have been reported in the literature regarding development of ATM security systems which offer a safer means of authenticating transactions. Some of which include biometric ATM, Europay, MasterCard and Visa (EMV) and ATM Video Surveillance Technology as reported in [10-17]. However, very few of these systems have incorporated anti-skimming defense systems to tackle the ever-growing threat of ATM skimming in our generation.

Thus, this paper seeks to focus on improving the current systems of ATM security by attempting to formulate a conceptual design of a GSM based skimming reporting systems which will alert the authorities via text message anytime an ATM skimmer is detected on an ATM.

2. ATM Machine

ATM is a modern-day technological wonder made up of different mechanisms working in synchronism to perform transactions on behalf of the bank and customer. It basically consists of a card reader's whose function is to decode the information encoded in the magnetic strip on the back of an ATM card. Once a user swipes his card, the reader sends that information to an internal computer, which then initiates a connection to the cardholder's bank. An ATM may use a dip card reader, which requires the user to insert his card into a slot or a swipe card reader.

It also has a keypad an input device which allows the cardholder to interact with the ATM. It allows the cardholder to inform his or her bank what sort of transaction (cash withdrawal, balance inquiry, etc.) he or she would like to undertake and for what amount. Also, the keypad allows the cardholders to input his or her Personal Identification Number (PIN) to verify his or her identity when making transactions.

The speaker allows the ATM to communicate with the cardholder by means of an audio. This functionality comes into play when a key is pressed or when the ATM wants to relay special information to the cardholder.

The display screen's function is to visually guide the cardholder through each step of the transaction whiles the cash-dispensing mechanisms are located deep inside the ATM stores and dispenses cash when prompted by an ATM user.

Finally, the receipt printer is responsible for providing the cardholder with a paper receipt as proof of the transaction. It employs thermal paper rather than ink to turn the paper black and form the necessary text.

There are other parts such as the rollers and suction cups which assist the ATM in performing its ultimate function of self service banking, but for simplicity sake only the above-mentioned parts have been discussed. Fig. 5 gives a simple visual anatomy of the ATM machine.

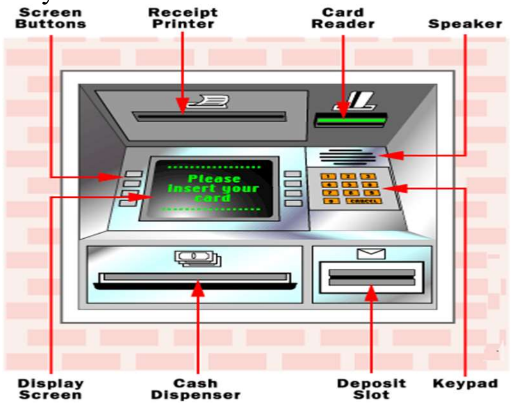


Fig. 5 ATM machine [18]

3. Methodology

3.1. Design Concept

The block diagram of the ATM skimming reporting system is shown in Fig. 6.

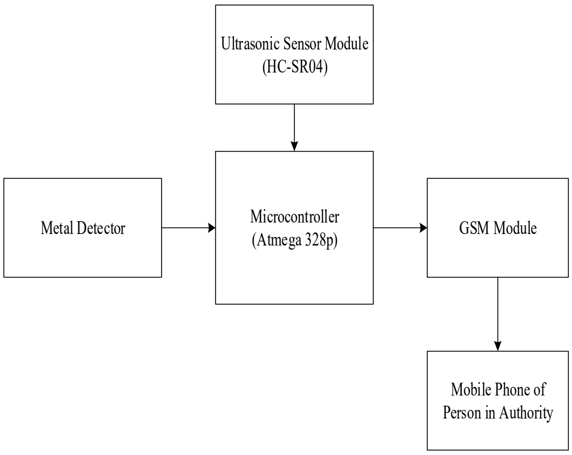

Ultrasonic Sensor Module (HC-SR04)
Metal Detector
Microcontroller (Atmega 328p)
GSM Module
Mobile Phone of Person in Authority

Fig. 6 Block diagram of ATM skimming reporting system

The concept employed in this design consists of two sub-systems working together to monitor the security status of the ATM machine. These two subs-systems are the skimmer detection system and the GSM reporting module. The actions of the two sub-systems are coordinated and interlinked by the processing power of an Atmega 328p Microcontroller. The skimmer detection system operates on the premise of two signal indicators to validate the presence of a skimmer. Firstly, the detection of the presence of a new metallic object within the perimeter of the ATM card slot region serves as the prime indicator. This is achieved by a metal detector placed near the ATM card slot which continually checks for the presence of any electronic components such as printed circuit boards, phone batteries or digital storage media around the ATM card slot perimeter.

In addition to that, a reduction in distance between the ATM card slot and an installed ultrasonic sensor indicates the presence of a new physical covering on the ATM card slot. This serves as a secondary indicator in the skimmer detection system. When the aforementioned conditions are met, the programmed microcontroller interprets it as the presence of an ATM skimmer installed on the ATM and a warning SMS message is sent to the appropriate authorities via a GSM modem.

Fig. 7 illustrates the proposed system without a skimmer and Fig. 8 depicts the proposed system with a skimmer.

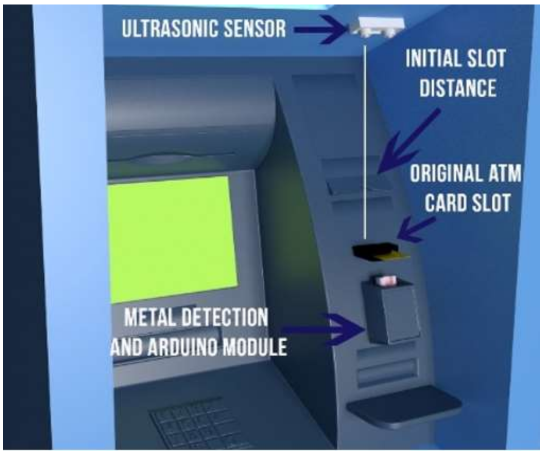


Fig. 7 Proposed system without skimmer

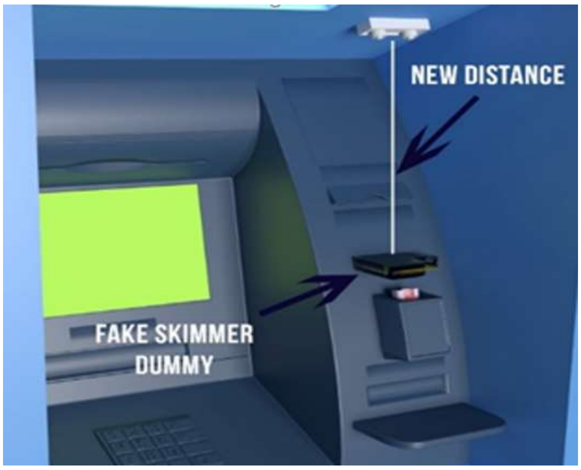


Fig. 8 Proposed system with skimmer

3.2. Materials

The materials that were employed in the design of the GSM based skimming reporting system were in two forms. Firstly, the hardware involved in the design include Metal detector, GSM SIM 900 modem, HC-SR04 Ultrasonic Sensor, Atmega 328p Microcontroller. The software components involved also include Proteus 8.0 simulation software and Arduino IDE. The schematic diagram of the designed circuit is as shown in Fig. 9.

The designed circuit works in such a way that when DC current from the battery powers the inverting operational amplifier U1, the natural noise component found in the operational amplifier produces a signal which charges up the tank circuit which consists of the 1 mH inductor L1 and both 0.1 µF capacitors C1 and C2. Inductors L2 and L3 represent different states of inductance of the metal detector coil's inductance when metals deviate the detector coil's inductance.

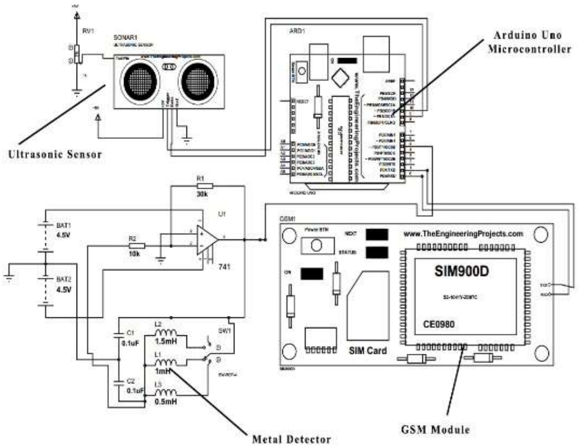


Fig. 9 Schematic diagram of the circuit

The oscillator of the metal detector then begins to oscillate at a frequency of 19.5 kHz at initial conditions which is the resonating frequency of the metal detector's oscillator. However, it is useful to note that the initial oscillating frequency may vary depending on the environment in which the metal detector finds itself. Furthermore, the oscillator feeds back a portion of the oscillating frequency signal back into the inverting operational amplifier to sustain its oscillations during its period of operation. After that, real-time signals are fed from the metal detector and ultrasonic sensor into digital pins 5, 9 and 10 of the Atmega 328p Microcontroller respectively and the Microcontroller processes these signals according

https://doi.org/10.25077/jnte.v9n3.770.2020

to its skimmer detection algorithm. Upon detection of a skimmer by the algorithm, the microcontroller then instructs the GSM module to send warning SMSs to persons in authority.

3.3. Flow Chart of the Proposed System

The flow chart in Fig. 10 depicts the algorithm employed in the system to detect the presence of skimmers on an ATM. When the aforementioned system is installed on an ATM, a system initialization procedure first takes place. The algorithm at system initialization contains a slight delay for accurate and stable initial measurements. During system initialization, the metal detector measures the original metallic objects present around the ATM and the ultrasonic sensor also measures its initial distance from its position to the ATM card slot. Both values are stored in the microcontroller for comparisons with future measurements. This serves as the key concept in this algorithm.

After that, the microcontroller continually compares the current incoming frequency from the metal detector with the earlier measured initial frequency of the metal detector to determine if there has been a significant change in the frequency measurement by ±500 Hz. This check is to ascertain that a new metallic presence (representing the electronic components in a skimmer) has been detected.

If that condition is satisfied then the microcontroller proceeds to compare the current distance measurement read by the ultrasonic sensor with the initial distance measurement taken at the point of the system's initialization.

If the current distance measurement is 1 cm less than the initial distance measured, then the detection algorithm supposes that the ATM card slot has been also covered with a new object (most probably an ATM skimmer). This condition when satisfied confirms the skimmer's physical presence. Subsequently, a warning SMS is sent to the appropriate authorities to inform them of the ATM skimmer's presence.

3.4. Design Assumptions and Considerations

In the design of this system, some assumptions and considerations were made. These are;

i. The frequency deviation required for the microcontroller in the simulation to detect a substantive change in the frequency that emanates from the metal detector was set to

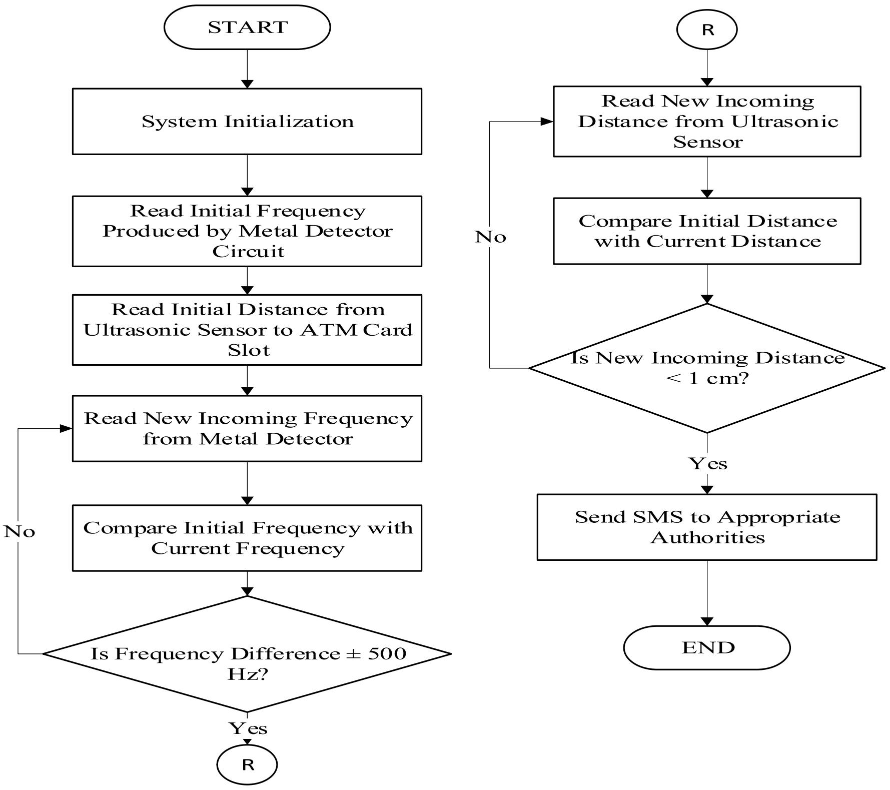

START
System Initialization
Read Initial Frequency Produced by Metal Detector Circuit
Read Initial Distance from Ultrasonic Sensor to ATM Card Slot
Read New Incoming Frequency from Metal Detector
Compare Initial Frequency with Current Frequency
Is Frequency Difference ± 500 Hz?
No
Yes
R
R
Read New Incoming Distance from Ultrasonic Sensor
Compare Initial Distance with Current Distance
Is New Incoming Distance < 1 cm?
No
Yes
Send SMS to Appropriate Authorities
END

Fig. 10 Algorithm of skimmer detection system

be ±500 Hz to satisfy the simulation programs sensitivity constraints.

ii. The initial distance measured by the ultrasonic sensor in the simulation was set to be 24 cm. This value was chosen arbitrarily to represent an ATM card slot's positioning from the ultrasonic sensor in the simulation process.

iii. The resonant frequency of the metal detection coil's oscillator was assumed to be 19.5 kHz so that the coil would be able to detect smaller metal targets.

iv. This design is considering ATMs with outwardly protruding card slots.

3.5. Design Formulae

In the proposed model a number of mathematical formulae were considered in the design of the metal detector coil. They have been presented below.

3.5.1. Oscillating Frequency of Tank Circuit

Firstly, the metal detector tank circuit oscillates at a frequency inversely proportional to the total inductance and capacitance of the tank circuit as shown in equation (1). However, it is good to know that in this design configuration of the tank circuit, the capacitance remains the same whilst the inductance changes as a result of different metallic objects in the skimmer affecting the inductance value of the metal detector coil [19].

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{1}$$

where, *f* is the oscillating frequency, L is the total inductance of tank circuit and C is the total capacitance of tank circuit.

3.5.2. Inductance of Metal Detector Coil

The inductance of the metal detector coil also generally, varies directly with the permeability of the metallic objects present within the region of the detector coil's core as shown in equation (2) [19].

$$L = \frac{\mu N^2 A}{l} \tag{2}$$

where, *L* is inductance of coil, μ is permeability of the core of coil, N is number of turns, A is cross-sectional area of the coil and *l* is length of the coil.

3.5.3. Permeability of the Metal Detector Coil

Finally, the permeability of the core of the metal detector coil varies directly with the relative permeability of the coil's core. Therefore, ferrous metals with higher relative permeability would increase the permeability of the coil's core and non-ferrous metals will decrease the permeability of the core due to eddy current action [20]. Equation (3) [19] depicts this relationship.

$$\mu = \mu_o \mu_r \tag{3}$$

where, μ is permeability of the core of coil, μ_o is permeability of air and μ_r is relative permeability of the core.

4. Results and Discussion

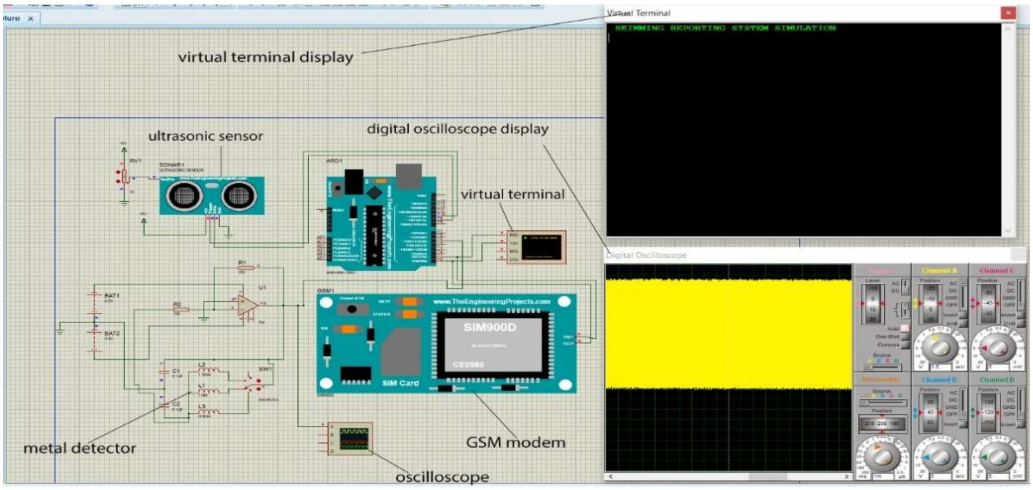
The results of the various simulation scenarios that this paper entails are discussed in this section. The results presented are based on the possible simulation scenarios of the circuit design. The results of the simulations are displayed and interpreted with the aid of two virtual instruments. Firstly, from an oscilloscope displaying the frequency of the oscillating waveform produced by the metal detector and secondly, a virtual terminal displaying the readings of the various quantities being measured and also the various actions the microcontroller performs during the simulation. Fig. 11 shows the simulation of the proposed system in Proteus with both virtual instruments in operation.

4.1. Simulation Results

The results from the simulations have been presented through a means of four different scenarios representing the four possible conditions the proposed design encountered during its operations.

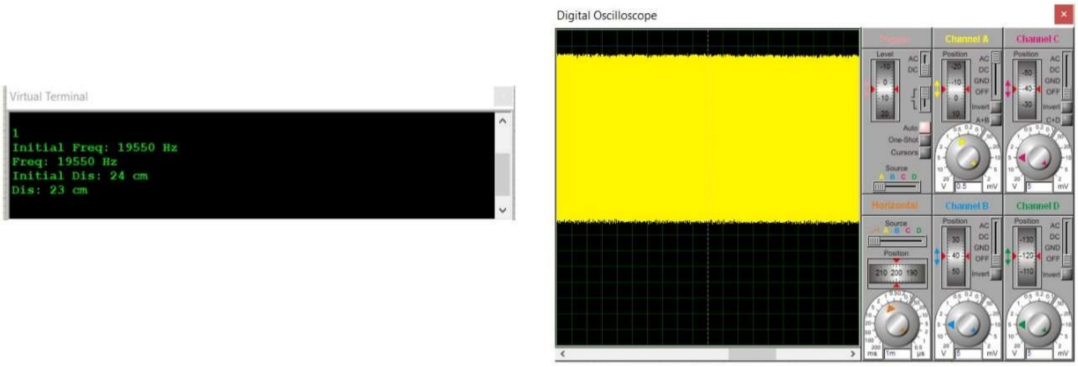
Fig. 12 depicts results of system at start up when no changes have been made to the ATM. The simulation results of Fig. 12 show that at starting conditions, the metal detection coil of 1 mH initial inductance oscillates at a frequency of 19.5 kHz. The oscilloscope also displays the waveform emanating from the metal detector circuit. A distance of 24 cm was also recorded by the ultrasonic sensor as the initial distance between the ultrasonic sensor and the ATM card slot. These values are the reference values the microcontroller will compare subsequent measurements to determine the skimming status of the ATM. It can also be observed that when the two measurements did not satisfy any of the detection conditions the microcontroller did not produce any different response.

https://doi.org/10.25077/jnte.v9n3.770.2020



```
SKIMMING REPORTING SYSTEM SIMULATION
```

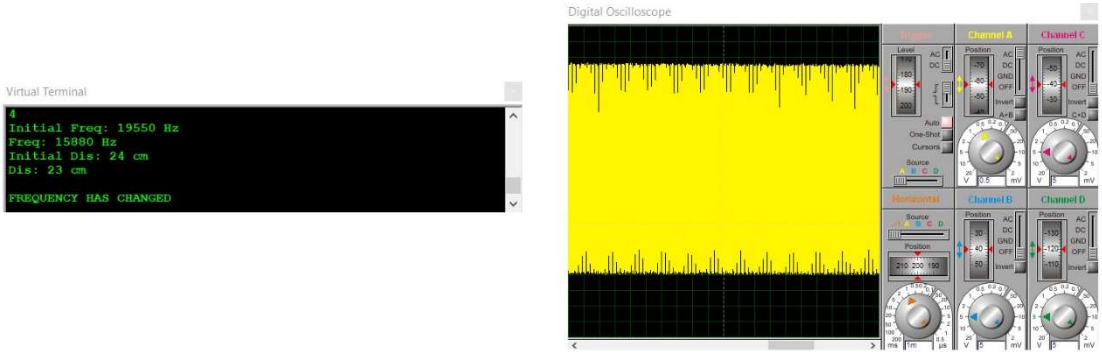
Fig. 11 Simulation model of system with virtual instruments



```
1
Initial Freq: 19550 Hz
Freq: 19550 Hz
Initial Dis: 24 cm
Dis: 23 cm
```

(a) Virtual terminal (b) Oscilloscope

Fig. 12 Results of system at start up when no changes have been made



```
4
Initial Freq: 19550 Hz
Freq: 15880 Hz
Initial Dis: 24 cm
Dis: 23 cm

FREQUENCY HAS CHANGED
```

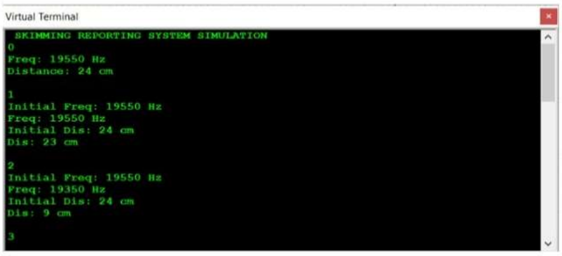
(a) Virtual terminal (b) Oscilloscope

Fig. 13 System results when frequency condition satisfied but distance unsatisfied

Fig.13 also shows one of the scenarios when frequency condition is satisfied but distance unsatisfied. From Fig. 13 the simulation results on the virtual terminal shows that when the metal detection coil's inductance increases to 1.5 mH, the oscillating frequency of the metal detector consequently reduces to 15.8 kHz.

It can also be seen that the sinusoidal frequency pattern on the virtual terminal becomes more distinct. This change further goes to prove there has been a reduction in the frequency value. Subsequently, the microcontroller indicates the change on the virtual terminal by displaying the text "FREQUENCY HAS CHANGED". However, the current distance measurement of 23 cm does not satisfy the secondary skimmer indicator condition therefore no alert SMS is sent to the authorities.

Fig. 14 also depicts the third scenario when distance condition is satisfied but frequency unsatisfied.



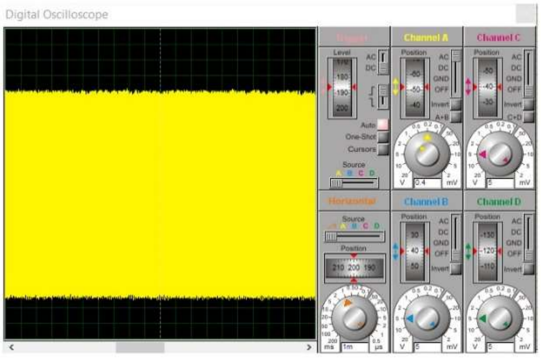
```
Virtual Terminal
 SKIMMING REPORTING SYSTEM SIMULATION
0
Freq: 19550 Hz
Distance: 24 cm

1
Initial Freq: 19550 Hz
Freq: 19550 Hz
Initial Dis: 24 cm
Dis: 23 cm

2
Initial Freq: 19550 Hz
Freq: 19350 Hz
Initial Dis: 24 cm
Dis: 9 cm

3
```

(a) Virtual terminal

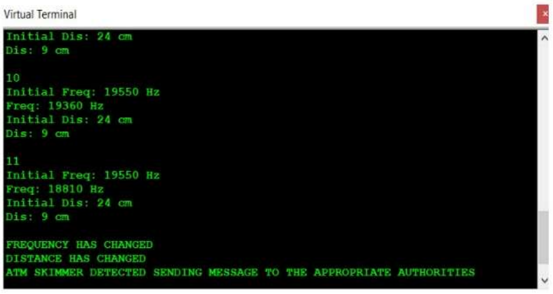


(b) Oscilloscope

Fig. 14 System results when distance condition satisfied but frequency unsatisfied

From Fig 14, it can be seen that there is a reduction in the original distance measurement from 24 cm to 9 cm the microcontroller also refuses to respond. This is because as earlier discussed in the operation of the detection algorithm there has to be a significant change in the metal detector frequency before there is even a check for changes in the distance. Therefore, the microcontroller is insensitive to any changes in distance when the frequency condition is not satisfied.

The last scenario shown in Fig. 15 depicts the simulation results when both distance and frequency conditions are satisfied.



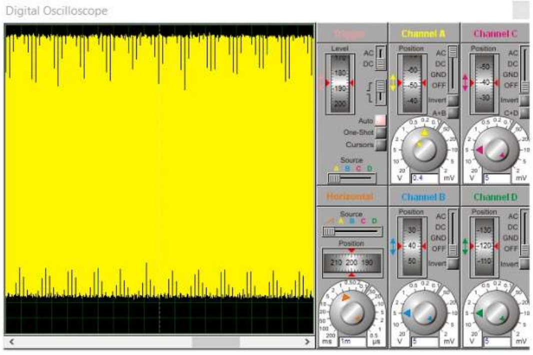
```
Virtual Terminal
Initial Dis: 24 cm
Dis: 9 cm

10
Initial Freq: 19550 Hz
Freq: 19360 Hz
Initial Dis: 24 cm
Dis: 9 cm

11
Initial Freq: 19550 Hz
Freq: 18810 Hz
Initial Dis: 24 cm
Dis: 9 cm

FREQUENCY HAS CHANGED
DISTANCE HAS CHANGED
ATM SKIMMER DETECTED SENDING MESSAGE TO THE APPROPRIATE AUTHORITIES
```

(a) Virtual terminal



(b) Oscilloscope

Fig. 15 System results when both distance and frequency conditions are satisfied

From Fig. 15 it can be observed on the virtual terminal that when both conditions are satisfied, the microcontroller proceeds to send an alert SMS to the appropriate authorities.

The Table 1 presents a truth table model which summarizes how the results of all the possible scenarios of this system played out during the simulation process.

4.2. Design Limitations

The proposed design faced a few pitfalls and limitations during the simulations. This section provides a list of those problems and how they affect the performance of the proposed system.

4.2.1. Difficulty in Modelling Skimmer Parameters

The design does not include a method of fully modelling the frequency response of the metal detector when an actual ATM skimmer is placed on an ATM. This is because a skimmer contains various metallic composites with different permeabilities which cannot be accurately analyzed with simple metal detector equations.

Table 1. Summary of Simulation Results

Figure No.	Condition 1 (metal detected?)	Condition 2 (distance reduced?)	System Response
12	False	False	No alert SMS sent
13	True	False	No alert SMS sent
14	False	True	No alert SMS sent
15	True	True	Alert SMS sent

This challenge was encountered because data analytics for such nefarious devices is kept from the public for security reasons. Therefore, this design model lacks a vital parameter in its detection algorithm. These parameters can be better modelled with data analytics collected from real ATM skimmers.

4.3. Unstable Oscillator Frequency Values

In some instances, there was the observance of unstable frequency values emanating from the metal detector coil. This phenomenon observed could be due to the negative effects of temperature changes and minor supply voltage imperfections in the oscillator circuit. Practically all electronic components have a thermal sensitivity hence as they heat up or cool down, their value or some other parameter may change and these changes may cause unstable frequency values and trigger false alarms.

4.4. Difficulty in Modelling GSM Response

This design does not include a method which fully represents the response the alert text message recipient's GSM mobile phone would experience when a text message is sent to indicate the presence of a skimmer. This is due to the limitations imposed by the simulation environment. Therefore, the validity of the GSM response of this system could be only properly modelled and verified when the system is implemented physically in future designs.

5. Conclusions

In conclusion, the design of the ATM skimmer detector has been achieved and from the simulation results it was able to detect change in the frequency of the metal detector and ultrasonic sensor distance respectively from the ATM card slot. The proposed system provides a decent theoretical detection technique in detecting overlay skimmers. However, there are many more issues to be considered when designing a stable metal detection system to detect ATM skimmers.

It is therefore recommended that a database on ATM skimmer device component characteristics should be established by banks to aid future designers with the necessary data to produce better skimmer detection models.

Future designs should consider incorporating a real time clock module and additional sub-system which give intermittent feedback of the ATM's security status in order to upgrade it to become a smarter monitoring system.

References

[1] B. Krebs, "Would You Have Spotted this ATM Fraud?", Available: *https://krebsonsecurity.com/2010/03/would-havespotted-this-atm-fraud/*. Accessed: November 19, 2017.

[2] Washington State Department of Financial Institution, "ATM Skimming Devices Popping up Across the Country", Available:*https:// dfi.wa.gov/consumer/alerts/atm–skimming–devices–popping–across-country*. Accessed: November 19, 2017.

[3] M. South, "Can't Hack a Hacker: Reverse Engineering a Discovered ATM Skimmer", Available: *https:// trustfoundry.net/reverse-engineering-a-discovered-atm skimmer/.* Accessed: November 20, 2017.

[4] R. Booker, "What is ATM Fraud?", Available: *http://www.wisegeek.com/what-is-atm-fraud.htm*. Accessed: April 10, 2018.

[5] L. Fricker-Gruss, "Analysis of Fraud Perpetrated through Automated Teller Machines: Strategic Solutions that will Assist Financial Institutions in Reducing Loss", *BSc Project Report*, Utica College, New York, 55pp, 2012.

[6] L. Gunn, "European ATM Crime Report", *European ATM Security Team Ltd, Europe*, 30pp, 2014.

[7] B. Krebs, (2016), "A Dramatic Rise in Skimming Attacks?", Available: *https://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/*. Accessed: November 19, 2017.

[8] E. E. Abbey, "Three Nigerians Busted; For Stealing GH¢3 million through ATM Fraud", Available: *https://www.graphic.com.gh/news/general-news/3-nigerians-busted-for-stealing-gh-3-million-through-atm-fraud.html.* Accessed: April 9, 2018.

[9] A. O. Sarpong, "Two Bulgarians Grabbed for ATM Fraud", Available: *http://www.ghanaiantimes.com.gh/2-bulgarians-grabbed-for-atm-fraud/.* Accessed: April 9, 2018.

[10] R. Arnfield, "Why EMV-Compliant ATMs Need Anti-Skimming Technology", Available:*http://www.atmatom.com/http://www.atmatom.com/why-emv-compliant-atms-need-anti-skimming-technology/*. Accessed: April 9, 2018.

[11] M. Anderka, T. Klerx, S. Priesterjahn, and H. K. Büning "Automatic ATM Fraud Detection as a Sequence-Based Anomaly Detection Problem", *Proceedings of the 3rd International Conference on Pattern Recognition Applications and Methods*, Angers, France, 6pp, 2014.

[12] R. R. Gooli and B. Imthiazunnisa, "Design and Implementation of Anti-Theft ATM Machine Using Raspberry Pi", *International Journal and Magazine of Engineering, Technology, Management and Research*, Vol.2, 2015, No.11, 4pp, 2015.

[13] K. A. M. Musallam and K. N. Smitha, "Detecting Skimming Devices in ATM through Image Processing", Available: *http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumb er=7507139*. Accessed: October 12, 2017.

[14] K. H. S. Sivaprasad and B. K. Vijay, "Design and Implementation of Anti-Theft ATM Machine Using Embedded Systems", *International Journey and Magazine of Engineering Technology, Management and Research*, Vol.3, 2016, No.3, 7pp, 2016.

[15] B. R. Rao, P. Rao, G. N. Rachana and B. V. Sushma, "Design and Implementation of High End Multiple Security Based ATM Monitoring System", *International Journal on Recent and Innovation Trends in Computing and Communication*, Vol. 4, 2016, No. 4, pp. 531-535, 2016.

[16] P. Banu, P. Kavith, T. Ashoh, N. Logesh-Kumar and M. Chandrasekar, "Smart ATM Access and Security System using RFID and GSM Technology", *International Journal of Scientific Research and Education*, Vol. 4, 2016, No. 6, pp. 5505 – 5509, 2016.

[17] A. M. Lawan, "Use of Biometrics to Tackle ATM Fraud", *2010 International Conference on Business and Economics Research*, IACSIT Press, Kuala Lumpur, Malaysia, pp. 331-335, 2010.

[18] J. Bowen, "How ATMs Work", Available:*https://money.howstuffworks.com/personalfinance/banking/atm3.htm*. Accessed: April 9, 2018.

[19] C. W. Mooreland, "BFO Theory", Avaiable:*http://www.geotech1.com/pages/metdet /info/bfotheory/bfo.pdf*. Accessed: February 22, 2018.

[20] F. Le Mantec, "Metal Detection: Beat Frequency Oscillator", Available: *https://www.embeddedrelated.com/showarticle/911.php*. Accessed: April 4, 2018.