Employing Smartphones Xenon Flashlight For Mobile Payment

Mariam M. Galal, Ahmed Abd El Aziz, Heba A. Fayed and Moustafa H. Aly
Photonics Research Lab (PRL)
Arab Academy for Science and Technology (AAST)
Alexandria, Egypt
prlsupervision@gmail.com

Abstract— Due to the huge dependence of the users on their smartphones and the huge technological advances in their design, smartphones have replaced many electronic devices nowadays. For that reason, it is of great interest to use such phones to replace magnetic cards. This paper uses the built-in Xenon flashlight in today's Android smartphones to experimentally transmit the data stored on the user magnetic card to a card reader or automatic teller machine (ATM). We experimentally modulate the embedded Xenon flashlight in a smartphone with the required information of a traditional magnetic card and transmit the light over a secure high speed optical link at 15 bps with no additional hardware at the user end. The paper introduces the design of an implemented small, inexpensive supplementary receiver circuit module, which is easily attached to a contemporary card reader or ATM machine. Furthermore, the paper tests the system performance under the effect of interference from another transmitter as well as compares its speed and security to the regular ATM card and to other competing technologies.

Keywords—Visible light communication; Xenon flashlight; ATM machines; smartphones; smart payments

I. Introduction

Only a few years ago, mobile phones were merely used for making vocal phone calls and sending short messages. Due to the enormous technological advances, increase in internal memory and processing power as well as the decrease of size and complexity of electronic devices, smartphones nowadays play a role in almost all of the daily tasks, replacing other devices such as cameras, personal digital assistants, media devices and navigation and positioning systems [1]. Most recently, they are even considered one of the main components in the financial sector, replacing credit, discount as well as gift cards and allowing their users to make both online and offline financial transactions using them [2].

In order to guarantee a secure and easy communication between smartphones and card readers or ATM machines, technology giants have proposed many techniques to transmit the required information to automatic teller machines (ATMs) or card readers [3]. Google and Samsung, amongst many others, embedded a Near Field Communication (NFC) chip in their newest smartphones, allowing their users to make the required payments via tapping the back of the mobile device on an NFC enabled card reader [4]. On the other hand, Square, another company working in the field of technology in payments, depends on a Wi-Fi connection to transmit the credit card information saved on the mobile phone via a cubic accessory attached to the smartphone [5]. Both technologies however, pose a considerable risk on the sensitive data of the user credit card and require the user to pay and use complex and expensive hardware. In addition, those systems are mostly incompatible with RF sensitive environments such as on airplanes and in hospitals. Hence, an alternative technique is still required [6-9].

In this paper, we experimentally created a secure visible light communication link between the smartphone and the ATM machine using only the embedded Xenon flashlight of a smartphone and a simple supplementary, easily integrated circuitry on the card reader side. Furthermore, we have tested the implemented system for interference when two or more users are making financial transactions on adjacent card readers. In the next section, previous research dealing with information and credit card data transmission over flashlight is introduced. In section 3, the experimental setup and circuitry of the proposed system is described, followed by the measured results in section 4. Section 5 tests the system speed and security and compares them to those of a regular magnetic ATM card. Section 6 concludes the experimental work.

II. Previous Related Work

Many researches have employed the smartphone built-in flashlight for communication in addition to photography or illumination purposes. T. Hesslemann et al studied in their paper the use of a Nexus S smartphone LED flashlight for transmitting data to interactive tabletops. Claiming that the visible light link is more secure and robust against hackers attacks compared to other RF technologies, the authors modulated the LED flashlight using Non-Return-to-Zero (NRZ) On-Off-Keying (OOK) modulation scheme to transmit data to an interactive tabletop at data rates of up to 25 bps by placing the smartphone screen-side up on the tabletop. The tabletop then detects the transmitted light on its surface and decodes the transmitted message [7].

In another research conducted by A. S. Shirazy et al, the built-in flashlight of a smartphone was used in its raw form to interact with large public displays. The user moves his mobile phone with the flash turned on in front of a large public display screen, while a webcam traces his hand movements and maps them to a moving cursor on the screen. The system allows selection of an item on the screen by turning the flashlight on and off again – similar to a double click action with the computer mouse – and zooming in and out by moving the mobile phone closer and farther away from the screen respectively [10].

M. M. Galal et al experimentally proved the possibility of a successful transmission of credit card information over a visible light link by modulating the LED flashlight of an Android based smartphone using intensity modulation. Their research successfully decoded the received signal employing an inexpensive microcontroller module placed on the card reader side. Data rates of up to 500 bps were achieved using this setup, allowing error-free transmission of the needed credit card information in less than half a second [11].

However, to our knowledge, all the previous research didn't consider modulating the widely available, much brighter yet much slower Xenon flashlight of a smartphone. In this paper, the Xenon flashlight of a smartphone is modulated with the required magnetic card information and transmitted over a short length free space shielded channel to a photodetector circuit on the receiver side. The paper further investigates the interference of the high brightness of the flashlight on a card reader nearby as well as the security of the system compared to the regular magnetic card.

III. Experimental Setup

The main purpose of the experiment is to successfully transmit the information stored on a magnetic ATM card to the ATM machine using only the flashlight of the smartphone. The magnetic strip on the back of the ATM card consists of three tracks. The first track carries 79 alphanumeric characters, containing detailed information about the card holder and his/her bank account, such as the full name, bank information and security codes. Although the data on this track is highly detailed, it's rarely used by any ATM machine or Point of Sale (POS). Much more commonly used however, is the data stored on the second track of the magnetic strip, which consists of 40 numeric characters, each represented as a 4-bit binary sequence followed by one parity bit for error detection, resulting in a total of 200 binary bits. For example, a numeric character '3' is represented as '0011' and a parity bit '0' which results in a 5 bit binary code '00110' [12]. Among others, this track carries the bank account number, encoded CVC number and personal identification number (PIN), expiry date, and some security information. The detailed structure of the second track is shown in Fig. 1 below. The third track of the magnetic strip is currently reserved for future use.

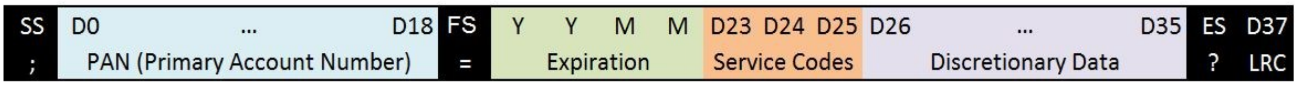
As shown in the block diagram of the implemented system in Fig. 2, these 200 binary bits are used to modulate the Xenon built-in camera flashlight of a Samsung smartphone running Android 4.3. For the user interface, a specially designed Android application has been developed. This allows the experiment with either On-Off-keying (OOK) or Pulse width modulation (PWM) as well as allows the tester to choose the pulse width to test the system performance at different data rates. In order to test the system with real data, we have entered the data from a real expired ATM card. The designed Android application decoded them into their binary representation as described above.

The modulated flashlight propagates along a free space, light shielded, short length and small diameter channel to the receiver module as shown in the block diagram. The receiver circuit consists of a photodetector which sends an equivalent electronic signal to an Arduino Uno kit equipped with an ATMEGA microcontroller for analog to digital conversion, data processing and signal decoding. The microcontroller is programmed with certain threshold values adjusted to the intensity of the Xenon flashlight to allow correct bit recognition. The programmed thresholds have been determined by measuring the intensity of the received light for both the on and the off state at a fixed short distance. The decoded information is then transmitted via a serial port to the computer and displayed on the screen.

Two identical transmitters as well as receiver circuits are used and placed at a variable distance from each other in order to test the interference caused by the transmitter smartphone on an adjacent second card reader or ATM machine.

IV. Results and Discussion

First, the flashlight is modulated using OOK with non-return-to-zero (NRZ) bit duration t_b of 50 ms. As a photodetector, a light dependent resistor (LDR) is used. The normalized light intensity of both transmitted and received data are displayed in Fig. . The transmitted flashlight was detected by the LDR, however, the system failed to detect the bits correctly even when the data rate has been further reduced. Higher errors occurred especially when long trains of consecutive '1's or consecutive '0's were transmitted. This is because the signal carrying flashlight was out of synchronization with the detector circuit, which is mainly because the Xenon flashlight has large built-in capacitors which need a relatively long time to charge and discharge to provide such high brightness to the flashlight when turned on. Being designed solely for lighting and photography purposes, not for communication, the response time of the flashlight is relatively high and inconsistent between consecutive bits. The delay accumulated vastly with increasing number of transmitted bits, resulting in no error-free transmission of the required information at any data rate.



SS	D0 … D18	FS	Y Y M M	D23 D24 D25	D26 … D35	ES	D37
;	PAN (Primary Account Number)	=	Expiration	Service Codes	Discretionary Data	?	LRC

Fig. 1 Numerical characters on track 2 of an ATM card

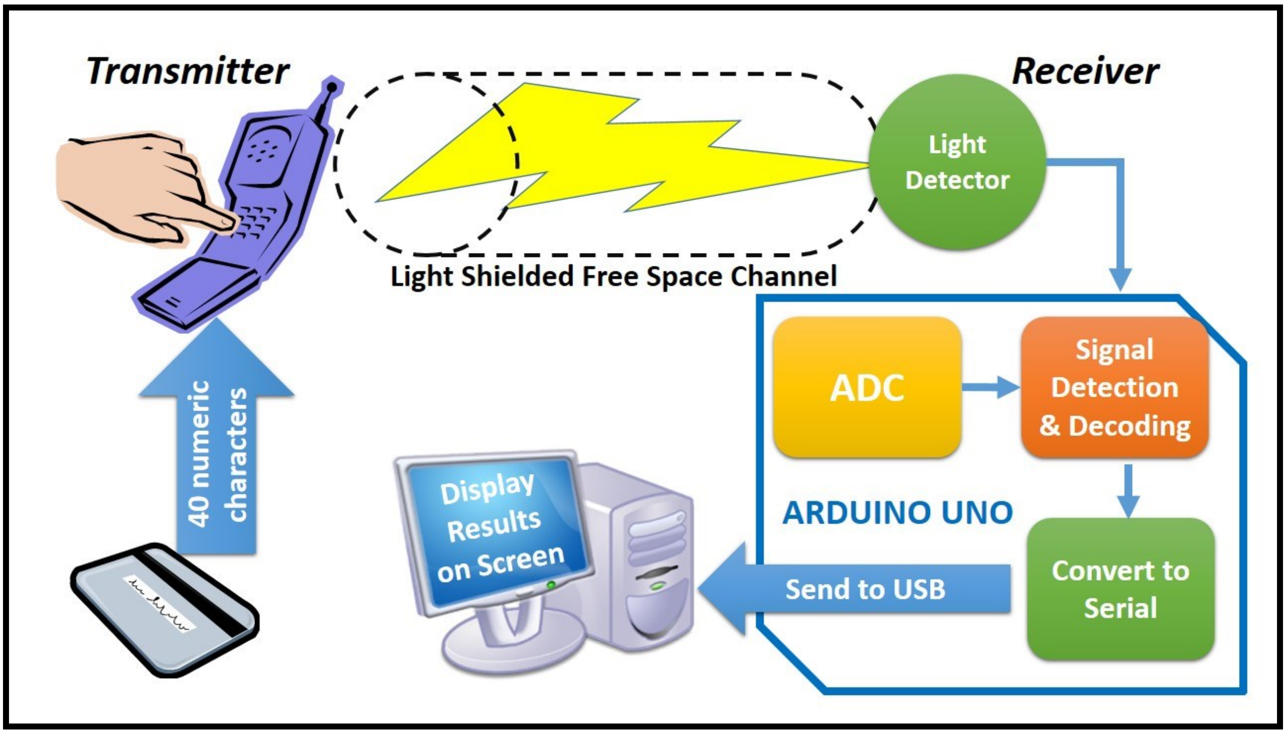


Fig. 2 Block Diagram of the implemented system

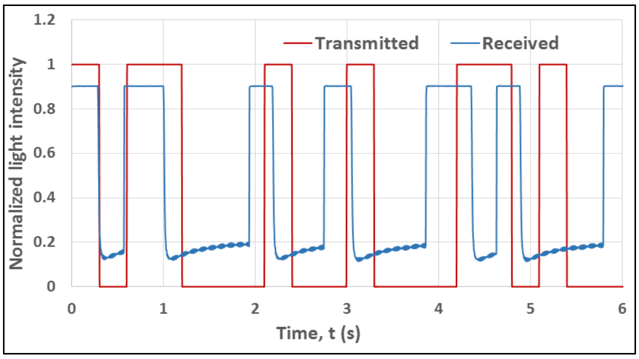


Fig. 3 The normalized light intensity of the transmitted and received signals with OOK modulation

In order to overcome this synchronization problem, PWM is used to encode the Xenon flashlight. This modulation technique uses return-to-zero (RZ) bits to ensure a transition of state after each bit. The ‘0’ and ‘1’ bits are transmitted over t_b and $3t_b$ of high intensity respectively, followed by t_b of zero intensity. This way, the system is able to detect exactly when each bit starts and ends, even when their width is not consistent. As a result, high synchronization between both transmitted and received signals is achieved using the PWM technique as shown in Fig. 4. This experimental setup results in error-free transmission of the data for data rates up to 4.2 bps (i.e. t_b = 230ms, assuming equal probability of ones and zeros). The bit error rate (BER) rises rapidly for higher speeds and oscillates about a value of 0.4 as shown in Fig. 5.

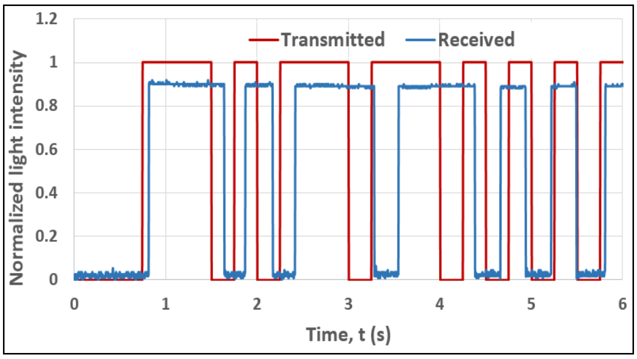


Fig. 4 The normalized light intensity of the transmitted and received signals with PWM modulation

In order to increase the speed of transmission, a photodiode with much higher sensitivity and lower response time than the LDR [13, 14] was used to detect the light signal. While the LDR has a rise and fall time of 18 and 120 ms respectively [13], a photodiode has a response time of only 1.5 µs [14]. As a result, error-free transmission is achieved at higher data rates reaching 15 bps (i.e. t_b = 22 ms assuming equal probabilities for ‘0’s and ‘1’s) as shown in Fig. 5. The figure compares the BER of the three experimental configurations at different data rates and shows that while OOK failed at all data rates, error-free transmission is successfully achieved when using PWM. Significant improvement of more than 300% in the transmission speed was obtained by replacing the LDR with a photodiode. Different channel length between 2 and 35 cm have been tested and showed no significant change of the achieved results, since the brightness of the Xenon flashlight exceeded that of the complete darkness provided by the light shield. However, when the light shield is removed, ambient light from the environment starts affecting the performance of the system resulting in more errors in detection. When the light shield is removed and the receiver circuit is 10 cm away from the transmitter in an indoor environment with an ambient light similar to a bank location, the system could only perform error-free at data rates of 11 bps or below, which is a nearly 30% drop of the error-free data rate compared to the light shielded experiment as shown in Fig. 5.

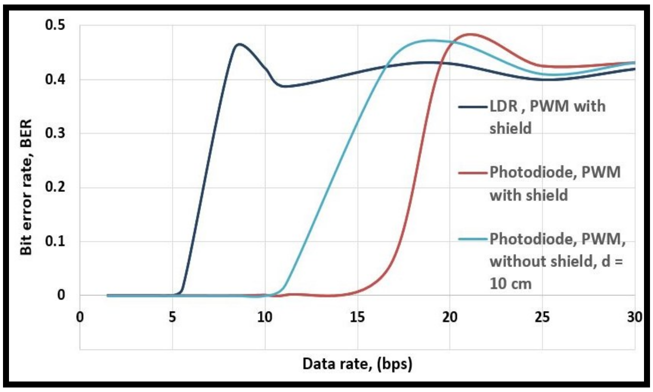


Fig. 5 Bit error rate with rising data rate with different experimental setups

Since more than one ATM machine or card reader are usually placed adjacent to each other in most stores and locations, it is important to test the performance of the system under the effect of interference caused by another transmitter placed close by. First we have tested the system with the presence of the light shield, which blocks out every light signal from the environment. The nearby transmitter had no effect on the system performance at any distance, since the light shielded channel allowed only light from the correct transmitter to be received by the photodetector placed in direct line of sight (LOS) with the transmitter. When the light shield is removed however, the Xenon flashlight was scattered in multiple directions affecting its environment, as shown in Fig. 6 which shows a snapshot of the Xenon flashlight of a smartphone taken at complete darkness with a digital camera set at very low shutter speed. The image shows clearly that the flashlight propagates in all directions, with the highest intensity being in the exact center of the flashlight and fading exponentially towards the circumference.

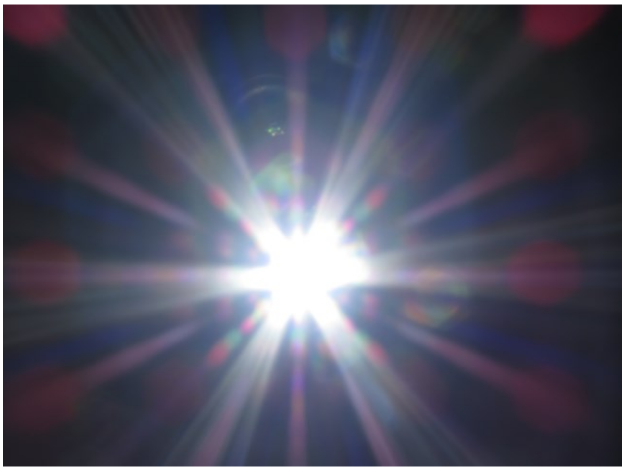


Fig. 6 Dispersion of a Xenon flashlight - snapshot taken in complete darkness

The illustration in Fig. 7 shows that at a distance of 10 cm from the receiver, the Xenon flashlight spreads in a cone-like manner with a circular base. At distances larger than 7 cm from the center of the base circle, the intensity of the flashlight starts to fall below half of its value at the center of the circle, and hence is below the threshold value considered as ‘high’ by the receiver circuit.

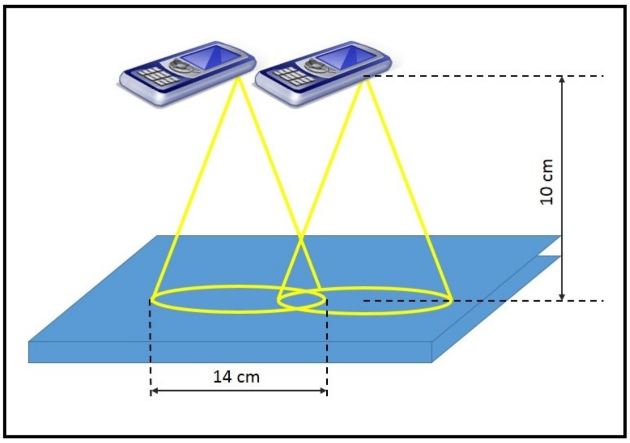


Fig. 7 Illustration showing the interference caused by another transmitter

When another transmitter is placed near the original transmitter smartphone, the intensity of its flashlight is however added to that of the original transmitter and may be detected as ‘high’ by the receiver module, which results in a significantly rising error rate. From this experimental setup we deduce that another transmitter causes an interference on the original signal when placed at a distance of 14 cm or less. It is therefore recommended to either place the receiver circuits more than 14 cm away from each other forcing the transmitters to be out of the range of interference or preferably install a short distance light shield concentric with the photodetector, which guarantees that the photodetector receives highest brightness from the intended transmitter phone and which completely blocks the interference signal from another transmitter smartphone flashlight.

V. Speed and Security of the Proposed System

While a data rate of 15 bps is considered very slow in the field of communication, it is sufficient in the case of user – machine interaction. In order to test the effect of the system speed on the user experience, we have measured the average time it takes 20 different individuals to access their bank account from an ATM machine, starting from the point when they insert their ATM card in the machine to the point when they have full access of their bank account and are ready for doing the financial transaction, including entering their pin number. The average time measured for this process is around 45 seconds, with some individuals having more trouble entering their PIN codes correctly. In comparison, it will only take less than 15 seconds to have full access to your bank account using the proposed system. In addition, it’s more user friendly, since the individuals don’t need to enter their PIN codes every time they are trying to access their bank account, since the system is already secured by the security features of the smartphone itself. This will eliminate the chances of any wrong passcodes being entered and the whole process being repeated, which wastes more time.

In addition to being faster and more user friendly than the regular ATM card, the proposed system is also considered more secure. Thieves stealing an ATM card can have full access to the bank account information of the card owner if they just know the 4 or 6 digit numeric PIN, which they retrieve easily either by guessing or by placing a hidden camera above the keypad of the ATM machine to capture the keypad strokes of the user. In comparison, the data stored on the smartphone's memory can be protected from hackers or thieves using multiple layers of security, which prevents it from being misused even if the phone is stolen or lost. First of all, the smartphone can be locked using not only a numeric but also an alphanumeric random length password, which is much harder to guess than the PIN of the ATM card. For even more security, the smartphone can be set up to unlock only when the moving face of its owner is detected or when a pre-programmed complicated pattern is recreated on the lock screen. Furthermore, the user has the option of allowing the designed payment application only to open upon entering another complicated user-chosen password, face image or even voice signature. The designed application also hides the real numbers of the credit card after the first setup and shows a number of bullets instead, which prevents any individual viewing the application from knowing or copying the credit card details entered by the owner. Moreover, all Android devices nowadays can be located and accessed from any web browser using the owner's account to delete all the saved data on the device before the hacker or thief has access to it on the stolen device. Last, the visible light communication (VLC) link is considered more secure than NFC or Wi-Fi since it requires a direct line of sight (LOS) between the transmitter and the receiver. Hence, any device used for eavesdropping must cut the direct LOS link and would cause the attack to be detected and stopped.

VI. Conculsion

This paper practically replaces the magnetic ATM card with mobile payment using visible light communication by modulating the built-in Xenon flashlight of an Android smartphone. While OOK failed to provide error-free transmission of the needed credit card information to the implemented microcontroller based hardware supplementary module, the change of the modulation scheme to PWM resulted in an error-free transmission of the 200 bits with data rates of 4.2 and 15 bps using LDR and photodiode as photodetectors respectively. Further investigations of the system performance under the effect of the interference from another transmitter smartphone proved the importance of a short length light shielded channel and showed that even without light shield, two transmitters can be placed at distances of 14 cm or more without altering the results. Since the system employs a visible light link - which requires direct LOS - as well as depends on the multi-level smartphone security for saving the credit card information, it is considered even more secure than the regular magnetic card and other alternatives such as RF and Wi-Fi.

References

[1] Amy K. Karlson, Brian R. Meyers, Andy Jacobs, Paul Johns, and Shaun K. Kane, "Working Overtime: Patterns of Smartphone and PC Usage in the Day of an Information Worker", Proceedings of Pervasive Computing, May 2009, pp 398-405.

[2] Diniz, Eduardo Henrique, João Porto de Albuquerque, and Adrian Kemmer Cernev, "Mobile Money and Payment: a literature review based on academic and practitioner-oriented publications (2001-2011).

[3] Blöchlinger, Michael. "Mobile Payment Systems." Internet Economics VI (2012): 41.

[4] G. Inc., "Google Wallet," 2012-2013. [Online]. Available: http://www.google.com/wallet/.[Accessed 30 June 2013].

[5] S. Inc., "Square," 2009-2013. [Online]. Available: https://squareup.com/. [Accessed 30 June 2013].

[6] M. Roland, J. Langer, and J. Scharinger: Applying Relay Attacks to Google Wallet. In: Proceedings of the 5th International Workshop on Near Field Communication (NFC 2013), Zurich, Switzerland, Feb. 2013, pp. 1-6

[7] T. Hesselmann, N. Henze, and S. Boll, "FlashLight: optical communication between mobile phones and interactive tabletops", in Proc. ITS, 2010, pp.135-138.

[8] Browning, D., & Kessler, G.C. (2009, May). Bluetooth Hacking: A Case Study. In G. Dardick (Ed.), Proceedings of the Conference on Digital Forensics, Security and Law, May 20-22, 2009, Burlington, VT, pp 57-71.

[9] "Aeronautics and Space.", 14 CFR 91.21. 2010

[10] A. . S. Shirazi, C. Winkler and A. Schmidt, "Flashlight Interaction: A Study on Mobile Phone Interaction Techniques with Large Displays," in *ACM 978-1-60558-281-8.*, Bonn, Germany, 2009.

[11] Galal, M.M.; Fayed, H.A.; El Aziz, A.A.; Aly, M.H., "Smartphones for Payments and Withdrawals Utilizing Embedded LED Flashlight for High Speed Data Transmission," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on, pp.63,66, 5-7 June 2013

[12] Information technology -- Identification cards -- Financial transaction cards, ISO/IEC 7813:2006

[13] RS, "Light dependent resistors," NORP12 datasheet, Mar. 1997.

[14] OSRAM, "Silicon photodiode for the visible spectral range," BPW21 datasheet, Apr. 2007.