IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 25, 2018, accepted November 8, 2018, date of publication November 26, 2018,
date of current version December 27, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2883250

LuxSteg: First Practical Implementation of Steganography in VLC

GRZEGORZ BLINOWSKI[1], (Member, IEEE), PIOTR JANUSZEWSKI[2], GRZEGORZ STEPNIAK[2], AND KRZYSZTOF SZCZYPIORSKI[2], (Senior Member, IEEE)

[1]Institute of Computer Science, Warsaw University of Technology, 00-665 Warsaw, Poland
[2]Institute of Telecommunications, Warsaw University of Technology, 00-665 Warsaw, Poland

Corresponding author: Grzegorz Blinowski (g.blinowski@ii.pw.edu.pl)

This work was supported by the Institute of Telecommunications, Warsaw University of Technology, through the Statutory Grant of the Polish Ministry of Science and Higher Education.

ABSTRACT Visible-light communication (VLC) is a new technique for high-speed, low-cost wireless data transmission services. One of the areas in which VLC is considered superior to traditional radio-based communication is security. The common slogan summarizing the VLC security features is WYSIWYS—"What You See Is What You Send." However, the broadcast nature of downlink VLC makes it possible for eavesdroppers to easily intercept the light communication in various settings, e.g., offices, conference rooms, plenum spaces, and so on. Similarly to radio-based data broadcasting systems, such as Wi-Fi, VLC opens the possibilities of hiding information in the public channel. In this paper, we describe (for the first time, to the best of our knowledge) the implementation of steganographic data transmission in a VLC system called LuxSteg. This VLC system utilizes pulse position modulation and direct sequence-code division multiple access modulation. In our implementation, multiple steganographic data streams are mixed with the spreading codes and combined with the overt data stream. We achieve a steganographic transmission rate of approximately 1 Mb/s hidden in a 110-Mb/s data stream. We analyze the influence of the spreading factor, spreading code type, number of hidden data streams, and the amplitude on the achievable transmission rate, undetectability, and robustness.

INDEX TERMS Communication system security, computer networks, network security, visible light communication.

I. INTRODUCTION

VLC is a novel wireless technology that was first proposed in the early 2000s for indoor and outdoor applications (see [1] and [2]). For indoor environments, VLC was proposed for several applications, including replacing radio frequency (RF)-based communication in offices [3], multimedia broadcasting [4], peer-to-peer data exchange (i.e. in Personal Area Networks - PANs), multimedia broadcasting in home audio and video systems [5]–[7], and geo-localization [8], [9]. The bulk of the commercial VLC systems currently available provide data broadcasting services, including solutions for public venues such as airports and train stations, museums, shopping and exhibition centers, as well as accessibility for disabled persons. Fully duplex VLC systems are currently the subject of intensive study, and are often considered as a component of hybrid communication systems [10].

VLC technology is considered to be more secure "by design" than traditional radio-based techniques. This is because the directivity and high obstacle impermeability of the optical signals in VLC are considered to provide a more secure way (compared to RF) of transmitting data within an indoor environment, making the signal difficult to intercept from outside. "What You See Is What You Send" (WYSIWYS) [11] is the common catchphrase used to summarize VLC security features. Recent research shows, however, that as with fiber-optic, and radio-based wireless networks, security issues must not be ignored or downplayed. In [12] transmission "snooping" was addressed, while in [13], the risk of various forms of attacks on VLC networks was described and classified.

According to [14], "steganography [...] is the art of embedding secret messages (steganograms) in a certain carrier, possibly to communicate them in a covert manner." Network steganography is the family of methods that uses telecommunication protocols as a carrier for hidden data. These methods [15] utilize modifications of packets to

perform covert communication by modifying the structure of the packet (e.g. the payload or protocol-specific fields), or by modifying time relations among packets (e.g. changing the sequence of the packets or inter-packet delays). Wireless protocols and systems such as those based on VLC are especially prone to various network steganography alterations because of the relatively huge bandwidth available at the physical layer.

The possibility of implementing steganography in VLC systems was addressed for the first time in [16]. Both the physical (PHY) and media access control (MAC) layers of VLC as possible carriers of hidden data transmission were considered, and different steganographic techniques were proposed. For each of the introduced techniques, the potential for bandwidth and undetectability was discussed.

In this paper, we describe (for the first time to our knowledge) an implementation of steganographic data transmission in VLC - *LuxSteg*. Our implementation is built into a VLC system which utilizes Direct Sequence-Code Division Multiple Access (DS-CDMA) modulation. In this system, steganographic data is mixed with orthogonal codes and added to an overt signal modulated in a Pulse Position Modulation (PPM) scheme. Our system is evaluated numerically and experimentally, and we establish the baseline for the maximal overt data rate, test steganographic transmission scenarios and collect data on the maximum hidden transmission rate and bit error rate (BER) using the basic parameters of steganographic transmission: amplitude, number of hidden data streams and spreading factor. We also test two spreading codes commonly used with DS-CDMA: orthogonal variable spreading factor (OVSF) and Gold codes.

It is worth mentioning that there is a number of papers proposing steganographic techniques in optical fiber transmission: [17]–[21]. These techniques are specific to optical fiber transmission and rely on phenomena present in optical fiber channel, for example - self-coherent detection of optical-phase-modulated signal of amplified spontaneous emission noise [17], applying pulse stretchers at transmitter [18], [19] or fiber chromatic dispersion [20], [21]. However, none of them can be applied to VLC, as this is intensity modulated free-space channel.

The structure of this paper is as follows: Section 2 contains a short introduction to the techniques used and covers VLC basics and the principles of DS-CDMA modulation. In Section 3, we describe our experimental setup, the principles of its operation and the idea of implemented hidden data transmission. In Section 4, we discuss the results (the achieved overt- and covert- data transmission rates), address the influence of modulation parameters on steganographic performance measures, and discuss the issue of detectability. Section 5 summarizes the paper.

II. VLC DATALINK – PRINCIPLES OF OPERATION

A VLC physical layer consists of a transmitter and receiver. In the transmitter, one of two types of white-light LED is used:

- red-green-blue (RGB) emitters
- blue LED on a yellow-light emitting phosphorus layer (''single-chip'' LED)

The second type is more widespread in LED luminaries due to its energy efficiency, lower cost and lower complexity. The choice of LED luminaire depends mainly on the environment: for indoor illumination purposes, high power LED arrays are typical, and low power devices are used in mobile appliances such as smartphones, tablets, etc.

The development of VLC was initially driven by demonstrations of growing transmission rates and more elaborate transmitter-receiver setups. A simple single-chip LED driven by a single modulation source achieved a bandwidth of approx. 2.5 MHz for the white and 14 MHz for the blue component [22]. A data throughput of up to 40 Mb/s has been demonstrated in a single-emitter–single-receiver scenario with simple analogue pre-equalization at the transmitter [23].

A combination of equalization and blue component filtering[1] raised the achieved data rate to 75 Mb/s [24]. A data throughput of 100-230 Mb/s has been demonstrated in a single-emitter–single-receiver scenario and On-Off Keying (OOK) [25]. Data transfer rates of up to 1 Gbps were attained with more advanced modulation techniques and by employing arrays of separately driven light sources and multiple receivers (VLC MIMO) [26].

In the receiver, the incoming light is collected and concentrated on a photo-detector. Various optical concentrators are used, ranging from simple one-lens designs to active fluorescent concentrators [27]. The receiver may use a simple low-cost photo-sensor (e.g. a photodiode) or a more complex imaging sensor (a CMOS array) - which is the case in personal devices. The photocurrent generated in the photodetector is amplified and fed to the D/A circuitry. With current technology, the major bandwidth limiting factor is not receiver design but rather the transmitter, channel loss and dispersion.

One of the major differences between VLC and RF-based technologies such as Wi-Fi or Bluetooth is that phase modulation cannot be used in VLC systems – the frequency band of visible light lies in the range of 430-770 THz, and the corresponding wavelength is 390-700 nm, which is significantly too short to encode information in the signal's phase (at least with current technology). Also, as LEDs have a limited linear operation region for electro-optical conversions, the modulating current signal must fall within strict amplitude constraints in order to avoid undesirable nonlinear effects. At the receiver, demodulation depends on direct detection at the receiver, hence Intensity Modulated/Direct Detection (IM/DD) modulation techniques are used in VLC. The major challenge in a VLC system is to obtain the highest possible data transmission rate while minimizing BER, and the system must also allow for light dimming (in case of infrastructure systems). With white-based LED VLC

[1]The slow response of yellow phosphorus to blue light modulation limits its spectral component bandwidth to 2MHz, hence the yellow component is filtered out at the receiver and only the blue component is detected.

systems, various modulation schemes have been demonstrated, including:

- *OOK* – in the simplest form of OOK modulation, the data bits 1 and 0 correspond to the LED being turned on and off respectively. As an alternative, in the 0 state, the LED's light intensity is reduced instead of it being completely turned off. The advantages of OOK are simplicity and ease of implementation.
- *Pulse Width Modulation (PWM)* – this scheme uses a rectangular waveform with the information encoded in its duty cycle. The pulse widths may be adjusted depending on the desired light dimming level.
- *Pulse Position Modulation (PPM)* – the amplitude and width of pulses in the waveform are constant, and the transmitted symbol is encoded in the pulse's position in a series of pre-defined time slots.
- *Variable Pulse Position Modulation (VPPM)* –proposed specifically for VLC transmission, this is a hybrid of PPM and PWM. As in PPM, VPPM optical symbols are encoded in pulse time position. Pulse width may be changed to achieve different dimming levels as in PWM.
- *Code-division multiple access (CDMA)* – this is a multiple access modulation scheme allowing multiple users to share a band of frequencies. This scheme employs spread-spectrum technology and a special coding scheme where each transmitter is assigned a pseudo-random spreading code.
- *Orthogonal Frequency-Division Multiplexing (OFDM)* – the communication channel is divided into multiple low-frequency, narrow band, orthogonal subcarriers over which the data is sent in parallel substreams. Standard RF-based OFDM techniques need to be adapted for application in VLC IM/DD techniques because OFDM generates complex-valued bipolar signals which need to be converted into real values.
- *Frequency Shift Keying (FSK)* – the data is encoded by discrete frequency changes of a carrier signal. Two (binary frequency shift keying, BFSK) or more (multiple frequency shift keying, MFSK) baseband frequencies may be used. In VLC, FSK is typically used in simple LED-ID systems [28].

The principles of OOK, PWM and PPM are illustrated in Fig. 1. The principle of DS-CDMA is illustrated in Figure 2. The source signal is multiplied by an orthogonal code with a frequency much higher than that of the source signal. Different codes may be used for different data sources, hence more than one hidden data stream may be transmitted at once. At the receiver, the signals are separated by correlating the received signal with the locally generated code for the desired user.

Our experimental VLC system uses two types of modulation: PPM and DS-CDMA. The overt data signal is encoded by PPM, while the steganographic signal is modulated with DS-CDMA. Both signals are modulated separately and added to the analogue output circuit. The CDMA scheme has been previously proposed for VLC systems [29] and there are

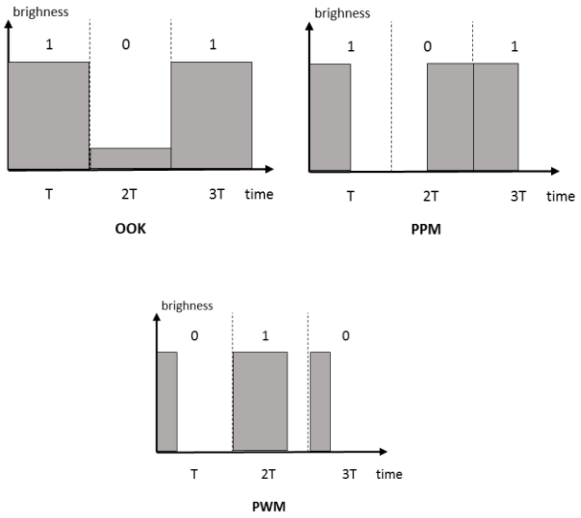


FIGURE 1. The principles of OOK, PPM, PWM modulation in VLC.

several specific reasons for using DS-CDMA for steganographic data transmission in VLC:

- CDMA is resistant to multipath interference – the delayed reflections of the transmitted pseudo-random codes have poor correlation with the original code, and thus appear as data from another user, which is ignored at the receiver. This is an important feature in indoor environments, where reflections from the walls and other objects cause severe speed degradation due to potential inter symbol interference (ISI).
- CDMA effectively rejects narrow band interference, which in the case of VLC may be caused by external light sources. Because narrow band interference affects only a small portion of the spread spectrum signal, it can easily be removed through notch filtering without significant loss of information.
- CDMA can transmit multiple data-streams to multiple users, which is practical for steganographic scenarios [30].

Our motivation for using CDMA signaling to hide covert data lies in its well-known immunity to interference from other sources, which in our case is mainly the overt signal. This feature allows for a very high reduction in the amplitude of the stealth signal, which makes it more difficult for the network operator to detect the presence of this signal. This ability of the CDMA system is described by the processing gain coefficient, which is defined in (1).

$$G_p = \log_{10}(W/R) = 10\log_{10} N \tag{1}$$

where W is the chip rate, R is the data bit rate and N is the code length or spreading factor (SF). The SF is the major characteristic of DS-CDMA modulation and is defined as the ratio of the chip rate and symbol rate, where chip rate is the rate of the pseudo-random noise and symbol rate is the rate of the data signal being transmitted. The higher the SF, the higher the processing gain, but also the lower the

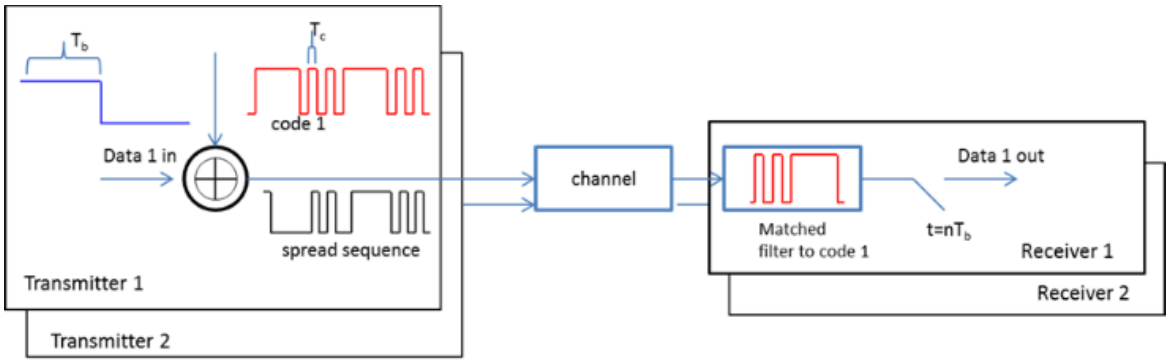


FIGURE 2. The principle of DS-CDMA modulation.

stealth channel bit rate. Typically, the chip rate is significantly larger than the symbol rate, i.e. one symbol is represented by multiple chips. In our system, SFs between 210 to 214 were considered. The choice of spreading code plays a crucial role in system performance. The best performance occurs when the signal of one of the data sources is separated from the sources of other signals.

The block diagram of a DS-CDMA system (for one spreading code) is shown in Figure 2. In the transmitter, the data bits are modulo 2 added to the spreading code sequence and sent to the channel. The receiver correlates the incoming signal with the same code as was used at the transmitter in a matched filter and samples at times when correlation peaks occur. The values of the correlation peaks are subsequently decoded to bits. Multiple transmitters and receivers may be used, provided that their spreading codes are different.

The separation is made by correlating the received signal with the locally generated code sequence of the i-th source. Hence, the code sequence should exhibit properties of good auto-correlation, and cross-correlation should be as close to zero as possible [31]. Different spreading codes have been proposed for DS-CDMA [32], and in our system we consider two popular types – OVSF and Gold codes:

- *OVSF codes* are orthogonal codes generated from a complete binary tree that reflects the construction of Hadamard matrices. OVSF codes are used in UMTS systems.
- *Gold codes* are generated by XOR-ing maximum length sequences [33] and are characterized by small cross-correlation. Gold codes are used in GPS systems.

In our system, each PPM pulse carries 1 bit, so there are two pulse positions available. The chip rate of CDMA is set to twice the baud rate of PPM, which means that 2 chips are transmitted during one PPM symbol. Thus, the SF and the number of CDMA channels determine the covert channel bit rate. CDMA provides a spreading gain, which facilitates the reception of covert signals at amplitudes far lower than that of the main signal. The spreading gain increases with SF. Hence, the amplitudes of covert channels can be decreased for a higher SF while maintaining the same transmission quality in both covert and overt channels. However, a higher SF means a lower covert channel data rate.

It should be noted that the introduction of an additional covert channel at the VLC transmitter must affect the transmission quality in the overt channel. This is a consequence of the information theory restrictions on channel capacity: (i) an additional non-orthogonal channel is an additional noise source to the overt channel; (ii) the transmitter power is shared between two signals, so it is effectively lowered in the overt channel. However, if the overt channel operates with forward error correction (FEC) and assumes a certain signal to noise ratio (SNR) margin, the post-FEC BER will not be affected by the covert channel. This may also be viewed from a different perspective: the total channel rate is a sum of the capacities of the overt and covert channels, and cannot exceed Shannon's channel capacity. The drop in transmission quality in the overt channel due to the presence of the covert channel will depend on the ratio of data rates in both channels and the total channel capacity following Shannon's formula. Note that a different scenario, where a separate transmitter is used for the covert channel, is also possible. In that case, the overt signal power remains the same regardless of the presence of the covert signal. However, the drop in quality due to interference still occurs, and receiver overdrive must also be considered.

III. EXPERIMENTAL SETUP

A. DATA TRANSMISSION SYSTEM

Fig. 3 illustrates the block diagram of the proposed LuxSteg data transmission system. The overt data stream (overt data) is modulated in the PPM block, while the steganographic block (steg $data_i$) consists of 1 to 16 data sources separately modulated by XOR-ing with n orthogonal codes. The whole signal modulation process is implemented in software (Matlab package was used) and uploaded as a file to the arbitrary waveform generator module (AWG – Tektronix model 71122), which drives the analog circuitry. A commercially available LED (Osram LE UW Q9WP) is used as a transmitter. The LED is driven by the voltage source at room temperature. The light is transmitted via the atmosphere over a variable

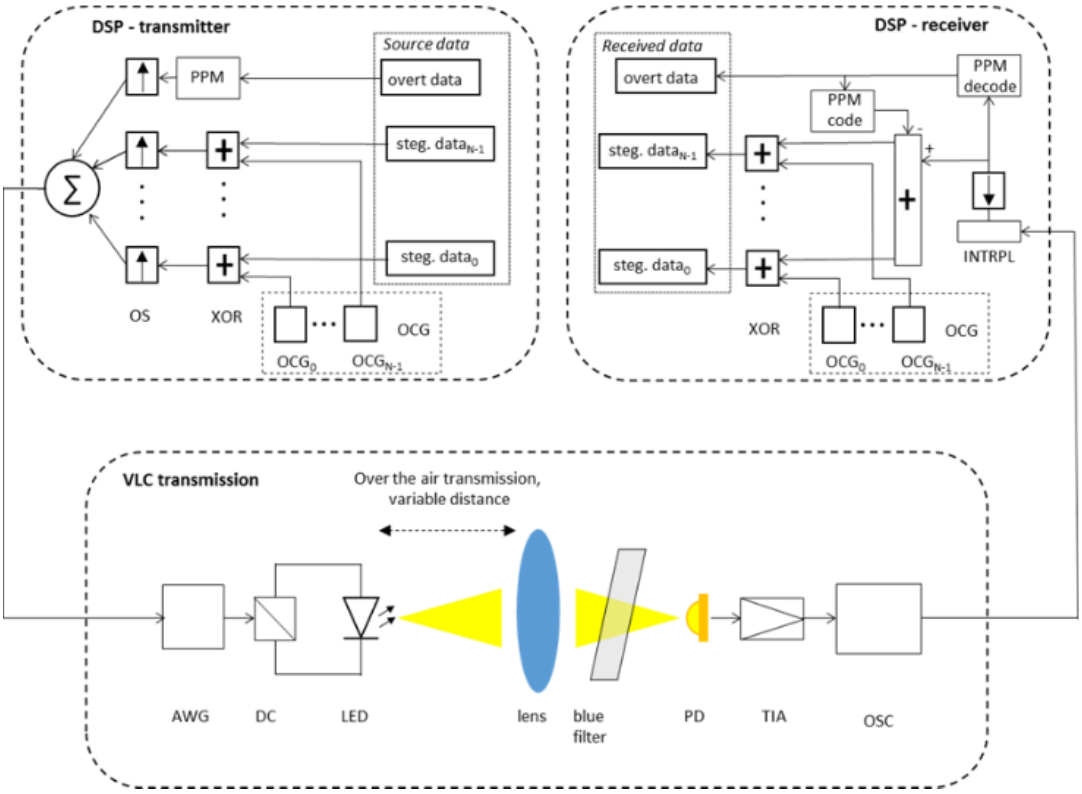


FIGURE 3. Block diagram of DS-CDMA VLC steganographic system. The module blocks are abbreviated as follows: PPM – Pulse Position Modulator, OS – oversampling, OCG – orthogonal code generation (for DS-CDMA), INTRPL – interpolation, AWG – arbitrary waveform generator, DC – driving circuit, PD – photo detector, TIA – transimpedance preamplifier, OSC – oscilloscope.

distance to the receiver. In the experiment, the illumination at the receiver plane was approximately 500 lux, which corresponds to typical lighting conditions in office rooms. On the receiving side, a lens, a blue filter, a p-i-n diode photodetector (PD – Hamamatsu S5972 of 0.8 mm diameter) and a MAX3665 transimpedance preamplifier (TIA) are used. The received signal is sampled at a rate of 2.5 Gs/sec. by a digital oscilloscope (OSC – Lecroy 202MX). The sampled signal is digitally filtered to cut out noise and transmitted on-line via Ethernet to the DSP program implemented in Matlab (DSP). The oscilloscope is used both for real-time signal quality verification (eye-diagrams) and as a source of digital unprocessed data for further processing. To improve the detection quality of the covert signal, the interference from the overt channel is removed first. This is done as follows: in the receiving DSP module, the overt component is demodulated, then fed back to the ''PPM code'' which restores the sent overt PPM signal, and then subtracted from the received signal. The resulting hidden component is convoluted with orthogonal codes to obtain the hidden data.

B. EXPERIMENT VERIFICATION

Before the LuxSteg transmission system was built and tested, a series of numerical tests were conducted. In these tests, the analogue part was simulated in Matlab [34] as the AWGN channel and the LED response was modeled with the standard *exp(-t/T)H(t)* function (where $H()$ is the Heaviside function and T is the *1/e* decay time constant). The simulations were conducted to verify the feasibility of the proposed steganographic transmission scheme and to establish the transmission parameters influencing SNR, namely:

- Steganographic signal amplitude necessary to achieve desired SNR under different values of SF.
- Dependence of noise and interference on SF and the choice of spreading code (OVSF, Gold).
- Dependence of noise and interference on the number of simultaneous steganographic streams.

Fig. 4 shows the relationship between steganographic signal amplitude and desired SNR for different values of SF. We can observe that longer spreading codes require a relatively lower signal level to achieve the desired SNR. At the same time, as was noted in Section 2 – larger SF values provide for lower hidden data transmission rates. In this case, SNR relates only to the AWGN introduced in the channel. An OVSF spreading code was used in this simulation. In this scenario, the amplitude values guarantee BER below the FEC threshold.

We also tested the influence of SF and choice of spreading code on the noise level, namely, the noise level of the signal obtained when the overt PPM component is removed. In Fig. 5, the standard deviation of signal convoluted with the

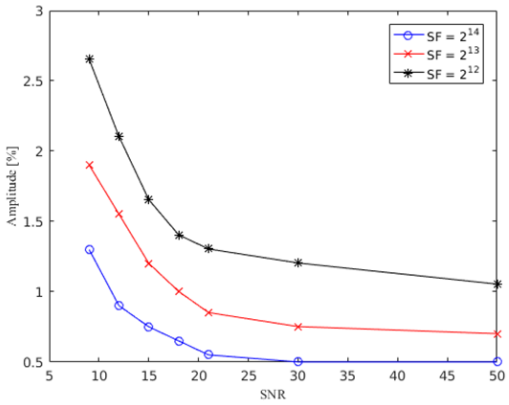


FIGURE 4. Simulation results – dependence of required steganographic signal amplitude on SNR for different values of SF. Amplitude is shown relative to (as a percent of) the overt-signal (PPM modulated) amplitude.

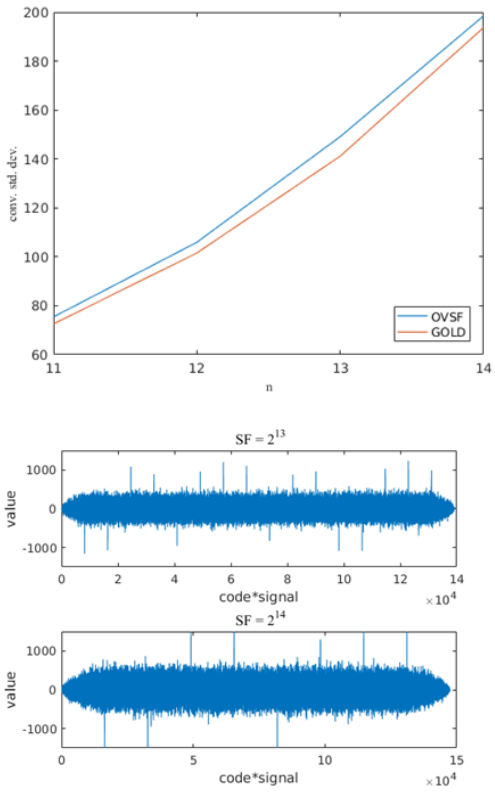


FIGURE 5. Simulation results – noise standard deviation as a function of SF; below – the received signal convoluted with the orthogonal code after the PPM signal was subtracted from it.

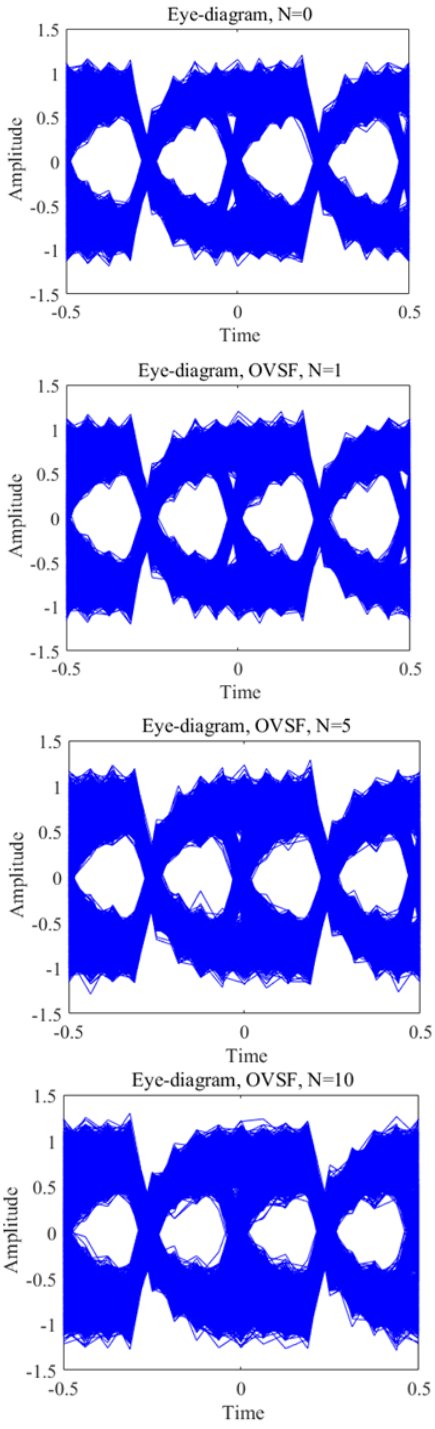


FIGURE 6. Received signal's eye-diagrams depending on the number of simultaneous steganographic data streams (N). OVSF codes were used in these simulations.

spreading code is shown to illustrate noise levels of the signal with no overt component. We can observe that a longer SF results in greater interference from the original signal "left-overs". Indeed, noise and interference of the signal with the subtracted overt component increase in power level when SF values increase. This is also illustrated on the lower part of the plot which shows the de-correlated signal for two SF values (Gold codes were used in this case).

In Fig. 6, the eye-diagrams obtained from the simulations are shown for different values of simultaneous steganographic data streams (N), where N is set to: 0 (no steganographic transmission), 1, 5 and 10. In this simulation, SNR in the channel was set to 27.5dB, SF was 2048, and the amplitude was adjusted for the steganographic transmission

to be decodable at the receiver. We can observe how the eye-diagrams close when N is increased, hence an increase in the number of steganographic streams in the signal results in the reception conditions of the overt signal becoming worse, and in consequence leads to detection of the hidden transmission. On the other hand, a reasonable small number of hidden data streams with the amplitude adjusted to the SF will pass undetected to the observer.

IV. EXPERIMENTAL RESULTS

A. THROUGHPUT AND BER

During the experiment, the primary goal was to test the feasibility of our steganographic scheme and to identify the influence of SF, steganographic component amplitude, spreading code choice and the number of steganographic channels on overall system performance. In the preliminary phase, we established the baseline – i.e. achievable transmission speed with no steganographic content. BER in relation to transmission speed is shown in Fig. 7. For overt transmission speed of 110 Mbps without error correction coding, BER is below $5{\cdot}10^{-4}$.

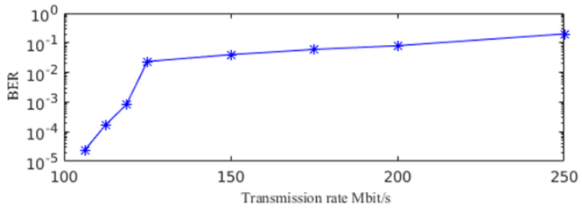


FIGURE 7. BER measured as a function of PPM transmission speed (no hidden data).

In the second phase, steganographic data was introduced into the channel. An SF of 2048 was used with N varied between 1 and 15 and steganographic signal amplitude (A_s) from 1% to 5% of the PPM signal. Fig. 8 shows eye-diagrams for "pure" PPM and a 10 source ($N = 10$) steganographic transmission. The presence of hidden transmission is clearly visible in this case.

To measure the reliability of overt transmission depending on the volume of steganographic data, we conducted a series of BER measurements using both Gold and OVSF spreading codes with $A_s = 5\%$, SF $= 2048$, and N varied. The results are summarized in Fig. 9. We can conclude that Gold codes are superior to OVSF with respect to reliability.

To determine the influence of the steganographic component on the overt signal, we used a penalty parameter. This shows how much we need to increase the power of the PPM signal when the steganographic signal is introduced to get same BER when no CDMA signal is present. Due to difficulties in power adjustment in the experimental setup, we calculated this relationship numerically (Fig. 10). The plot shows that the "penalty" that is introduced by the hidden transmission is in the range of 0.3 – 0.4 dB.

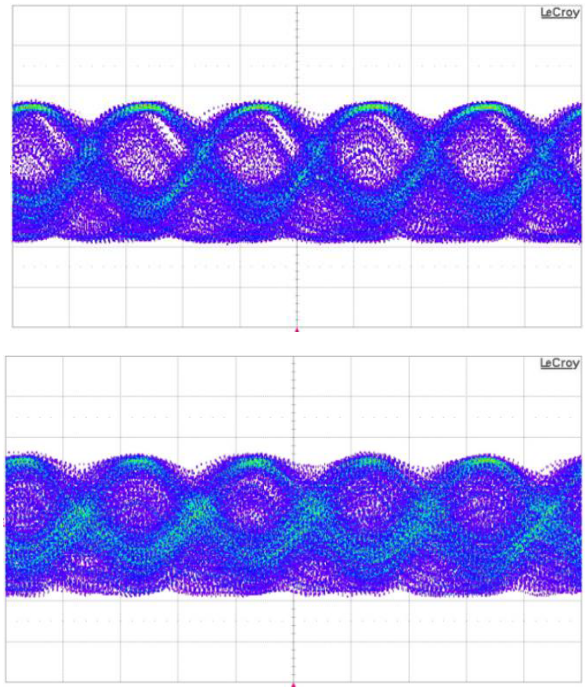


FIGURE 8. Signal received: eye-diagrams: no steganographic data (top), N = 10 signal (bottom).

B. STEGANOGRAPHIC TRANSMISSION RATE

The upper theoretical rate of steganographic transmission in a system with DS-CDMA modulation can easily be calculated as follows:

$$R_{bsteg} = \frac{2R_{bPPM}}{SF} \tag{2}$$

where R_{bPPM} is the transmission rate for the overt (PPM) channel, SF is the spreading factor and N is the number of simultaneous steganographic sources. During the experimental tests we were able to achieve R_{bsteg} of 0.976 Mbps with $R_{bPPM} = 110\ Mbps$, $SF = 2048$, $N = 10$ and Gold codes – which is close to the limit defied in (2) – 1.074 Mbps. However, we must note that the transmission was hardly undetectable – as described below.

C. PERFORMANCE AND UNDETECTABILITY

Any method of network steganography can be characterized by four basic and interdependent features: maximal transmission rate, undetectability, robustness and cost. Steganographic bandwidth describes how much secret data can be sent via the channel using the particular method per time unit; undetectability is defined as an inability to detect a steganogram; robustness is defined as the amount of alteration that a steganogram can withstand without its secret data being destroyed; and cost describes the degree of degradation of the carrier caused by the steganogram insertion procedure. For each method of network steganography, there is always a tradeoff between the above features. Typically we want to maximize the steganographic transmission rate and still remain undetected [35].

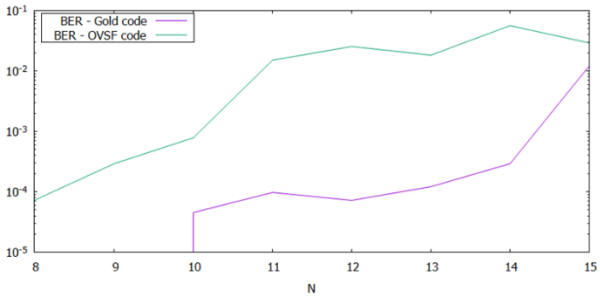


FIGURE 9. BER for the PPM (overt) signal measured for gold and OVSF spreading codes, measured for 100 Mbit/s bit rate.

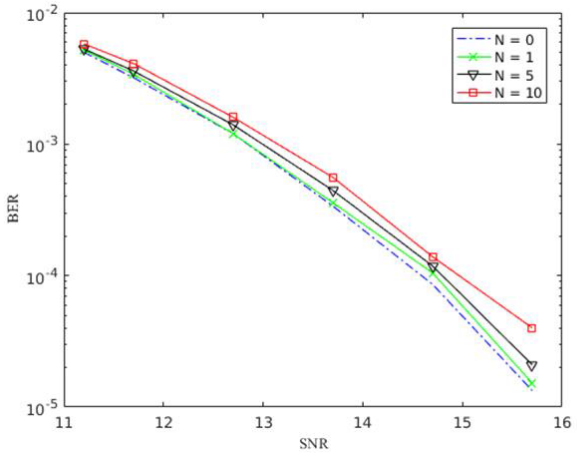


FIGURE 10. SNR to BER relation with no steganographic data (N = 0) and with a steganographic signal introduced (N = 1, 5, 10).

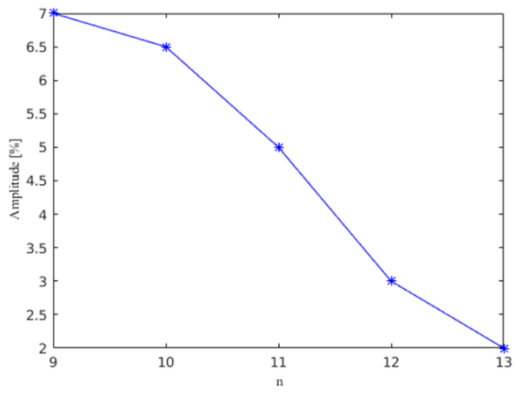


FIGURE 11. Steganographic amplitude required for reliable transmission as a function of SF. OVSF code was used.

In Fig. 11, we show the A_s required for reliable overt and steganographic transmission depending on the length of the SF. As was previously determined in the simulations, the longer the spreading code, the lower amplitude of steganographic signal with respect to PPM signal is required. The amplitude determined during the experiment proved to be higher than that obtained during the simulation (compare with Fig. 4). This is caused by an additional noise factor not accounted for in the numerical model.

In LuxSteg the transmitter has a significant degree of freedom regarding the tradeoff between bandwidth and undetectability. SF and As can be varied – for desirable robustness (BER) with large values of SF, amplitude may be reduced and multiple transmissions may be conducted; conversely, a low value of SF and high amplitude permits for one transmission. These tradeoffs are summarized in Table 1.

TABLE 1. Summary of basic parameters on overall DS-CDMA steganographic system characteristics.

Characteristic	SF (increase)	N (increase)	A_s (increase)
robustness	increases	no influence	increases
transmission rate	decreases	increases	no influence
undetectability	increases	decreases	decreases
cost	no influence	decreases	decreases

In [36], a broad qualitative classification of steganographic methods for wireless network communication was proposed which were based on the idea of a moving observer. For a full explanation of this classification method, we refer the reader to this cited article. A short summary of the classification follows:

Three levels of undetectability are ''good'', ''bad'', and ''ugly'', defined as

- ''*Good*'' – the observer is unable to detect hidden communication at the source of the steganograms.
- ''*Bad*'' – the observer is able to detect hidden communication at the source of the steganograms, but is unable to detect this communication when he/she is moved away from the source.
- ''*Ugly*'' – the observer is able to detect hidden communication anywhere in the network, even at the steganographic receiver.

With respect to the above classification, we can consider LuxSteg as ''*Bad*'', because detection of this method is possible only in proximity of the steganographic sender (transmitter), where the hidden transmission is below noise, when the observer has a proper code. Only setting up improper parameters like amplitude or SF can increase the probability of catching this covert transmission.

V. SUMMARY

In this paper, we have experimentally demonstrated LuxSteg - a steganographic VLC system that is capable of delivering 0.976 Mbps of DS-CDMA traffic encoded in 10 separate streams hidden in 110 Mbps of a PPM encoded overt data stream. We have discussed the tradeoffs between undetectability, robustness and maximal transmission rate specific for our system, the major ones being: the simultaneous increase in undetectability and decrease in rate with the increase of spreading factor, and the simultaneous decrease in undetectability and increase in rate with the growing number of simultaneous steganographic streams. We must also note, that, the full implementation of the system would require use

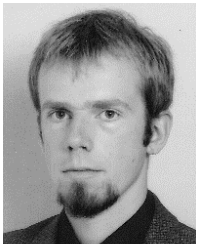
of forward error correction (FEC) both for overt and covert channel. However, it is commonly assumed that for 7% FEC overhead errorless transmission can be achieved when pre-FEC BER is below 1e-3 which is in accordance with BER values that we have obtained.

REFERENCES

[1] S. Hranilovic, L. Lampe, and S. Hosur, "Visible light communications: The road to standardization and commercialization," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 24–54, Jul. 2013.
[2] A. Tsiatmas, C. P. M. J. Baggen, F. M. J. Willems, J.-P. M. G. Linnartz, and J. W. M. Bergmans, "An illumination perspective on visible light communications," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 64–71, Jul. 2014.
[3] M. B. Rahaim, A. M. Vegni, and T. D. C. Little, "A hybrid radio frequency and broadcast visible light communication system," in *Proc. IEEE Global Commun. Conf. (GLOBECOM) Workshops*, Dec. 2011, pp. 792–796.
[4] L. B. Chen *et al.*, "Development of a dual-mode visible light communications wireless digital conference system," in *Proc. 18th IEEE Int. Symp. Consum. Electron. (ISCE)*, Jun. 2014, pp. 1–2.
[5] K.-D. Langer *et al.*, "Optical wireless communications for broadband access in home area networks," in *Proc. Int. Conf. Transparent Opt. Netw. (ICTON)*, Jun. 2008, pp. 149–154, doi: 10.1109/ICTON.2008.4598756.
[6] D. C. O'Brien *et al.*, "Home access networks using optical wireless transmission," in *Proc. IEEE 19th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2008, pp. 1–5.
[7] D. C. O'Brien *et al.*, "Gigabit optical wireless for a home access network," in *Proc. IEEE 20th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2009, pp. 1–5.
[8] M. Yoshino, S. Haruyama, and M. Nakagawa, "High-accuracy positioning system using visible LED lights and image sensor," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2008, pp. 439–442.
[9] Z. X. Ren, H. M. Zhang, L. Wei, and Y. Guan, "A high precision indoor positioning system based on VLC and smart handheld," *Appl. Mech. Mater.*, vol. 571–572, pp. 183–186, Jun. 2014.
[10] M. Ayyash *et al.*, "Coexistence of WiFi and LiFi toward 5G: Concepts, opportunities, and challenges," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 64–71, Feb. 2016.
[11] J. P. Conti, "What you see is what you send," *Eng. Technol.*, vol. 13, no. 19, pp. 66–67, Nov. 2008.
[12] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proc. 2nd ACM MobiCom Workshop Visible Light Commun. Syst. (VLCS)*, 2015, pp. 9–14.
[13] G. Blinowski, "Practical aspects of physical and MAC layer security in visible light communication systems," *Int. J. Electron. Telecommun.*, vol. 62, no. 1, pp. 7–13, 2016.
[14] E. Zielinska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," *Commun. ACM*, vol. 57, no. 3, pp. 86–95, 2014.
[15] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr, and K. Szczypiorski, *Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures*, 1st ed. Hoboken, NJ, USA: Wiley, 2016.
[16] G. Blinowski and K. Szczypiorski, "Steganography in VLC systems," *J. Universal Comput. Sci.*, vol. 23, no. 5, pp. 454–478, 2017.
[17] B. Wu *et al.*, "Optical steganography based on amplified spontaneous emission noise," *Opt. Express*, vol. 21, no. 2, pp. 2065–2071, 2013.
[18] M. P. Fok and P. R. Prucnal, "Compact and low-latency scheme for optical steganography using chirped fibre Bragg gratings," *Electron. Lett.*, vol. 45, no. 3, pp. 179–180, Jan. 2009.
[19] Z. Wang and P. R. Prucnal, "Optical steganography over a public DPSK channel with asynchronous detection," *IEEE Photon. Technol. Lett.*, vol. 23, no. 1, pp. 48–50, Jan. 2011.
[20] B. B. Wu, P. R. Prucnal, and E. E. Narimanov, "Secure transmission over an existing public WDM lightwave network," *IEEE Photon. Technol. Lett.*, vol. 18, no. 17, pp. 1870–1872, Sep. 2006.
[21] B. Wu, M. P. Chang, B. J. Shastri, P. Y. Ma, and P. R. Prucnal, "Dispersion deployment and compensation for optical steganography based on noise," *IEEE Photon. Technol. Lett.*, vol. 28, no. 4, pp. 421–424, Feb. 15, 2016.
[22] D. C. O'Brien, L. Zeng, H. Le-Minh, G. Faulkner, and J. W. Walewski, "Visible Light Communications: challenges and possibilities," in *Proc. Int. Symp. Pers., Indoor Mobile Radio Commun. (IEEE PIMRC)*, Cannes, France, Sep. 2008, pp. 1–5.
[23] H. Le Minh *et al.*, "High-speed visible light communications using multiple-resonant equalization," *IEEE Photon. Technol. Lett.*, vol. 20, no. 14, pp. 1243–1245, Jul. 15, 2008.
[24] L. Zeng *et al.*, "Equalisation for high-speed visible light communications using white-leds," in *Proc. 6th Int. Symp. Commun. Syst., Netw. Digit. Signal Process.*, Jul. 2008, pp. 170–173.
[25] K.-D. Langer *et al.*, "Exploring the potentials of optical-wireless communication using white LEDs," in *Proc. 13th Int. Conf. Transparent Opt. Netw.*, Jun. 2011, pp. 1–5.
[26] A. H. Azhar, T. Tran, and D. C. O'Brien, "A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications," *IEEE Photon. Technol. Lett.*, vol. 25, no. 2, pp. 171–174, Jan. 15, 2013.
[27] R. Mulyawan *et al.*, "MIMO visible light communications using a wide field-of-view fluorescent concentrator," *IEEE Photon. Technol. Lett.*, vol. 29, no. 3, pp. 306–309, Feb. 1, 2017.
[28] G. Blinowski and A. Kmieciak, "Modelling and evaluation of a multi-tag LED-ID platform," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, 2016, pp. 1049–1056, doi: 10.15439/2016F89.
[29] C. Yang, Y. Wang, Y. Wang, X. Huang, and N. Chi, "Demonstration of high-speed multi-user multi-carrier CDMA visible light communication," *Opt. Commun.*, vol. 336, pp. 269–272, Feb. 2015.
[30] P. Łąka and P. Maksymiuk, "Steganographic transmission in optical networks with the use of direct spread spectrum technique," *Secur. Commun. Netw.*, vol. 9, no. 8, pp. 771–780, 2015, doi: 10.1002/sec.1379.
[31] H. Chen, D. Hank, M. E. Maganaz, and M. Guizani, "Design of next-generation CDMA using orthogonal complementary codes and offset stacked spreading," *IEEE Wireless Commun.*, vol. 14, no. 3, pp. 61–69, Jun. 2007, doi: 10.1109/MWC.2007.386614.
[32] J. K. Holmes, "Spread spectrum systems for GNSS and wireless communications," in *GNSS Technology and Applications Series*. Norwood, MA, USA: Artech House, 2007.
[33] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA, USA: Holden-Day, 1967.
[34] D. Srivastava and R. K. Prasad, "Spreading codes performance for correlation function using MATLAB," *Int. J. Electron., Commun., Instrum. Eng. Res. Develop.*, vol. 3, no. 2, pp. 15–24, 2013.
[35] I. S. Moskowitz, L. Chang, and R. E. Newman, "Capacity is the wrong paradigm," in *Proc. New Secur. Paradigms Workshop (NSPW)*, 2002, pp. 114–126.
[36] K. Szczypiorski, A. Janicki, and S. Wendzel, "The good, the bad and the ugly: Evaluation of Wi-Fi steganography," *J. Commun*, vol. 10, no. 10, pp. 747–752, Oct. 2015, doi: 10.12720/jcm.10.10.747-752.

GRZEGORZ BLINOWSKI (M'18) was born in Warsaw, Poland. He received the M.Sc. and Ph.D. degrees in computer science from the Faculty of Electronics and Information Technology, Institute of Computer Science, Warsaw University of Technology, Poland, in 1993 and 2001, respectively. He received the Certified Information Security Professional Certificate in 2014. Since 2001, he has been an Assistant Professor with the Parallel and Distributed Computing Research Group, Institute of Computer Science. He is the author of two books. His areas of research and scientific interests include distributed memory systems, dataflow and macro-dataflow systems, distributed computer systems, software engineering, Internet technology, network, and system security—especially in the context of WSN and IoT and, recently, VLC systems. He twice received the Warsaw University of Technology Rector's Award for Academic Achievements.

PIOTR JANUSZEWSKI was born in Otwock, Poland. He received the B.S. degree in telecommunications from the Warsaw University of Technology, Warsaw, Poland, in 2017, where he is currently pursuing the M.Sc. degree. His current research interests are focused on information hiding and network security.



GRZEGORZ STEPNIAK was born in Warsaw, Poland. He received the M.Sc., Ph.D., and D.Sc. degrees in telecommunications from the Warsaw University of Technology, Warsaw, in 2005, 2009, and 2016, respectively. He has published over 20 papers in the IEEE/OSA journals and many others in conference proceedings. His research interest covers wide aspects of optical transmission: advanced modulation formats in direct detection systems, multimode fiber transmission, holographic waveform shaping, and optical wireless communications. He has been distinguished by The Polish Ministry of Science and Higher Education Award for Outstanding Young Scientists 2015.

KRZYSZTOF SZCZYPIORSKI (M'13–SM'13) was born in Warsaw, Poland. He received the M.Sc. (Hons.), Ph.D. (Hons.), and D.Sc. (Habilitation) degrees in telecommunications from the Faculty of Electronics and Information Technology (FEIT), Warsaw University of Technology (WUT), Poland, in 1997, 2007, and 2012, respectively. He also completed the postgraduate studies in psychology of motivation at the University of Social Sciences and Humanities, Warsaw, in 2013. He graduated in advanced networking from Budapest Tech (now Óbuda University), Hungary, in 2003, and the Hass School of Business, University of California at Berkeley, in 2013. He is currently a Professor of telecommunications with the Institute of Telecommunications (IT), FEIT, WUT, where he is the Head and the Co-Founder of the Cybersecurity Division. Since 2015, he has been the Co-founder and the R&D Director of Cryptomage S.A—a cybersecurity company. He has been the Director of Cybersecurity Bureau, Polish Chamber of Digital Economy, since 2016. He is the author or the co-author of over 190 papers, three patent applications (one is granted), and over 80 invited talks. He is a Senior Member of the American Society for Research. He has been an Expert Member (since 2015) and the Vice-Chairman (since 2016) of the Telecommunication Section, Electronics and Telecommunications Committee, Polish Academy of Sciences.