



Research article

Jens R. Ziehn*, Masoud Roschani, Miriam Ruf, Dennis Bruestle, Jürgen Beyerer and Melanie Helmer

Imaging vehicle-to-vehicle communication using visible light

<https://doi.org/10.1515/aot-2020-0038>

Received June 30, 2020; accepted October 26, 2020;

published online November 19, 2020

Keywords: connected driving; cooperative driving; cybersecurity; VLC; V2V; V2X.

Abstract: With advances in automated and connected driving, secure communication is increasingly becoming a safety-critical function. Injection of manipulated radio messages into traffic can cause severe accidents in the foreseeable future, and can currently be achieved without having to manipulate on-board vehicle systems directly, for example by hijacking cellphones instead and using these as senders. Thereby, large-scale attacks on vehicles can be executed remotely, and target relatively vulnerable devices. To mitigate remaining vulnerabilities in current automotive security architectures, this paper proposes a secondary communication channel using vehicle head and taillights. In contrast to existing approaches, this method allows both to achieve a sufficient data rate *and* to extract the angular position of the sender, by means of an imaging process which only requires close-to-market, cost-efficient technology. Through this, injecting false messages by masquerading as a different sender is considerably more challenging: The receiver can verify a message's source position with the supposed position of the sender, e.g. by using on-board sensors or communicated information. Thereby, reliably faking both the communicated messages *and* the position of the sender will require direct manipulation of on-board vehicle systems, raising the security level of the function accordingly, and precluding low-threshold, wide-range attacks.

1 Introduction and motivation

With increasing levels of automated driving, connected driving functions are also gaining importance and complexity: Connected updates of navigation maps, traffic jams and road hazard warnings are already established applications. A direct inclusion of connected data in automated maneuver decisions, however, opens up new ways to improve traffic safety and efficiency.

The key to leveraging these advantages is establishing trust in data and intentions communicated by other traffic participants, as seen for example in Frese and Beyerer [13] or Tas et al. [27]. This allows for a reduction of safety distances without a reduction of safety, as in Batz et al. [2], or the execution of emergency maneuvers without a direct line of sight. At the same time, trust increases vulnerability: Consequences of a manipulated communication can reach from traffic obstructions up to severe accidents. Taking advantage of the trust established by connected and cooperative driving without the risk of misuse cases therefore is a core challenge in developing such driving functions.

We describe the working principles of a system, originally introduced by Ziehn et al. [35], which supplements current radio-based vehicle-to-vehicle (V2V) communication by a secondary channel using *visible light communication* (VLC); specifically the modulation of humanly invisible authentication messages onto LED head and taillights. While the data rate, which is even under favorable conditions limited to the kilohertz domain (cf. Section 2.3), is far lower than radio-based communication, it provides a significant increase in cybersecurity, by allowing to accurately localize the source of the signal, and thus to uniquely authenticate the sender. This is achieved by exploiting the “rolling shutter effect” in CMOS sensors, which enables the proposed *imaging transmission of information*: Message data and sender

*Corresponding author: Jens R. Ziehn, Fraunhofer IOSB, Karlsruhe, Germany, E-mail: jens.ziehn@iosb.fraunhofer.de

Masoud Roschani, Miriam Ruf and Dennis Bruestle, Fraunhofer IOSB, Karlsruhe, Germany

Jürgen Beyerer, Fraunhofer IOSB, Karlsruhe, Germany; and KIT Vision and Fusion Laboratory, Karlsruhe, Germany

Melanie Helmer, Karlsruher Institut für Technologie (KIT), Lichttechnisches Institut (LTI), Karlsruhe, Germany

position are received simultaneously in a single measurement within a low-cost system.

2 Background and state of the art

The proposed system concerns the areas of connected driving, cybersecurity, communication channels, as well as the exploitation of the so-called “rolling shutter effect”.

Radio-based vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I; generally vehicle-to-anything, V2X) is the backbone of connected driving, with heterogeneous applications ranging from non-critical functions such as onboard navigation up to safety-critical features such as cooperative perception, cooperative maneuver planning and cooperative collision avoidance (see [14, 13, 27]).

For the discussion of risks in automated driving, we distinguish between *safety* (against accidents, for example by airbags) and *security* (against cyberattacks, for example by encryption), which coincide in the given scenario. Cyberrisks in automated and connected driving are the subject of extensive research, due to their potential serious consequences, and are mitigated by advanced countermeasures, for example as described by Petit and Shladover [24], Yağdereli et al. [33] or Weimerskirch [30]. Attacks may either require physical presence at the vehicle, or be conducted remotely, by exploiting vulnerabilities in connected features. Physical presence at the vehicle can generally allow for a wide range of manipulations; however, the threat of sabotage is not specific to automated and connected vehicles, and such attacks are risky and logistically complicated. By contrast, attacks on vehicles that can be carried out remotely are novel to connected driving. Targets may include, beside privacy and property, also safety-critical features, for example vehicle control or the airbag system (see Dürrwang et al. [9, 10]). To authenticate messages and senders, *public key infrastructures* (PKI, details in Whyte et al. [31], Bißmeyer et al. [3]) are implemented, which provide a high level of security, but are vulnerable to theft of certificates or keys (see Schramm et al. [25] for side channel attacks, and Matrosov et al. [21] for a description of the Stuxnet attack). The risk for attacks on connected driving is increased by the possibility to send V2X-compatible radio signals from a wide range of devices, including cellphones, whereas the receiver must rely on the message contents (including certificates) to identify the sender, as V2X radio signals are generally undirected.

An alternative to radio transmission is the so-called *visible light communication* (VLC), which is already in use

today for a variety of applications. Data are typically sent by LED light sources, and received by photodiodes (an overview of applications is given by Khan [20]), which are undirected like radio antennae, but may be subject to visual occlusion. The commonly noted advantages of VLC include a license-free and less cluttered bandwidth, but also security advantages by increased protection against eavesdropping and directional sending, as described by Jovicic et al. [19]. Disadvantages include sensitivity to stray ambient light, the relatively low data rate and range, and the disadvantages of visual occlusion.

Applications that used the directed information of light for localization purposes are described by Jovicic et al. [19], Yoshino et al. [34] and Moon et al. [23]; however, the application of interior ego-localization avoids the challenge of providing sufficient data rates for highly dynamic environments. The necessity for localized but fast transmission of data is pointed out by Yamazato [32], with two solutions given: High-speed cameras with frame rates of 1000 FPS (frames per second), and a system described by Takai et al. [26] and extended in Goto et al. [15] named Optical Communication Image Sensor (OCI). Both transmit high-frequency data packages that cannot be visually perceived by the human eye, but allow for localization in camera images at close to pixel accuracy. However, prices of several hundred USD/EUR for high-speed consumer cameras (such as the Sony IMX382 introduced 2017), which at that still only provide low resolutions (640×80 px VGA or less), indicate that general automotive applications are currently unlikely. OCI on the other hand provides a specialized image sensor which, in addition to regular image pixels, introduces *communication pixels* (CPx) which are distributed in alternating columns with regular image pixels (IPx) across the sensor surface. These are based on photodiodes which can be selected upon signal detection and read at rates of up to 55 Mbit/s. For the development of OCI, the focus is on the considerably improved data rate with respect to high-speed cameras, which allows to use VLC as a stand-alone data channel. The approach provides a regular image from the IPx, as well as a binary image mask for regions of high-frequency signals, and signal data from these regions, both from the CPx, which allow localizing the sender if optical effects such as halation (overflow) do not excessively dilate the CPx’ detection region.

The VLC method proposed herein, in contrast, is limited to the same data rates as extracting the signal directly using 1000 FPS cameras (as given by Yamazato [32]; possibly moderately higher under favorable conditions), but enables the localized and simultaneous

reception from a large number of VLC senders using only market-ready, cost-efficient technology. For this, the system exploits the rolling shutter effect, a usually undesired but at least tolerated temporal artifact in CMOS sensor images. This effect (details in Section 2.2) has been used in various applications to measure fast or high-frequency information (e.g. by McCloskey and Venkatesha [22] and Davis et al. [7]), including the reception of VLC, by Danakis et al. [6], Chow et al. [5] and Do and Yoo [8]. An automotive V2X application is described by Ji et al. [18] which transmits data using a vehicle’s taillights, and receiving data using the rolling shutter effect. The authors note security gains by limiting the transmission to a direct line of sight, while localized transmission of high data rates is not intended.

2.1 Principle

The aim of the proposed *imaging V2V communication* is to transmit data using modulated vehicle lights under the following constraints:

- The legally required light function must be preserved
- Data reception must support multiple sources, including an angular direction for each source, to allow localizing and thereby authenticating the sender of a message, e.g. by comparison with other vehicle sensors
- Transmission rates must be sufficient for the intended security gains (details in Section 2.3)
- Emission and reception of data must only require available and low-cost technology that allows for automotive applications

No other solution is known that satisfies these requirements with currently available technology.

If data transmission via VLC is to avoid visual disturbance, a constant average intensity and a sufficiently high flicker frequency must be assured in accordance with ECE regulations (cf. UNECE Regulation 48 [29], 112 [28] and 123 [28]). A constant average intensity for arbitrary bit sequences of data is achieved through *Manchester encoding* (as described by Cailean et al. [4]) (Figure 1), which represents a **0** bit as the sequence [on, off], and a **1** bit as the sequence [off, on]. At frequencies above the *flicker fusion rate* (also *critical flicker fusion frequency CFF*), which depends on absolute and relative intensities of the signal, the human eye perceives such a signal with the constant average intensity. Experiments with the proposed system indicate that in the given application, switching frequencies of at least 1000 Hz are required for disturbance-free signal modulation at

maximum bright-dark contrast¹. If a signal of this frequency was to be received by a high-speed camera with an according frame rate of 1000 FPS or more, costs would be significant, with typical automotive or consumer cameras operating at only around 15 to 60 FPS.

2.2 Reception using “rolling shutter”

The goal of receiving and localizing VLC messages that use switching frequencies of at least 1000 Hz motivates the following approach. The most commonly used type of CMOS sensors is limited to reading one pixel line at a time, such that the entire image is read sequentially over lines (although exposure intervals may and will usually overlap). This gives rise to artifacts labeled “rolling shutter effects”, which includes geometric distortions as well as uneven light distribution for non-constant light sources. This effect is commonly tolerated in consumer cameras; in industrial applications, however, it can complicate image exploitation considerably, for example due to complex deformations from camera vibrations (as discussed by Hedborg et al. [16] or Baker et al. [1]). Therefore, industrial applications often rely on more complex CMOS sensors providing a *global shutter* that reads all pixels simultaneously.

A vertical image *column* containing multiple *lines* $y \in \{1, 2, \dots, Y\}$ can be modeled using a time- and line-dependent intensity $b(t, y)$, which is accumulated into a measurement $I(y)$ over an exposure time T_{exp} to give

$$I(y) = \int_{\tau(y)}^{\tau(y)+T_{\text{exp}}} dt b(t, y) \quad (1)$$

where $\tau(y)$ is the shutter motion over image lines, which is typically linear with a constant offset T_{line} between lines, $\tau(y) = y \cdot T_{\text{line}}$.

¹ The experiments included $N = 7$ persons, which were asked to judge visual disturbance from flicker using Manchester-encoded messages, both in the projected beam pattern and directly in the headlight, under various ambient light conditions. Frequencies significantly below 1000 Hz were perceived as disturbing, while frequencies near or above 1000 Hz were occasionally perceived as flicker, but not as disturbing. A similar scale is given by Yamazato [32]. While more rigorous and exhaustive experiments on visual disturbance and potential health effects clearly are required, these limited results strongly suggest that frequencies notably below 1000 Hz are likely inadequate. For general applications, the IEEE Std 1789–2015 “Recommended Practices for Modulating Current in High-Brightness LEDs” [17] provides an analysis of how modulation-related parameters affect visual disturbance and health effects in LED lights, however, this does not take into account the effect of communication messages modulated onto the light, or focus on the particular domain of automotive lighting.

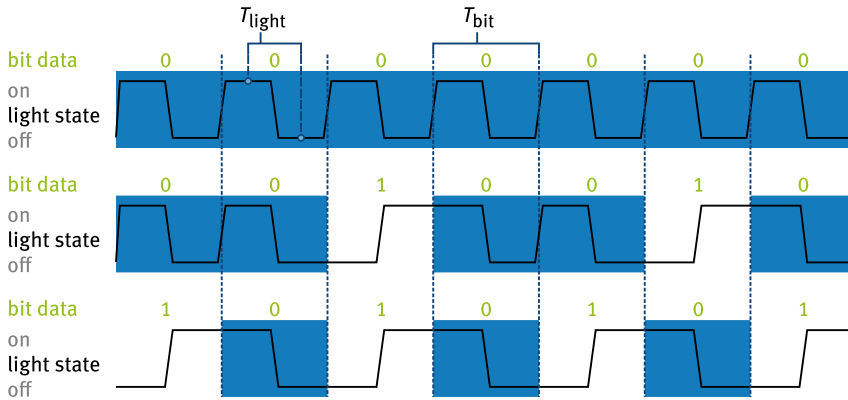


Figure 1: To achieve constant average intensity over time, Manchester encoding transforms n bits into $2n$ light states, which are switched at intervals of T_{light} . The data rate is $1/T_{\text{bit}}$. The visible-light frequency in turn varies between $1/T_{\text{bit}}$ for a constant bit sequence (above) and $1/2T_{\text{bit}}$ for an alternating bit sequence (below).

Generally for (integral) $n \geq T_{\text{exp}}/v$, two lines y and $y + n$ are exposed during strictly disjoint intervals. Thereby, the rolling shutter effect enables the reception of high-frequency data with low-cost technology, as shown in Figure 2.

At the same time, Figure 2C indicates why this setup is still insufficient to transmit V2V data: While the vehicle takes up a large portion of the image, the signal is visible only within a small image region; furthermore, the separation of signal and spatial information is difficult.

2.2.1 Optical Filtering and Localization

To allow a signal extraction along all image lines, an anisotropic optical low-pass filter (also *diffusor*) is introduced into the optical path, which distributes incident light

across the vertical axis by a “streak”, while maintaining a sharp horizontal resolution of the light source, allowing an accurate lateral localization of the sender (Section 3, Figure 3). Depending on the filter kernel in the vertical direction, the sender’s vertical position can only be extracted with lower accuracy, or not at all (for a wide kernel with near-homogeneous vertical light distribution). The process for resolving the vertical position, if possible, is given in Section 3. Note that the sensor and filter can be rotated freely about the viewing direction, leading to different streak directions, which may be advantageous for different applications. However, it is assumed for the automotive domain, where traffic participants are distributed mainly across the horizontal plane, that aligning the streak with the vertical scene axis (as shown here throughout) maximizes discriminability of senders by

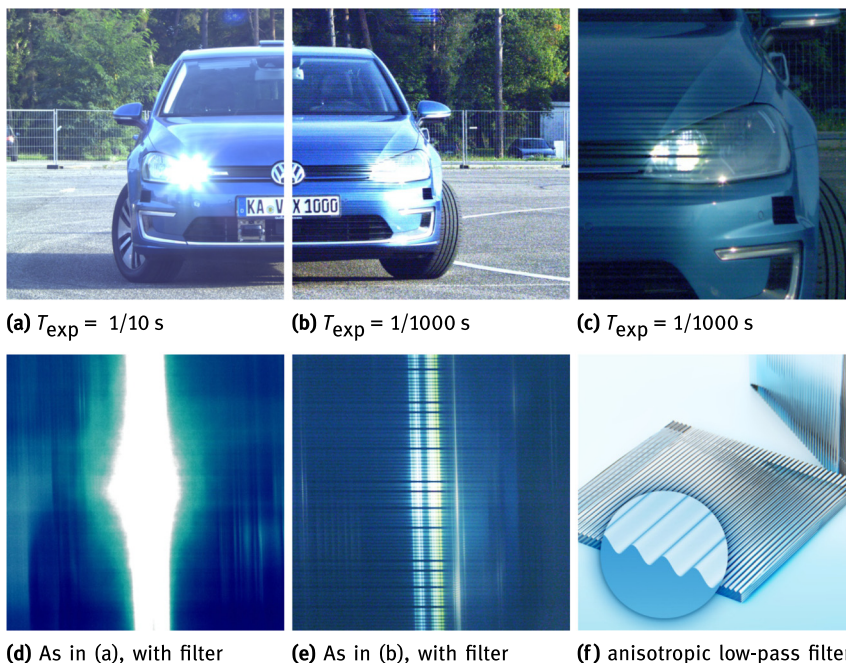


Figure 2: Headlights with Manchester-coded signal at a switching rate of $1/T_{\text{light}} = 1000$ Hz in a CMOS camera with different exposure times without (a–c) and with (d–e) an optical low-pass filter, shown in (f), which distributes the signal across the entire vertical axis.

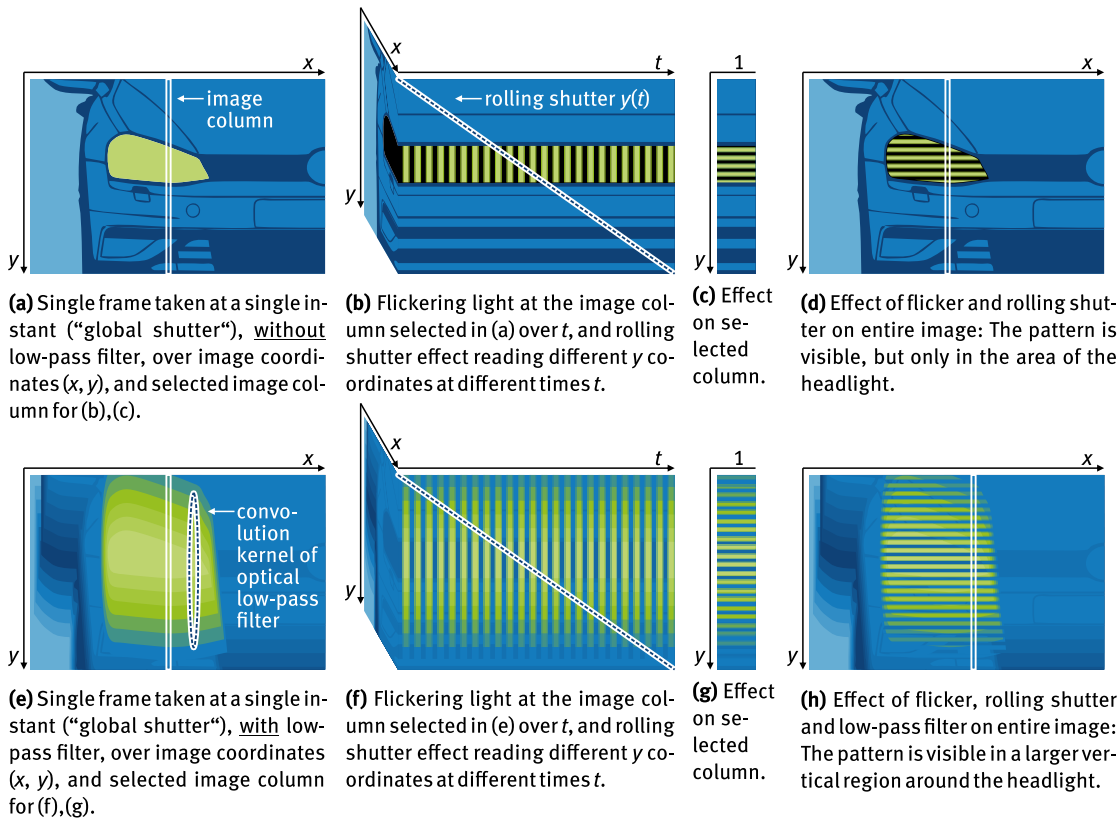


Figure 3: Overview of the relationship between image space (x, y) , time t , the rolling shutter effect $y(t)$ and the optical low-pass filter. The rolling shutter effect reveals the high-frequency flicker to the camera, by mapping time onto the vertical image axis (y) . Without an additional filter (upper row), the signal is only visible in the vicinity of the headlights. By introducing a low-pass filter into the optical path (lower row), incident light is distributed across a wider y interval by an anisotropic convolution kernel, such that more bits can be received. The incidence angle of the signal however can still be estimated: The horizontal x position is not affected significantly; the vertical y position can be estimated from the peak in the distribution, if applicable, as described in Section 3.

position, *and* minimizes overlapping light sources from different senders.

2.2.2 Signal extraction

The resulting image, as seen in Figures 2e, 7b, 7e, 7h, contains the signal along the vertical axis, such that by $T_{\text{line}} < T_{\text{light}}$, different light states are mapped to different lines. For Figure 2, for example, $T_{\text{line}} \cdot 18 \approx T_{\text{light}} = 1/1000$ s, such that individual bits span several lines. Synchronization between sender and receiver can be aided by referencing the signal to GPS times, or via radio-based communication. Sections 2.3 Sections 2. and 3 will outline, however, that for the intended purpose of improved cybersecurity, the signal and its timing can be expected to be known by the receiver a priori, and is only verified, such that a constant offset can be calibrated and compensated using the message constants themselves. Do note for overlapping streaks, signal extraction and sender localization are far more difficult, if not

impossible: Signals and peaks will overlap, such that processing and extraction as in Section 3 is not applicable. However, the overlap of two priorly known, different signals can in theory be verified similarly, though no such experiments were conducted so far. It is expected that practical applications should aim to minimize overlap.

2.3 Application for improved cybersecurity

The intended switching rate of only above 1000 Hz (Section 1) and practical results (Section 3) make it clear that the system is not, by far, laid out as a substitute for current V2X communication (which for example achieves 50 MBit/s for DSRC or HSPA+). In the ideal case of common low-cost cameras, which provide 50 FPS at 1080 pixel lines, a maximum of 27 kBit/s Manchester-coded data can be transmitted; under realistic operating conditions (Section 4), data rates will even be considerably lower. Also, many

current V2X applications rely on the vehicles establishing communication without a direct line of sight.

Improved cybersecurity thus cannot be achieved by relocating all V2X communication to the proposed imaging VLC. Instead, the VLC system is intended to augment radio-based communication by visual authentication of the sender, to prevent the injection of false messages by other units in specific critical situations.

For this reason (cf. [35], for details), vehicles can continue exchanging cooperative messages, such as maneuver planning data, by radio-based V2V. In addition to this, the negotiation result is used to generate a set of arbitrarily long, unique code sequences for each participating vehicle. All sequences are known among all participants of the negotiation; during execution of the maneuver, each vehicle transmits its own code sequence via VLC, and observes the sequences of all other partners. This process is exemplified in Figure 4.

Since all sequences are known in advance, the signal can be received and validated at bit-level (possibly even below bit-level, cf. Section 3); a flawless transmission of complete data packages is not necessary. Even temporary occlusion or low signal-to-noise ratios can be modeled this way. The process leads to an exponential decay of probability for an error in the received sequence over the time of visual contact (cf. Figure 5). At a maneuver-dependent time t_{decision} , at which the maneuver can last be safely aborted, the system allows to check whether a maneuver-dependent trust level p_{min} was reached; otherwise, the maneuver must be canceled. The computation of t_{decision} , p_{min} and a prediction of visual contact times can be efficiently included into cooperative planning. Thereby, the system enables an a priori risk estimation for safety-critical maneuvers along with a secure mode of maneuver execution. This allows to

already discard maneuvers during planning where p_{min} can unlikely be achieved before t_{decision} .

This renders attacks near-impossible that are based on the injection of false V2X messages for example via infected cellphones. Through the use of imaging VLC, attacks on cooperative safety-critical maneuvers require manipulating vehicle light controls; such attacks can therefore no longer be carried out purely remotely without access to the on-board vehicle systems. Additional details are given by Ziehn et al. [35].

3 Processing

The signal extraction from a greyscale image with linear intensities $I(x, y)$ (cf. Figure 6) provides an estimate of the sender light coordinates $[x^*, y^*]$, as well as real-valued signal intensities $N(y)$ and their significance ratios $R(y)$. A general implementation involves the following steps:

- **Estimate the columns x^*** with strong y derivatives. Due to the optical low-pass filter, these can only result from temporal, not from spatial contrasts.
- For each such column $I_x^*(y)$:
- **Compute the upper and lower envelopes $U(y)$, $L(y)$** by morphological *opening* and *closing*
- **Compute the light profile envelope** as the Gaussian-convolved function $E = \mathcal{N}(0, \sigma) * E'$ using $E'(y) = U(y) - L(y)$
- **Estimate the vertical line y^*** as the peak of $E(y)$
- **Estimate the normalized signal $N(y) = (I_x^*(y) - L(y))/E(y)$**
- **Estimate the significance ratio $R(y) = (U(y) - L(y))/S$** , where S is the image noise scale

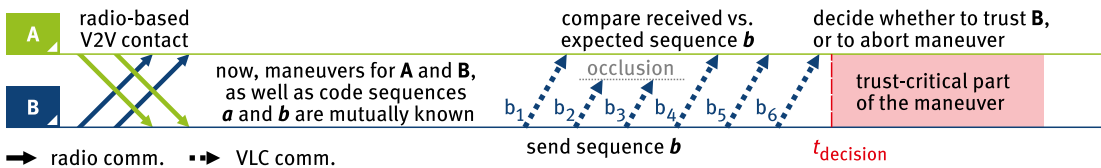


Figure 4: Simplified example, based on Ziehn et al. [35], of the proposed interplay of radio-based V2V communication (solid) and VLC-based communication (dashed) between two cars A and B (for simplicity presented only from the perspective of A checking whether to trust B – the process will usually be symmetric). Any communication of data, intentions and the negotiation of cooperative maneuver planning still relies on the broad radio-based V2V channel. In this process, if trust is critical for the maneuver, each participant (here A and B) is assigned an individual binary code sequence (here $a = [a_1, a_2, \dots]$ and $b = [b_1, b_2, \dots]$), which is mutually known among all participants. After this negotiation step, each car sends their respective code sequence via the narrow imaging VLC channel, and verifies the observed sequences and sender positions of all other partners. If, as in the example, some bits are not received (due to occlusion, range, interference, viewing angle, ...), trust is neither gained nor lost (see Figure 5). If sufficient trust is *not* established before reaching the trust-critical (or safety-critical) part of the maneuver by t_{decision} at the latest, the maneuver is aborted. Whether visual contact until t_{decision} will be sufficient can be predicted during initial planning, to exclude maneuvers in advance that will likely have to be aborted.

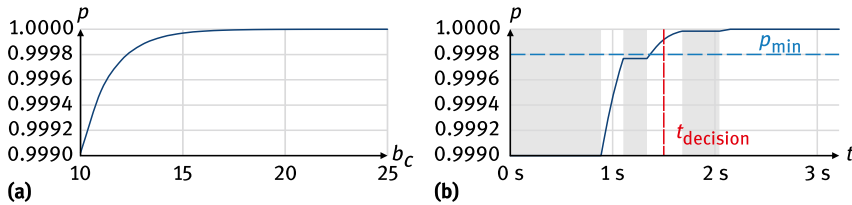


Figure 5: Already at very few bits received correctly b_c (and without any indications for false bits), an incorrect signal can be excluded with high probability (a). Since the entire sequence is known a priori, and is only verified by the imaging VLC, the protocol can incorporate temporary occlusions or measurement uncertainties. Without line of sight (shaded areas in (b)), the trust p is not increased. During line of sight, trust increases with the significance ratio of received bits. Safety-critical actions are executed or aborted depending on whether a maneuver-dependent trust level p_{\min} is reached before a maneuver-dependent critical time t_{decision} . Typically, as shown here, p_{\min} should be reached well before t_{decision} , such that a lossy visual connection between sender and receiver does not regularly lead to maneuvers being canceled unexpectedly.

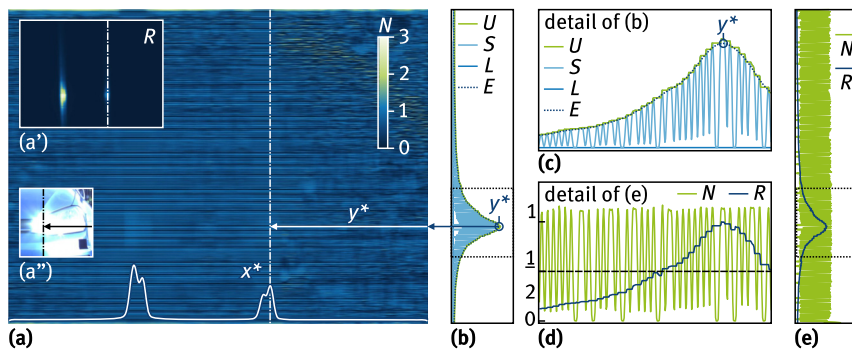


Figure 6: Processing example using actual data from Figure 2. Frequency peaks x^* are determined (a, lower image edge). Next, for each peak (as shown here on the example of the right light), first the upper and lower envelopes U , L of the signal S are computed, to obtain the light profile envelope E (b, c). From this, the normalized signal N can be computed (d, e, and in this example for the entire frame in a), as well as the significance ratio R (d, e, a'). From the frequency peaks x^* and the peaks y^* in E , the position is estimated. The result is shown in (a'') in the reference image. As can be seen in (a), the signal can be extracted from large portions of the entire frame, not only near the headlights.

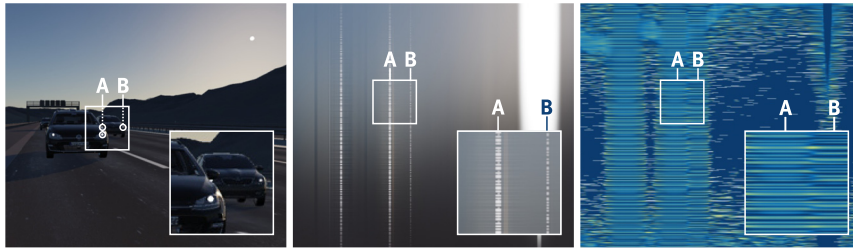
This processing implementation only employs simple signal processing operations with moderate computational effort and high potential for parallel execution. The estimated sender coordinates $[x^*, y^*]$ can subsequently be compared to data from regular vehicle sensors, to authenticate the sender. The signal data N and the significance ratios R can be compared to the expected signal, to determine the trust gain per line, or possible deviations.

4 Evaluation

The system was tested on non-public parts of the Test Area Autonomous Driving Baden-Wuerttemberg (see Fleck et al. [12]), as well as in the laboratory and in simulated traffic scenarios (Figure 7, simulated in OCTANE², to evaluate

challenges under operating conditions involving multiple senders as well as vehicles with regular lights). For the reception, an IDS UI-3590CP-C-HQ camera was used (1/2.08" sensor, 4912 × 3684 pxl frame, 8.5 mm focal length, 39.7 × 30.3 field of view) with adjustable shutter, as well as an IMX219PQ embedded sensor (1/4" sensor, 1920 × 1080 pxl frame, 3 mm focal length, 62.2 × 48.8 field of view). As a sender, headlights of a Golf VII test vehicle (see Filsinger and Roschani [11]) were modified by replacing the original light bulbs by LED replacement bulbs (not certified) to bypass the regular control unit, which were triggered directly by a microcontroller (ATmega328P). Both high beam and low beam lights were tested, the following evaluation results refer to the low beam application. The maximum tested switching frequency was 1000 Hz. To automatically evaluate the transmission (and in contrast to the proposed protocol), a transmission of 12-bit data packages was used. Only a complete transmission of an entire package was counted as a successful transmission.

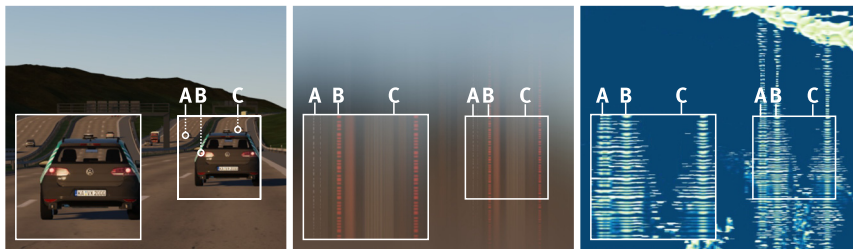
² www.octane.org.



(a) Sharp image. **A**: Overlapping headlights of fore and back car; **B**: Headlight of back car.

(b) Low-pass-filtered image.

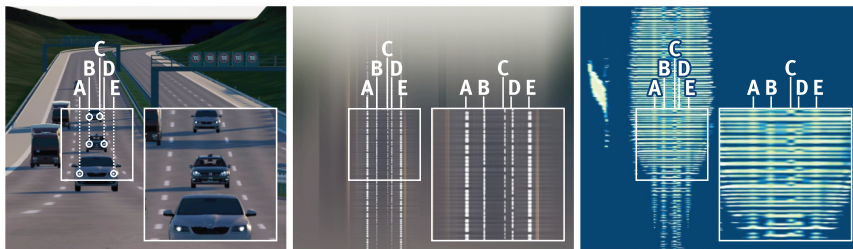
(c) Processing result. In the overlap column **A** the fore car's headlight dominates the result, the back car's headlight is extracted around column **B**.



(d) Sharp image. **A**: Headlight of an oncoming car. **B**: Taillight of car directly in front. **C**: Taillight of a distant car.

(e) Low-pass-filtered image.

(f) Processing result. The distant car's taillight **C** is so faint that the signal is only extractable in very few lines.



(g) Sharp image. **A**: Headlight of fore car. **B**: Overlapping headlights of center and back car. **C–E**: Non-overlapping headlights of back, center and fore car.

(h) Low-pass-filtered image.

(i) Processing result. In the overlap column **B** the signals of center and back car cannot be separated. However, if both expected signals are known, the overlap area can be used to validate whether both are as expected.

Figure 7: Shader-based photometric simulation of the challenges in the operational environment of three scenarios (each using $T_{\text{exp}} = 1/1000$ s and an aperture of $f/8$) with different signal sources **A–E**. Each scenario includes perfectly sharp images (a, d, g), low-pass-filtered images (b, e, h) and processing results as in Section 3/Figure 6 (c, f, i). Overlapping headlights and incident sunlight reduce the data reception; however, if the signal is verified at or below bit-level, even missing or overlapping information can be used for trust gain.

Tests were conducted under various lighting conditions, both in terms of varying environment light and by varying reception intensities by camera aperture. Even in direct sunlight, at a static distance of 200 m (the maximum available distance on the non-public test area), data rates of 100 Bit/s were robustly achieved using the IDS camera, including an $[x, y]$ localization of the sender at an accuracy of $[0.01, 0.19]$ (which corresponds to $[3 \text{ cm}, 66 \text{ cm}]$ at this range, and is expected to be sufficient to uniquely identify the sending vehicle). Direct sunlight above the light source leads to a loss of data rate due to insufficient signal-to-noise ratio; in contrast, precipitation (rain and snow) with

overcast sky will likely improve reception rates by reducing incident sun light.

5 Summary and outlook

We have presented a system for imaging visible light communication (VLC) in automotive applications, which can transmit 1000 Hz signals using available low-cost technology *and* localize the sender of the signal in the same measurement. Sending appropriate data via vehicle lights is already established in the state of the art. The extraction

of the sender angle along with the signal by use of the “rolling shutter effect” in combination with an optical low-pass filter allows for a cost-efficient implementation. The limited available test results indicate that under typical conditions, data rates of at least 100 Bit/s can be achieved. While this clearly does not permit substituting radio-based V2X messaging, it is sufficient for the intended use case: Authenticating senders using visual verification of their position, which was estimated to better than 1° in experiments.

Future work will focus on setting up a prototype that is certified for operation and testing on public roads using both head and taillights, including a closed-loop protocol implementation to validate V2V messages. This prototype will enable testing on the operational environment of public traffic, including realistic and dynamic scenarios, as well as conclusive analyses and comparison of optical components and parameters used in the transmission. The practical security gains will be tested and quantified in simulated scenarios of cooperative and connected driving.

Acknowledgment: This publication was written in the framework of the Profilregion Mobilitätssysteme Karlsruhe, which is funded by the Ministry of Science, Research and the Arts and the Ministry of Economic Affairs, Labour and Housing in Baden-Württemberg and as a national High Performance Center by the Fraunhofer-Gesellschaft.

Author contribution: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.

Research funding: This publication was written in the framework of the Profilregion Mobilitätssysteme Karlsruhe, which is funded by the Ministry of Science, Research and the Arts and the Ministry of Economic Affairs, Labour and Housing in Baden-Württemberg and as a national High Performance Center by the Fraunhofer-Gesellschaft.

Conflict of interest statement: The authors declare no conflicts of interest regarding this article.

References

- [1] S. Baker, E. Bennett, S. B. Kang, and R. Szeliski, “Removing rolling shutter wobble,” in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, IEEE, 2010, pp. 2392–2399.
- [2] T. Batz, K. Watson, and J. Beyerer, “Recognition of dangerous situations within a cooperative group of vehicles,” in *2009 IEEE Intelligent Vehicles Symposium*, 2009, pp. 907–912.
- [3] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. Stotz, and B. Lonc, “A generic public key infrastructure for securing Car-to-X communication,” in *World Congress on Intelligent Transport Systems (ITS)*, 2012, pp. 12–24.
- [4] A. Cailean, B. Cagneau, L. Chassagne, M. Dimian, and V. Popa, “Miller code usage in Visible Light Communications under the PHY I layer of the IEEE 802.15.7 standard,” in *2014 10th International Conference on Communications, COMM*, 2014, pp. 1–4, <https://doi.org/10.1109/ICComm.2014.6866699>.
- [5] C.-W. Chow, C.-Y. Chen, and S.-H. Chen, “Visible light communication using mobile-phone camera with data rate higher than frame rate,” *Optic Express*, vol. 23, no. 20, pp. 26080–26085, 2015.
- [6] C. Danakis, M. Afgani, G. Povey, I. Underwood, and H. Haas, “Using a cmos camera sensor for visible light communication,” in *2012 IEEE Globecom Workshops*, IEEE, 2012, pp. 1244–1248.
- [7] A. Davis, M. Rubinstein, N. Wadhwa, G. Mysore, F. Durand, and W. T. Freeman, “The visual microphone: passive recovery of sound from video,” *ACM Trans. Graph.*, vol. 33, no. 4, pp. 79:1–79:10, 2014.
- [8] T.-H. Do and M. Yoo, “Analysis on visible light communication using rolling shutter cmos sensor,” in *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, 2015, pp. 755–757.
- [9] J. Dürrwang, J. Braun, M. Rumez, and R. Kriesten, “Security evaluation of an airbag-ecu by reusing threat modeling artefacts,” in *International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, 2017, pp. 37–43.
- [10] J. Dürrwang, J. Braun, M. Rumez, R. Kriesten, and A. Pretschner, “Enhancement of automotive penetration testing with threat analyses results,” *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 1, pp. 91–112, 2018, (11-01-02-0005).
- [11] M. Filsinger and M. Roschani, “Strategisches Invest: versuchsfahrzeuge für Technologie-Experimente (VERTEX),” *visit Autonome Mobilität*, pp. 12–13, 2017 <https://www.iosb.fraunhofer.de/servlet/is/69530/>.
- [12] T. Fleck, K. Daaboul, M. Weber, et al. “Towards large scale urban traffic reference data: smart infrastructure in the test area autonomous driving baden-württemberg,” in *Intelligent Autonomous Systems*, 15, M. Strand, R. Dillmann, E. Menegatti, and S. Ghidoni, Eds., Cham, Springer International Publishing, 2019, pp. 964–982, ISBN 978-3-030-01370-7.
- [13] C. Frese and J. Beyerer, “Collision avoidance by cooperative driving maneuvers,” *ATZelextronik worldwide eMagazine*, vol. 6, no. 5, pp. 48–52, 2011, ISBN 2192-9092.
- [14] C. Frese, T. Batz, M. Wieser, and J. Beyerer, “Life cycle management for cooperative groups of cognitive automobiles in a distributed environment,” in *IEEE Intelligent Vehicles Symposium*, 2008, pp. 1125–1130, <https://doi.org/10.1109/IVS.2008.4621206>.
- [15] Y. Goto, I. Takai, T. Yamazato, H. Okada, T. Fujii, S. Kawahito, S. Arai, T. Yendo, and K. Kamakura, “A new automotive vlc system using optical communication image sensor,” *IEEE Photonics Journal*, vol. 8, no. 3, pp. 1–17, 2016.
- [16] J. Hedborg, P.-E. Forssén, M. Felsberg, and E. Ringaby, “Rolling shutter bundle adjustment,” in *2012 IEEE Conference on Computer Vision and Pattern Recognition*, IEEE, 2012, pp. 1434–1441.

- [17] IEEE, "IEEE recommended Practices for modulating current in high-brightness LEDs for mitigating health risks to viewers," *IEEE PAR*, p. 1789, 2015.
- [18] P. Ji, H.-M. Tsai, C. Wang, and F. Liu, "Vehicular visible light communications with led taillight and rolling shutter camera," *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, IEEE, 2014, pp. 1–6.
- [19] A. Jovicic, J. Li, and T. Richardson, "Visible light communication: opportunities, challenges and the path to market," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26–32, 2013.
- [20] L. U. Khan, "Visible light communication: applications, architecture, standardization and research challenges," *Digital Communications and Networks*, vol. 3, no. 2, pp. 78–88, 2017.
- [21] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, *Stuxnet under the Microscope*, ESET LLC, 2010, (September 2010).
- [22] S. McCloskey and S. Venkatesha, "Rolling shutter bar code imaging," US Patent 9,454,689, Sept, 2016.
- [23] M.-g. Moon, S.-i. Choi, J. Park, and J. Y. Kim, "Indoor positioning system using led lights and a dual image sensor," *J. Opt. Soc. Korea*, vol. 19, no. 6, pp. 586–591, 2015.
- [24] J. Petit and S. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transport. Syst.*, vol. 16, no. 2, pp. 546–556, 2015, ISSN 524-9050.
- [25] K. Schramm, K. Lemke, and C. Paar, "Embedded cryptography: side Channel attacks," in *Embedded Security in Cars*, K. Lemke, C. Paar, and M. Wolf, Eds., Springer, 2006, pp. 187–206.
- [26] I. Takai, S. Ito, K. Yasutomi, K. Kagawa, M. Andoh, and S. Kawahito, "Led and cmos image sensor based optical wireless communication system for automotive applications," *IEEE Photonics Journal*, vol. 5, no. 5, 2013, 6801418–6801418.
- [27] Ö. Tas, N. Salscheider, F. Poggenhans, S. Wirges, C. Bandera, M. Zofka, T. Strauss, J. Zöllner, and C. Stiller, *Making Bertha Cooperate – Team AnnieWAY's Entry to the 2016 Grand Cooperative Driving Challenge*, IEEE Transactions on Intelligent Transportation Systems, 2017.
- [28] United Nations Economic Commission for Europe (UNECE), *UNECE Regulation No. 123 – Uniform Provisions Concerning the Approval of Adaptive Front Lighting Systems (AFS) for Motor Vehicles*, 2010.
- [29] United Nations Economic Commission for Europe (UNECE), *UNECE Regulation No. 48 – Uniform Provisions Concerning the Approval of Vehicles with Regard to the Installation of Lighting and Light-Signalling Devices*, 2016.
- [30] A. Weimerskirch, "An overview of automotive cybersecurity: challenges and solution approaches," in *Proceedings of the 5th International Workshop on Trustworthy Embedded Devices, TrustedED '15*, ACM, New York, NY, USA, 2015. 53–53, <https://doi.org/10.1145/2808414.2808423>. ISBN 978-1-4503-3828-8.
- [31] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 1–8, <https://doi.org/10.1109/VNC.2013.6737583>.
- [32] T. Yamazato, "V2x communications with an image sensor," *Journal of Communications and Information Networks*, vol. 2, no. 4, pp. 65–74, 2017.
- [33] E. Yağdereli, C. Gemci, and A. Aktaş, "A study on cyber-security of autonomous and unmanned vehicles," *The Journal of Defense Modeling and Simulation*, vol. 12, no. 4, pp. 369–381, 2015.
- [34] M. Yoshino, S. Haruyama, and M. Nakagawa, "High-accuracy positioning system using visible led lights and image sensor," *2008 IEEE Radio and Wireless Symposium*, IEEE, 2008, pp. 439–442.
- [35] J. Ziehn, J. Beyerer, M. Filsinger, et al. "A non-invasive cyberrisk in cooperative driving," in *Lehrstuhl für Fahrzeugtechnik mit TÜV SÜD Akademie*, 8, Munich, Tagung Fahrerassistenz, 2017.