Secret Key Distribution Leveraging Color Shift Over Visible Light Channel

Hongbo Liu
Dept. of CIGT
IUPUI
Indianapolis, IN 46202
Email: hl45@iupui.edu

Bo Liu
Dept. of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
Email: bliu11@stevens.edu

Cong Shi
Dept. of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
Email: cshi5@stevens.edu

Yingying Chen
Dept. of ECE
Stevens Institute of Technology
Hoboken, NJ 07030
Email: yingying.chen@stevens.edu

***Abstract*—Given the widely adoption of screen and camera in many electronic devices, the visible light communication (VLC) over screen-to-camera channel emerges as a novel short range communication technique in recent years. Active research explores various ways to convey messages over screen-camera channel, such as barcode and unobtrusive optical pattern. However, with the prevalence of LED screens of wide viewing angles and mobile devices equipped with high standard cameras, the threat of information leakage over screen-to-camera channel becomes in-negligible. Few studies have discussed how to ensure the security of data transmission over screen-to-camera channel. In this paper, we propose a secret key distribution system leveraging the unique color shift property over visible light channel. To facilitate such design, we develop a practical secret key matching based method to map the secret key into gridded optical patterns on screen, which can only be correctly recognized by the legitimate user through an accessible region and allow regular data stream transmission through valid grids. The proposed system is prototyped with off-the-shelf devices and validated under various experimental scenarios. The results show that our system can achieve high bit-decoding accuracy for the legitimate users while maintaining comparable data throughput as regular unobtrusive VLC systems with very low recovery accuracy of the encrypted data for the attackers.**

I. Introduction

Due to the ever-growing crowded radio environments, visible light communication (VLC), especially over screen-camera channel [1]–[4], emerges as a promising way for short range communication in recent years. Active research explores various ways to convey messages over screen-camera channel. Particularly, it falls into two main categories, barcode (i.e., machine-readable optical labels visible to human eyes) and unobtrusive optical pattern (i.e., invisible optical patterns due to low luminance sensitivity or temporal flick-fusion property of human eyes). Unlike the broadcast nature of radio communication, the highly directional propagation property renders visible light communication with much less interference from multiple concurrent data transmissions. Compared with NFC and other RF-based short range communication technologies, which need additional hardware support to secure the short range communication, VLC can be deployed in more practical environments given the widely adoption of screen and camera in many electronic devices. We envision the emerging VLC over the screen-to-camera channel will become a more competitive form for short range communication, and benefit many security-sensitive mobile applications. For example, there is an increasing need on mobile private information sharing [5], [6], such as exchanging business cards and documents, in social places and business meetings. NFC and short range RF channel usually suffer from replay or man-in-the-middle attacks [7], whereas VLC-enabled mobile information sharing could fundamentally combat such threats due to line-of-sight propagation of visible light signal. Furthermore, mobile payment and ticketing systems [8] become more popular due to their ubiquitous payment possibilities and timely access to financial assets. The existing mobile payment methods based on NFC and RF techniques have the vulnerability under various attacks such as eavesdropping and DDoS [9]. Future mobile payment systems grounded on VLC would overcome these vulnerabilities by manipulating visible light signals on screen to conceal the information embedded in screen content [3], [10].

As the prevalence of LED screens of wide viewing angle and mobile devices equipped with high standard camera, the threat of information leakage over screen-to-camera channel however becomes in-negligible. Significant recent research efforts have been spent on improving the data transmission performance of visible light communication, but few works study securing data transmission over screen-to-camera channel. Traditional data encryption methods, such as AES or PKI [11], either require prior knowledge on secret keys or rely on central authority for secret key distribution. However, due to the lack of infrastructural management, such prerequisites may not be fulfilled in many short range device-to-device communication scenarios, especially for screen-to-camera channel. Further, the physical layer-based secret key extraction approaches over radio channel [12] are also not applicable to visible light channel due to the non-reciprocity of screen-to-camera channel. In this paper, we focus on securing key distribution over visible light channel using unobtrusive optical patterns under the presence of eavesdropping attackers. Because the secret key distribution serves as the first step to secure data transmission. Recent work of SBVLC [6] is a secure system on barcode-based visible light communication heavily relying on screen viewing angle changes induced by user motions. Kaleido [13] utilizes the disparities between the screen-to-eye channel and the screen-to-camera channel to prevent unauthorized users from videotaping leveraging random unobtrusive optical patterns, but such random optical patterns also prevent the regular data transmission over the screen-to-camera channel.

To ensure the regular data transmission over visible light channel while maintaining the data confidentiality, a new information security system is needed to cope with adversarial eavesdropping of the secret information over screen-to-camera channel. Kim et. al. [14] utilizes the color shift on a twisted nematic LCD screen to present two independent views concurrently when watching from two different viewing angles.

978-1-5386-0683-4/17/$31.00 ©2015 IEEE

This is the author's manuscript of the article published in final edited form as:

Liu, H., Liu, B., Shi, C., & Chen, Y. (2017). Secret key distribution leveraging color shift over visible light channel. In 2017 IEEE Conference on Communications and Network Security (CNS) (pp. 1–9). https://doi.org/10.1109/CNS.2017.8228626

Inspired by the above observation, we conduct close examination on the color shift property on screens. Our empirical studies reveal consistent color shift patterns on the captured screen contents when varying the viewing angles of camera. Specifically, the luminance and color intensity values of the captured screen contents appear differently when the camera is situated at different relative positions from the screen. Such findings motivate us to design customized optical patterns on screens that can only be correctly decoded by the users at certain viewing angles. The confidential data stream will be encoded with the secret key mapped from such optical patterns, and thereby securely transmitted over the visible light channel. Meanwhile, the optical pattern is hard to be inferred by the attackers from different viewing angles.

Based on the above useful findings, we design a secret key distribution system leveraging the unique color shift property over visible light channel. We target at delineating a *legitimate user access region* that ensures the secret key could be successfully decoded and received by the legitimate user. We refer the surround area where the user resides as the legitimate user access region. Whereas none or only partial secret information could be recovered by unauthorized users outside of this region. If an unauthorized user enters the legitimate user access region, he will have an increased chance to be exposed as an attacker to the legitimate user, hence defeating his advertorial intent. To facilitate such a design, we develop a practical secret key matching based algorithm to map the secret key into gridded optical patterns on the screen. The proposed method allows the secret key to be recognized correctly by the legitimate user and enables regular data stream transmission through valid grids. The throughput of our proposed system is comparable to the regular VLC systems, indicating low overhead is introduced by the security mechanisms. Specifically, we make the following major contributions in this project:

- Revealing the important fact that the changing viewing angles with respect to the screen would result in color shift on the captured screen contents. This useful phenomenon enables the design of the legitimate user access region.

- Proposing to secret key distribution over visible light channel leveraging the unique color shift property under the presence of eavesdropping attackers.

- Developing a practical secret key matching based algorithm to secure data transmission through encoding the color shift patterns on screen.

- Implementing the prototype of the proposed secret key distribution system and validating its performance with real experimental results, which confirms the effectiveness and efficiency of the proposed system.

II. Related Work

Visible light communication (VLC), as a subset of optical wireless communication, is an emerging short range data transmission technology that works on the visible light spectrum. The VLC technologies mainly fall into two categories, screen-to-camera-based [1]–[3] and fluorescent-based [15], [16] according to what type of transceiver is adopted. Specifically, screen-to-camera-based VLC transmits the data that is embedded as a special color pattern in the screen contents, while any camera that is able to capture the screen content extracts the embedded data; the fluorescent-based VLC uses ordinary fluorescent lamps or standard off-the-shelf visible light LED luminaries to transmit the data stream, which is modulated in the form of light pulses and correspondingly demodulated by the receiving photodiode.

Many studies have been proposed to prevent unauthorized users to access the fluorescent-based VLC [17], [18], but the security for short range screen-to-camera VLC has not been systematically studied. It is difficult to add security features to the screen-to-camera VLC channel due to its visual nature. Specifically, the screen contents are subject to all receivers including unauthorized users when they are displayed on the screen. Recently, Zhang et. al. [6] propose a secure system (SBVLC) for barcode-based VLC channel between smartphones. It provides a physical security enhancement mechanism leveraging screen viewing angle changes induced by user motions to ensure secure information exchange. However, this study only supports barcode as the information carrier over screen-to-camera channel and heavily relies on human involvement. To secure short-range communication, the near field communication (NFC) technique has enabled popular mobile applications [7], [19] over secure communication channel such as contact-less payments, mobile advertisements, and device pairing, etc. However, NFC requires additional hardware that is only available on a few smartphone platforms on the market, and is also vulnerable to eavesdropping and jamming attacks [8], [20].

Active studies have been driven by the color shift property [21], [22] to display different contents to the users at different viewing angles. Harrison et. al. [23] make the screen content invisible when viewed straight-on, but visible at oblique angles. Kim et. al. [14] propose a software solution which allows the screen to present two independent views concurrently on twisted nematic LCD screens. The above studies built upon the color shift property only serve for specific viewing pattern on screen, but they did not consider the confidential information transmission on the screen under the presence of adversaries. Kaleido [13] utilizes the disparities between the screen-to-eye channel and the screen–to-camera channel to prevent unauthorized users from videotaping a video played on a screen by re-encoding the original video frames. However, Kaleido prevents the data communication over screen-to-camera channel due to the randomly adopted optical patterns on screen. Unlike the existing studies, our proposed approach introduces a secret key distribution mechanism over the screen-to-camera VLC channel leveraging the color shift property on LCD screen. The proposed secure communication system is integrated with our previous visible light communication system, Uber-in-Light [4], for communication performance study.

III. System Overview

A. System Design

1) Background of Visible Light Communication: Visible light communication (VLC) over screen-to-camera channel has the data encoded as specific optical patterns displayed on screen, which can be captured by any camera-equipped devices thereafter for data decoding. The encoded information is usually represented as some specific optical patterns on screen [2], [3], [6]. In this paper, we focus on utilizing the luminance value L, an optical pattern contributed by three color channels (i.e., Red, Green, and Blue) as the secret key, to encode the data stream over the screen-to-camera channel. The data is encoded in such a way that the normal viewing experience of users such as displaying a picture or watching a video is not disturbed. Given the viewing angle in horizontal and vertical directions (Θ, Φ) and the distance (D) with respect to the screen, the expected luminance $\hat{L}^C$ (where C indicates

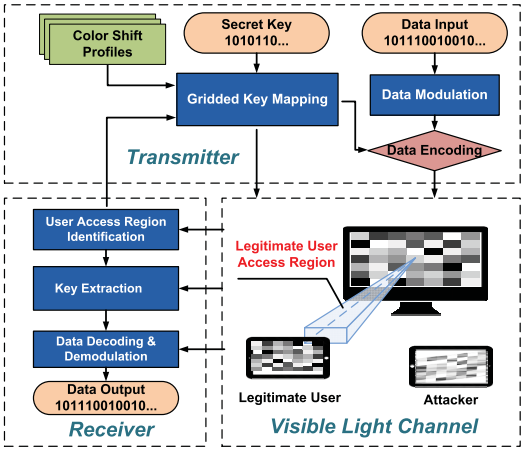


Fig. 1. Workflow of the proposed VLC security system.

a particular color $C \in \{R, G, B\}$) on camera is derived based on the visible light channel model:

$$\hat{L}^C(\Theta, \Phi, D) = H(\Theta, \Phi, D) * L^C + N \quad (1)$$

where L^C is the luminance value of the color C displayed on screen, $H(\Theta, \Phi, D)$ represents the channel response function on the screen-to-camera channel, and N represents external light interferences. Note that $*$ indicates the operator that applies the channel response to L^C, and $H(\Theta, \Phi, D)$ will be obtained through our empirical study (i.e., color shift curves).

2) Problem Formulation: Our objective is to secure the visible light communication over screen-to-camera channel under the presence of eavesdropping adversaries. Instead of relying on traditional data encryption methods, the color shift property of screen-to-camera channel is utilized to prevent the unauthorized users from decoding the transmitted data successfully. In particular, the expected luminance pattern should be only correctly decoded by the legitimate user from certain viewing angles. Whereas the unauthorized users situated outside of the region of the legitimate user's viewing angles cannot decode the pattern correctly. Assuming the luminance values observed by an attacker K and the legitimate user U are $\hat{L}^C_K(\Theta', \Phi', D')$ and $\hat{L}^C_U(\Theta, \Phi, D)$, respectively, the following condition should be satisfied to ensure the communication security as follows:

$$\begin{aligned} &|\hat{L}^C_K(\Theta', \Phi', D') - \hat{L}^C_U(\Theta, \Phi, D)| \geq \Delta L, \forall \Theta', \Phi', d' \\ &s.t., [\Theta, \Phi] [\Theta', \Phi']^T \geq \Delta, D' \geq \lambda, \\ &\Theta \in \left[\theta^b, \theta^u\right], \Phi \in \left[\phi^b, \phi^u\right], D \in \left[d^b, d^u\right]. \end{aligned} \quad (2)$$

where ΔL is the predefined luminance threshold, $[\Theta, \Phi] [\Theta', \Phi']^T$ (with T represents vector transpose) represents the inner product of the 2D viewing angle vector between the attacker and the legitimate user, Δ and λ are the thresholds indicating the restriction on viewing angle and distance of the attacker with respect to the screen, $\left[\theta^b, \theta^u\right]$, $\left[\phi^b, \phi^u\right]$ and $\left[d^b, d^u\right]$ together regulate the region where the legitimate user locates. In practice, if the screen is partitioned into multiple grids, the proposed system should ensure as many grids as possible to satisfy the above condition.

B. Design Challenges

To realize such a VLC security system based on the problem formulation, we need to address the following three main challenges:

- *Easy Deployment.* Due to the increasing popularity of the VLC system to support a broad range of applications, easy deployment is highly desirable. The designed system should target to use off-the-shelf devices.

- *Reliable Key Mapping.* We plan to design luminance patterns on the screen, which could only be correctly decoded by the legitimate user at a specific viewing angle/region. Thus, the proposed system should ensure the uniqueness of the secret key for the legitimate user, while the attacker will most likely derive the incorrect secret key from his viewing angle.

- *Efficient Key Extraction for Various Screen Contents.* Given a specific viewing angle, the camera-equipped user should be able to fast and accurately identify the encoded luminance pattern by eliminating both the geometric distortion due to the perspective effects and external luminance interference. - *Maintaining System Throughput.* The designed VLC secret key distribution system should maintain the throughput of visible light communication and does not disturb the normal viewing experience of the legitimate user.

C. System Workflow

The basic idea of the proposed system is to map the secret key to a unique optical pattern, which can only be correctly decoded by the legitimate user situated at an expected viewing angle. According to the color shift property, the change of the viewing angle towards the screen results in different captured optical patterns at the camera. The details of the color shift property are presented in Section IV. Such a unique optical pattern then acts as a gridded mask to encode the transmitting data stream embedded in the screen contents, and it also can be decoded at the receiver for data stream extraction. Since we focus on the secret key distribution over visible light channel, existing VLC modulation & demodulation approaches will be adopted here [4]. As depicted in Figure 1, the proposed system consists of five main components: *Gridded Key Mapping*, *Data Modulation & Encoding*, *User Access Region Identification*, *Key Extraction* and *Data Demodulation & Decoding*.

The proposed system divides the screen into smaller grids, and each grid acts an independent visible light channel for data transmission. The system utilizes the independent grid channel characteristics to encode the secret key. Different grids play different roles. For instance, some of the grids filled with the key information are referred as *invalid grids*, while other grids do not carry any key information but are used for data transmission referred as *valid grids*. The usage of the grids, including both the number and position of the invalid grids, to carry key information is flexible and could be adjusted by the system. The valid grids also change their luminance randomly during data transmission to confuse the attacker.

To start, our system can flexibly adjust the transmission optical pattern based on the position of the legitimate user, instead of restricting the user have to reside at a fixed position to obtain the secret key information. To achieve this, our strategies is to set a default luminance value at four corner grids on the transmitter screen. Then the legitimate user captures the screen content, and acknowledges the transmitter about the observed luminance values at the four corner grids through public wireless channels. Specifically, the legitimate user can encode the observed luminance values as flashlight signals that can be captured by the camera on the transmitter, or utilize WiFi and Bluetooth connections that are publicly accessible in many places nowadays to send the observed

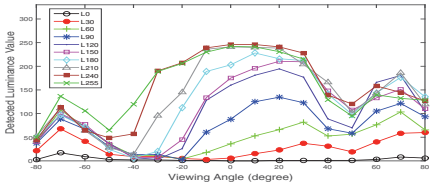


Fig. 2. Luminance curves of vertical angle range $\Phi \in (-80°, 80°)$ with horizontal angle fixed at $\Theta = 0°$.

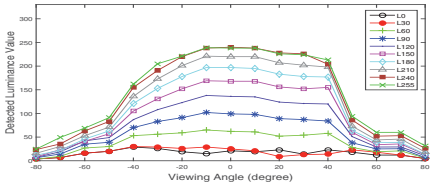


Fig. 3. Luminance curves of horizontal angle range $\Theta \in (-80°, 80°)$ with vertical angle fixed at $\Phi = 0°$.

luminance values. We do not require the security of out-of-band channels (e.g., WiFi and Bluetooth).. By matching these values to the color shift profiles, the legitimate user access region could be uniquely determined based on the relationship between the expected luminance pattern and viewing angles. The secret data will then be modulated to the corresponding optical patterns on screen with respect to the legitimate user access region.

The system has the secret key and data stream as two inputs for Gridded Key Mapping and Data Modulation & Video Fusion components, respectively. The secret key is first mapped to such an optical pattern that can only be correctly decoded by the legitimate user based on the pre-built color shift profile for each grid on screen. The color shift profile only needs to be built once, and solely maintained at the transmitter (i.e., screen). Then the optical pattern is mapped to the valid grids with different number and screen positions each time when there is a secret key to be distributed. Thus, it is difficult for an attacker to predict the expected optical pattern used for the secret key transmission. Specifically, we develop a secret key matching based algorithm, which utilizes each grid independently to encode the secret key. The expected optical pattern at receiver will be converted to a gridded mask. After the secret key is successfully received, the data stream, as the second input, is then modulated as unobtrusive luminance changes against arbitrary video contents. Before being sent to the screen-to-camera channel, the modulated data stream is encoded with the gridded mask. Correspondingly, the data demodulation & decoding will be performed based on the captured screen contents and recover the original data stream. The detailed description of each component is presented in later sections.

D. Attack Model

In this work, we utilize the terminologies of unauthorized user and attacker interchangeably. The attacker has the capability to access the screen (i.e., transmitter), but at a different angle and distance from the legitimate user. The attacker is equipped with the same kind of devices as the legitimate user's to capture the screen contents and eavesdrops the security information embedded in the detected luminance. The decoding algorithms for security information extraction are public for any receiving device. The attacker makes the efforts to avoid residing at the same viewing angle and distance as the legitimate user. The closer the attacker gets to the legitimate user, the higher the risk he/she will be exposed. Thus the attacker is detected in proximity, and the system will suspend the data transmission. Therefore the adversarial intent can not be achieved. Furthermore, the attacker does not access the legitimate users color shift profiles. In this work, we only consider an attacker with passive behaviors such as eavesdropping with the purpose of obtaining the secret key, while for those active attackers who would interfere with the environmental light conditions will end up not be able to crack a correct key.

IV. Feasibility Study

Color shift property over screen-to-camera channel would result in significant difference on the expected optical patterns from different vertical viewing angles. Therefore, it is critical to ensure the expected optical pattern can be correctly detected by the legitimate user. Specifically, two requirements should be satisfied: 1) the expected optical pattern captured by the legitimate user should be known by the transmitter; 2) the expected optical pattern captured by the legitimate user should be unique from all available vertical viewing angles.

A. Color Shift Study

An LCD comprises of a matrix of LC (liquid crystal) molecules between two polarizers and a uniform backlight beneath them. Varying the voltage applied to the LC molecules controls their direction and in turn the light intensity eventually emitted from the screen. When the viewer looks at the screen from different angles, the line of light transmission is also at different angles with regard to the direction of the LC molecules. This results in the light polarization directions being rotated differently by the LC molecules, leading to different light intensities emitted from the same pixel to different angles. To study the color shift property, we carry out a series of preliminary experiments in a typical home/office environment, where a number of default luminance values (e.g., 10) ranging from 0 to 255 applied to the same screen are detected from different viewing angles from (0°,−80°) to (0°,80°). Figure 2 and Figure 3 depict the luminance curves along the vertical and horizontal directions respectively. The important observations are that 1) given one default luminance on screen, the detected luminance values are different as the viewing angles changes, and 2) given one particular viewing angle, the detected luminance values show different variation trend as the default luminance value on the screen changes. The above observations indicate that it is difficult to predict the color shift pattern at different viewing angles, unless all the combination of default luminance values and viewing angles are visited. For different LCD screens, the color shift patterns are also exhibited differently, so there is no way to derive the color shift pattern of one particular LCD screen from other LCD screens. Further, the color shift pattern is asymmetric, so it is also impossible to infer the expected optical pattern at a particular viewing angle from its symmetrical viewing angle. This phenomenon is more obvious in the vertical direction than that in the horizontal direction.

Next, we need to locate the most appropriate range of viewing angles that ensures the legitimate user to obtain reliable expected optical pattern. Given the color shift pattern along vertical direction as in Figure 2, we partition the viewing angle Θ into two different regions as below: *1) Vertical angle* $\Phi \in (-80°, -50°) \bigcup (50°, 80°)$ *and horizontal angle* $\Theta = 0°$ *:* The detected luminance values are much lower than the default luminance values set on screen, so it is not reliable to retrieve the expected luminance values at the receiver side

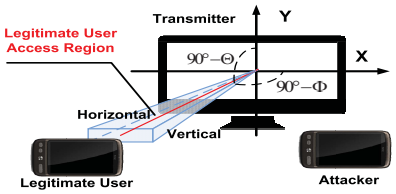


Fig. 4. Illustration of the legitimate user access region.

due to the limited luminance sensitivity on camera. We do not prefer to adopt this region for our proposed system; *2) Vertical angle* $\Phi \in (-50°, 50°)$ *and horizontal angle* $\Theta = 0°$*:* The detected luminance values do not have significant degradation in comparison with the default luminance values set on the screen, so it should satisfy the requirements for expected luminance value detection. More importantly, the detected luminance value does not keep constant in this viewing angle region, so it would result in different luminance values to be detected from any two different viewing angles. For the color shift pattern along horizontal direction as shown in Figure 3, *1) Horizontal angle* $\Theta \in (-80°, -50°) \bigcup (50°, 80°)$ *and vertical angle* $\Phi = 0°$: the detection luminance values also have sharp degradation as that in vertical direction; *2) Horizontal angle* $\Theta \in (-50°, 50°)$ *and vertical angle* $\Phi = 0°$*:* the detected luminance curves are so smooth that may result in similar detected luminance values at two far-away viewing angles, so it is not practical to rely the color shift properties solely along horizontal direction to secure the VLC channel.

In general, the color shift properties on screen-to-camera channel can be summarized as follows: 1) fixed RGB combination color follows stable detected luminance curve with viewing angle change; 2) the vertical angle impact on the detected luminance is larger than horizontal angle impact; and 3) each luminance curve is unpredictable and unique. It cannot be obtained with theoretical calculation.

B. Legitimate User Access Region

Before introducing the proposed system, we first need to define the legitimate user access region, which is critical to perform secret key distribution utilizing the color shift profiles. As introduced in Section IV-A, the luminance values on each individual color channel represent a unique pattern at a specific vertical viewing angle, correspondingly the overall luminance value contributed from three color channels also show distinct patterns from different vertical viewing angles. It enables the legitimate user to map the secret key to an expected luminance pattern dedicated to a small vertical viewing angle region, which is different from that of attacker's. In the meanwhile, since the detected luminance in horizontal direction changes much smoother than that in the vertical direction, the horizontal viewing angle has more flexibility on the region that allows legitimate user to access. Specifically, the *legitimate user access region* is defined as a pyramid region with the width in horizontal direction (i.e., X axis) larger than that in vertical direction (i.e., Y axis) as shown in Figure 4. Within this region, the legitimate user can receive the expected luminance pattern from the screen. Outside this region, the users obtain different luminance patterns, and thereby miss or only access partial secret key embedded in the expected luminance values. Considering the symmetric color shift property in the horizontal direction of LCD screen, the legitimate user access region should be as much as close to the horizontal angle $0°$.

V. Algorithm

The goal of the algorithm design is to map a secret key to a unique luminance pattern on screen, and such luminance pattern can only be correctly decoded within the legitimate user access region.

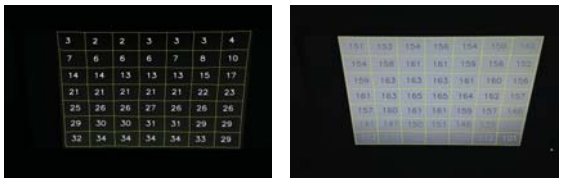
A. Color Shift Profiling

In order to perform practical secret key distribution, we first need to build the color shift profiles, which are the collections of the detected luminance values from different viewing angles. We have the screen divided into multiple grids to carry out concurrent data transmissions, where the secret key is transmitted in the manner of valid grids, and the data transmission is performed through invalid grids. According to color shift study, the camera will obtain different expected luminance patterns on each grid even if the whole screen has one single luminance value from different viewing angles. Therefore, the color shift profiles should include 1) (luminance setting, angle) on the screen, and 2) (expected luminance value, angle) can be captured by the camera.

In our empirical study, we choose 10 luminance values ranging from 0 to 255 with the interval 30 as the benchmark luminance, and each of these luminance values will be applied to $m \times n$ grids on the screen. For the convenience of processing, we utilize a chessboard-like pattern to represent the grids on screen. Next, the expected luminance values on these grids will be collected by the camera from 17 different viewing angles ranging from $-80°$ to $+80°$ in vertical direction. At each viewing angle, $m \times n$ expected luminance values are recorded. Figure 5 displays an example of color shift profiles from different viewing angles. It confirms that different grids have different expected luminance values with the same benchmark luminance. Considering all the benchmark luminance values and viewing angles, $17 \times 10 \times m \times n$ expected luminance values will be collected to build the color shift profiles in total. To facilitate practical system design, the transmitter (i.e., screen) only needs to build the color shift profile once, which is unknown to the users.

B. User Access Region Identification

Before the secret key transmission, in order to avoid the ambient light interference, the transmitting screen at first is set to pure black color before performing key extraction, so that the receiver could collect current ambient light signals N projected on the screen in Equation 2. Such interference will be deducted from the detected luminance values in the rest of the frames. Next, the transmitter needs to recognize the legitimate user access region, which is critical to establish the secure visible light channel between a pair of transceivers. Without loss of generality, the transmitter sends a default luminance value at four corner grids on screen, and the legitimate user acknowledges the corresponding observed luminance values through public wireless channels (i.e., encoded as flashlight signals to be captured by the camera on transmitter, or sent over existing WiFi or Bluetooth links). Next, the transmitter is able to identify the legitimate user access region based on the relationship between expected luminance pattern and viewing angles in color shift profiles. Therefore, the secure visible light channel is established with the common knowledge on the legitimate user access region between transmitter and receiver. Since the attackers have no idea about the color profiles that are stored on transmitter, they still can not determine the legitimate user access region even the acknowledged luminance values from receiver are intercepted.



(a) Default luminance 30 at the viewing angle $(\Theta, \Phi) = (0°, 10°)$.

(b) Default luminance 120 at the viewing angle $(\Theta, \Phi) = (0°, 20°)$.

Fig. 5. Illustration of color shift profiling for different viewing angles.

C. Key Matching based Method

Basic Idea. Key matching based method aims to encode the secret key to such a luminance pattern on screen that could only be successfully decoded by the receivers within the legitimate user access region. To achieve this, it is critical to select appropriate valid grids on the screen, and assign luminance values from the color shift profiles to these valid grids. Therefore, it could involve as many as possible valid grids rendering different expected luminance values between legitimate user and attacker in Equation 2.

Key Mapping. In this step, the transmitter maps out such a luminance pattern on screen that could result in the expected luminance value L^e on the valid grids for the legitimate user. We first choose a certain number of valid grids on the screen, and the number of valid grids is defined as the key length K. It is essential to have the valid grids widely distributed over the screen. According to the color shift study in Section IV, the expected luminance value is sensitive to the changes on the legitimate user access region, so the wide distribution of valid grids could minimize the opportunities of the attacker to obtain the correct expected luminance values. Specifically, we traverse the luminance profile of each grid on the chessboard, and seek for a subset of valid grids G_v that could produce the expected luminance value at the legitimate user access region. Next, K valid grids of G_v will be chosen and filled with appropriate luminance values $\hat{L}$ to ensure that the detected luminance values at the legitimate user access region match the expected luminance values L^e. Since each grid on the screen has an independent color shift profile, $\hat{L}$ will be obtained through exhaustive search in the color shift profiles for different valid grids.

By now we could retain the expected luminance value for the valid grids within the legitimate user access region. There may be multiple $\hat{L}$ values fulfilling the above requirement, but some $\hat{L}$ may make the attacker also obtain the expected luminance value for the valid grids outside the legitimate user access region. Improper $\hat{L}$ should be eliminated based on the required condition in Equation 2. Therefore, the valid grids assigned by the transmitter can only be correctly identified by legitimate user. Furthermore, since the expected luminance value is publicly available for any user, to further enhance the security and confuse the attacker, some of the remaining grids (i.e., invalid grids) will be filled in with the luminance values that would also match the expected luminance value outside of the legitimate user access region.

Key Extraction. Next, the legitimate user will identify the expected luminance pattern, and extract all the valid grids. We assume $\tilde{L}$ is the luminance value read out from the captured screen content for a specific valid grid $[m, n]$. According to the visible light channel model in Equation 1, $\tilde{L}$ may not exactly match the expected luminance value at the legitimate user access region due to the ambient light interference. The difference between $\tilde{L}$ and L^e is represented as $\delta = |L^e[m, n] - \tilde{L}[m, n]|$.

To tolerate the error introduced by the interference, we validate each grid through the following hypothesis test with a predefined threshold ΔL:

$$I = \begin{cases} 0 & \delta \leqslant \Delta L \\ 1 & \delta > \Delta L \end{cases} \tag{3}$$

where I indicates whether the grid matches the expected luminance value. If the difference between the detected luminance value and expected luminance value is less than ΔT, the grid will be marked as a valid grid; otherwise it will be marked as an invalid grid, which will participate in the data communication.

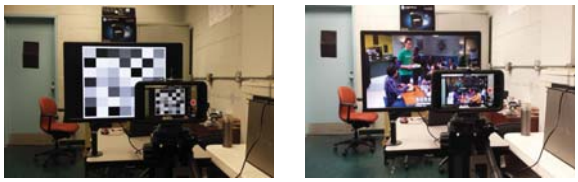
Security Analysis. The key matching based method results in a set of discrete valid grids on the screen, and the luminance value on each valid grid is chosen from the color shift profiles with respect to a particular legitimate user access region. Experimental results (in Section VII-C) show that it is highly impossible for the attacker to obtain all valid grids without entering the legitimate user access region. Furthermore, the invalid grids are also designed to produce the expected luminance value at some viewing angles outside of the legitimate user access region. If the attacker happens to reside at these viewing angles, some invalid grids will incorrectly be detected as valid grids. Since the number of valid grids, which represents the key length, is randomly chosen at the transmitter, the attacker may obtain different numbers of valid grids outside the legitimate user access region.

D. Data Transmission

After the secret key is successfully distributed to the legitimate user, we adopt the existing work [4] to perform the data transmission. The data stream embedded in the video frames is transmitted in an unobtrusive luminance manner, which will not disturb the user's viewing experience on watching a video. Specifically, the data stream is multiplexed as complementary color intensity changes over Red, Green, and Blue (RGB) channels onto the video frames. As shown in the system workflow in Figure 1, we next need to perform the data encoding via the secret key in the key matching algorithm after the data modulation. The real data stream embedded in the video frames are only appeared on invalid grids for transmission, while the valid grids only create random data streams to confuse the attackers. So the data throughput is proportional to the number of invalid grids.

VI. Prototype Implementation

We implement the proposed secret key distribution system over visible light channel with C++ and OpenCV libraries. OpenCV libraries provide well-developed image processing and feature detection functions. The transmitter and receiver are deployed on an LCD monitor and smartphone respectively. In particular, we choose Dell 24// LCD monitor with the refresh rate of $60fps$ as the transmitter because for the transmitter to encode data, its screen needs to be able to display at least 60 frames per second and exhibits color shift at various viewing angles. There are two inputs, the data stream and a binary secret key, for the transmitter to processing. The transmitter maps the secret key to a gridded optical pattern, modulates the data stream onto the video frames, and displays the multiplexed video stream on screen. We utilize the built-in



(a) Chessboard Display. (b) Video Display.

Fig. 6. Experimental setup.

function *cvRectangle* in OpenCV to create a communication layer, which is used to generate chessboard grids and assign different luminance values on the grids based on the secret key to be distributed.

For the receiver, we choose iPhone 6, which has the built-in camera with the refresh rate of $240fps$, so that it can be able to capture the data stream embedded in the video stream at $60fps$, To implement the receiver, we use the module *AVCapture* in the iOS AVFoundation framework to record videos, and then decode the secret key from the recorded video with the build-in OpenCV functions. The receiver captures the screen contents on screen, detects the gridded optical pattern and calculate average luminance on each grid. Specifically, we utilize *cvFindChessboardCorners* function to identify the chessboard from the captured screen content, and extract the luminance value of each grid. To provide reliable detection results, we enable the built-in light sensor in smartphone to adjust the ISO value in camera, so that it could adapt to the darkness of external environment.

VII. Performance Evaluation

In this section, we evaluate the performance of the proposed secret key distribution system. We examine the detected luminance of the grids on the screen from different viewing angels, and evaluate the grid identification accuracy and bits decoding accuracy over the screen-to-camera VLC channel. We first introduce our experimental methodology and metrics, and then discuss the evaluation results.

A. Methodology

The proposed secret key distribution system is evaluated with a TN LCD screen (i.e, 24// Dell monitor with 1600×900 resolution and $60Hz$ refresh rate as the transmitter) and two smartphones (i.e., we use iPhone 6 to act as both legitimate users and attacker) in typical home/office environments, where the external light interferences keep constant. Note that the proposed system is suitable for generic monitors and off-the-shelf mobile devices without specialized hardware requirements. The screen is held by a monitor arm that can adjust the orientation of the screen as shown in Figure 6 (a). The exposure time and ISO of camera are fixed at $1/90sec$ and 100, respectively, and the white balance on the camera is locked.

To evaluate the key distribution effectiveness and security of the proposed system, we place one iPhone 6 within the legitimate user access region that could be $65cm$, $80cm$ and $100cm$ from the screen as shown in Figure 6 (a), and we also have another iPhone 6 reside outside the legitimate user access region with the same distance. The reason why we use the same type of devices acting as both the legitimate user and attacker is to ensure equivalent capabilities when extracting the secret key from the transmitter. if other types of devices are employed, the attacker will experience low possibility to successfully to obtain the correct secret key. The color shift profiling process has the screen automatically display the default luminance values, while the camera captures the color shift profiles when the viewing angle is manually adjusted to cover all the viewing angles. The whole process usually lasts for less than 1 hour. The expected luminance patterns, which involve 10 different luminance values ranging from 0 to 255, with respect to different legitimate user access regions are designed according to the rules defined in the proposed key matching algorithm. We vary the viewing angles of the camera by changing the orientation of the screen to capture the luminance pattern on the screen, and both legitimate user and attacker will perform key extraction individually. In this experiment, the viewing angle varies from -80° to 80° both vertically and horizontally, which is controlled by a digital protractor, and we examine security performance from different viewing angles. In particular, we generate 5 different chessboards of the size 5×5, 6×6, 7×7, 8×8 and 9×9 for performance evaluation. Only the results for the size 5×5 and 9×9 are given in this paper, since the performance of other sizes falls between that of 5×5 and 9×9. Based on our empirical study, in general the expected luminance detection threshold is fixed at ± 5 unless explicitly mentioned.

To evaluate the encrypted data transmission accuracy and throughput, we develop the proposed secure communication system based on our visible light channel communication system, Uber-in-Light [4], which has achieved comparable data rate with other existing VLC communication systems (Highlight [3] and Inframe [2]). We evaluate the communication performance of the proposed secure communication system based on Uber-in-light [4]. The data streams are embedded into a drama video with $30fps$ lasting for $1min$ as shown in Figure 6 (b), and only the invalid grids allow real data transmission. Both legitimate user and attacker are equipped with the cameras to capture the video frames for data decoding. The data transmission accuracy is evaluated with respect to specific legitimate user access regions, and the throughput is inspected under the impact of chessboard size.

B. Metrics

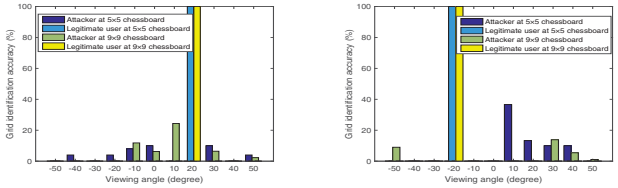
To evaluate the system performance comprehensively, we define the following two metrics, Grid Identification Accuracy and Bit Decoding Accuracy, as follows:

1) Grid Identification Accuracy: The system independently detects the luminance value on each grid when distributing the secret key, and identify the grids who render the expected luminance values. The grid identification accuracy P_{grid} is defined as the percentage of correctly identified grids G_r over the grids that are supposed to produce expected luminance value in legitimate user access region G_s, i.e., $P_{grid} = (G_r \bigcap G_s)/G_s$.

2) Bit Decoding Accuracy.: The bit decoding accuracy is defined as the percentage of correctly received bits over all data bits transmitted over the screen-to-camera channel as, $P_{bits} = (b_r \bigcap b_s)/b_s$, where b_r is the bits correctly decoded at the receiver, and b_s is all the transmitted bits.

C. Evaluation Results

1) Grid Identification Accuracy: **Impact of Viewing Angles.** We first study the grid identification accuracy when varying the viewing angles in vertical direction Φ but fixed at $\Theta = 0^\circ$ in horizontal direction. Both the 5×5 and 9×9 chessboard are deployed in the experiments. Figure 7 depicts the average grid identification accuracy for both the legitimate user and attacker given 4 different legitimate user access regions (i.e., $(\Theta, \Phi) = (0^\circ, \pm 20^\circ)$ and $(0^\circ, \pm 40^\circ)$). For both chessboard



(a) $(\Theta, \Phi) = (0^\circ, 20^\circ)$. (b) $(\Theta, \Phi) = (0^\circ, -20^\circ)$.

(c) $(\Theta, \Phi) = (0^\circ, 40^\circ)$. (d) $(\Theta, \Phi) = (0^\circ, -40^\circ)$.

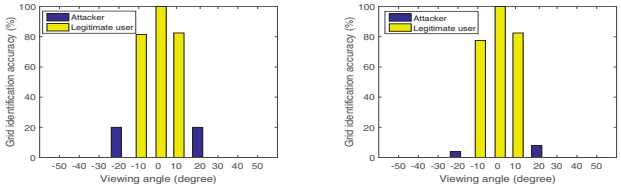
Fig. 7. Grid Identification Accuracy in the vertical direction when the legitimate user is positioned at four different vertical angles, $(0^\circ, 20^\circ), (0^\circ, -20^\circ), (0^\circ, 40^\circ)$, and $(0^\circ, -40^\circ)$ on the 5×5 and 9×9 chessboards; and the attacker accesses the screen from outside the legitimate user access region.

sizes, the legitimate user always has 100% grid identification accuracy while the attacker outside legitimate user access region maintains consistent low accuracy. It implies that the attacker can barely recover most of the valid grids without entering the legitimate user access region. This is because the expected luminance values vary so sharply as shown in Figure 2 that even small changes on the viewing angle would induce significant changes on the expected luminance outside legitimate user access region. Given that the valid grids are scatteredly distributed, it is easy to infer that the key matching based method is not sensitive to the chessboard size, which is confirmed by the results shown in Figure 7. We focus on 5×5 chessboard in the rest of the performance evaluation due to the less impact on chessboard size.

Next we discuss the grid identification accuracy when the viewing angle varies in the horizontal direction but fixed in vertical direction. As shown in Figure 8 (a)-(c), given any specific angle in vertical direction (i.e., $\Phi = \pm 20^\circ$ or 40°), it always retains the grid identification accuracy for legitimate user as high as over 80% when the legitimate user access region is restricted within $\Theta = [-10^\circ, 10^\circ]$ in horizontal direction, while the attacker has low accuracy (i.e., less than 20%) outside of this region. Figure 8 (d) has relatively higher grid identification accuracy for the attacker (i.e., 60%), since the expected luminance at $\Phi = -40^\circ$ does not change as sharp as those at other vertical angles along the horizontal direction.

Grid Identification Accuracy Study of different key lengths. We study the impact of key length to our key matching based approach. Specifically, the grid identification accuracy is examined as the difference of viewing angles between legitimate user and attacker changes. Figure 9 shows that the grid identification accuracy for the attacker always maintains as low as 20% for both short and long key lengths (i.e., ≤ 4 and ≥ 5). It indicates that our key matching method is robust to defend against the attacks with different key lengths.

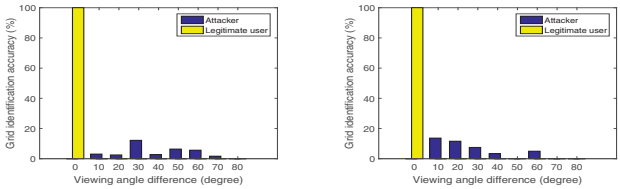
Impact of Distance, Threshold and Wide-Range User Access Region. In Figure 10 (a), we study the impact of geometric distance between transmitter and receiver to the grid identification accuracy. As the distance increases, the mutual interference on the adjacent grids become innegligible for key matching based method. It may result in similar expected



(a) $(\Theta, \Phi) = (-10^\circ, 20^\circ)$ to $(10^\circ, 20^\circ)$. (b) $(\Theta, \Phi) = (-10^\circ, -20^\circ)$ to $(10^\circ, -20^\circ)$.

(c) $(\Theta, \Phi) = (-10^\circ, 40^\circ)$ to $(10^\circ, 40^\circ)$. (d) $(\Theta, \Phi) = (-10^\circ, -40^\circ)$ to $(10^\circ, -40^\circ)$.

Fig. 8. Grid Identification Accuracy of different legitimate user access region in the horizontal direction.



(a) short key length: ≤ 4. (b) long key length: ≥ 5.

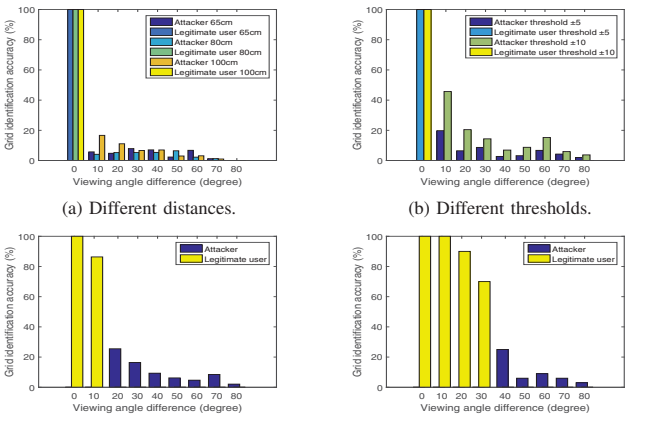
Fig. 9. Grid Identification Accuracy of the attacker across multiple chessboards under different key lengths.

luminance for the same valid grid at different viewing angles. So the overall performance with short distance is slightly better than that with long distance.

Figure 10 (b) presents the impact of different thresholds (i.e., ± 5 and ± 10) for the expected luminance detection. As the threshold increases, the grid identification accuracy for the attacker increases accordingly. The expected luminance values of some grids may not have much difference between the legitimate user and attacker. If these grids happen to be valid grids, it is also possible to correctly determine them as valid grids with a larger threshold by the attacker. Further, the threshold should not be too small in avoid of the impact of ambient light interference.

Previous results study the security performance for narrow-range legitimate user access region, which corresponds to one specific viewing angle. However, with careful design on the expected luminance pattern, the proposed system could also serve for wide-range legitimate user access region. As shown in Figure 10 (c) and (d), we find that the grid identification accuracy still maintains over 90% when the viewing angle differences increases to 10° and 20° in the vertical and horizontal directions, respectively. The above results indicate the possibility of introducing wide-range legitimate user access region to our proposed system for secret key distribution. Such wide-range legitimate user access region provides the flexibility for mobile users, but it also increases the risk that the attacker may enter the legitimate user access region.

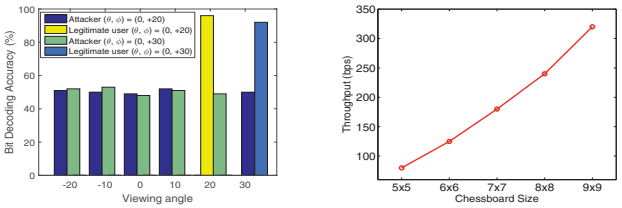
2) System Bit Decoding Accuracy: We discuss the bit decoding accuracy for the data stream encrypted with secret key generated by the key matching based method. As shown in the Figure 11 (a), we observe that the bit decoding accuracy



(a) Different distances. (b) Different thresholds.

(c) Wide-range in the vertical direction. (d) Wide-range in the horizontal direction.

Fig. 10. Grid Identification Accuracy with different transmission distances, thresholds and wide-range legitimate user access region.



(a) Bit decoding accuracy (b) Throughput

Fig. 11. Performance of Data Transmission.

of legitimate user keeps as high as over 95% at the viewing angle 20° and 30°, while the attacker can only achieve around 50% accuracy outside legitimate user access region, which is equivalent to random guess.

3) System Throughput: Finally, the throughput performance of the proposed VLC security system is studied. Figure 11 (b) presents the throughput for key matching based method under different number of grids on chessboard. We find that the throughput keep increasing while the number of grid on the chessboard goes larger. Particularly, it achieves over $300bps$ when deploying 9×9 chessboard. The results also confirms that the proposed security mechanisms introduces little throughput overhead comparing with Uber-in-Light [4].

VIII. Conclusions

In this paper, we propose a secret key distribution system leveraging the color shift property over screen-to-camera channel. Inspired by such observation that the visible information displayed on screen would result in different optical patterns from different viewing angles, we develop the secret key matching based algorithm to map the secret key into a unique gridded optical pattern that is only accessible from a specific region. In particular, the proposed method encodes the secret key to an expected luminance pattern on each grid independently, so it provides high flexibility of the legitimate user access region with different key lengths, and controls the system throughput easily. We prototype the proposed system with off-the-shelf devices and evaluate it under various experimental scenarios. The experimental results confirm the effectiveness of our system in terms of high bit-decoding accuracy for the legitimate users and very low key recovery accuracy for the attackers.

IX. Acknowledgment

This work was supported in part by the US National Science Foundation under grant numbers CNS-1409767, CNS-1514436, and the Army Research Office under grant number W911NF-13-1-0288.

References

[1] W. Hu, H. Gu, and Q. Pu, "Lightsync: Unsynchronized visual communication over screen-camera links," in *ACM MobiCom*, 2013, pp. 15–26.

[2] A. Wang and et al., "Inframe++: Achieve simultaneous screen-human viewing and hidden screen-camera communication," in *ACM MobiSys*, 2015, pp. 181–195.

[3] T. Li and et al., "Hilight: Hiding bits in pixel translucency changes," in *VLCS*, 2014, pp. 45–50.

[4] I. Mostafa and et al., "Uber-in-light: Unobtrusive visible light communication leveraging complementary color channel," in *IEEE INFOCOM*, 2016.

[5] R. Nandakumar, K. K. Chintalapudi, V. Padmanabhan, and R. Venkatesan, "Dhwani: Secure peer-to-peer acoustic nfc," in *SIGCOMM*. New York, NY, USA: ACM, 2013, pp. 63–74.

[6] B. Zhang and et al., "Sbvlc: Secure barcode-based visible light communication for smartphones," in *IEEE INFOCOM*, 2014, pp. 2661–2669.

[7] C. Mulliner, "Vulnerability analysis and attacks on nfc-enabled mobile phones," in *Availability, Reliability and Security*, 2009, pp. 695–700.

[8] M. M. A. Allah, "Strengths and weaknesses of near field communication (nfc) technology," *Global Journal of Computer Science and Technology*, vol. 11, no. 3, 2011.

[9] K. Laeeq and J. A. Shamsi, "A study of security issues, vulnerabilities and challenges in internet of things," *Securing Cyber-Physical Systems*, p. 221, 2015.

[10] G. Woo, A. Lippman, and R. Raskar, "Vrcodes: Unobtrusive and active visual codes for interaction by exploiting rolling shutter," in *ISMAR*, Nov 2012, pp. 59–64.

[11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc., 1995.

[12] B. Prashanth and Y. Pandurangaiah, "Generation of secret key for physical layer to evaluate channel characteristics in wireless communications," *Conference on Emerging Research in Computing, Information, Communication and Applications*, 2013.

[13] L. Zhang and et al., "Kaleido: You can watch it but cannot record it," in *ACM MobiCom*, 2015, pp. 372–385.

[14] S. Kim and et al., "Enabling concurrent dual views on common lcd screens," in *ACM SIGCHI Conference on Human Factors in Computing Systems*, 2012, pp. 2175–2184.

[15] A. Burton and et al., "Performance analysis for 180 receiver in visible light communications," in *IEEE ICCE*, 2012, pp. 48–53.

[16] S. Schmid and et al., "Led-to-led visible light communication networks," in *ACM MobiHoc*, 2013, pp. 1–10.

[17] C.-W. Chow and et al., "Secure communication zone for white-light led visible light communication," *Optics Communications*, vol. 344, pp. 81–85, 2015.

[18] C. Rohner and et al., "Security in visible light communication: Novel challenges and opportunities," *Sensors & Transducers Journal*, vol. 192, no. 9, pp. 9–15, 2015.

[19] G. Van Damme, K. Wouters, and B. Preneel, "Practical experiences with nfc security on mobile phones," *Proceedings of the RFIDSec*, vol. 9, p. 27, 2009.

[20] K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," *RFIDsec*, vol. 12, p. 21, 2012.

[21] M. C. Stone, "Color and brightness appearance issues in tiled displays," *IEEE Computer Graphics and Applications*, vol. 21, no. 5, pp. 58–66, 2001.

[22] T. Toyooka and et al., "Viewing angle performance of tn-lcd with hybrid aligned nematic film," *Displays*, vol. 20, pp. 221–229, 1999.

[23] C. Harrison and S. E. Hudson, "A new angle on cheap lcds: making positive use of optical distortion," in *ACM symposium on User interface software and technology*, 2011, pp. 537–540.