Poster: Secure Visible Light Communication via Two-Dimensional Spatially Aliased Patterns

Hao Pan*
Shanghai Jiao Tong University
panh09@sjtu.edu.cn

Yi-Chao Chen*
Shanghai Jiao Tong University
yichao@sjtu.edu.cn

Guangtao Xue
Shanghai Jiao Tong University
gt_xue@sjtu.edu.cn

ABSTRACT

Screen-camera communication has attracted considerable attention as a form of visible light communication (VLC) using commercial-off-the-shelf devices. Nonetheless, the security of screen-camera communications in mobile applications has largely been disregarded, despite the fact that information displayed on an open screen is easily intercepted. One-way communication systems also make it difficult to add security features. In this paper, we propose a secure screen-camera communication system in which a visual encryption algorithm is designed to camouflage transmitted images between the screen and camera. When the targeted receiver holds a camera in a designated viewing position (i.e., directly in front of the screen at a distance of $50cm$), the camouflaged image is revealed due to aliasing effect. From any other position, only the camouflaged image can be seen.

ACM Reference Format:
Hao Pan, Yi-Chao Chen, and Guangtao Xue. 2019. Poster: Secure Visible Light Communication via Two-Dimensional Spatially Aliased Patterns. In *13th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH'19), October 25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3349623.3355724

1 INTRODUCTION

Communication between screens and cameras involves the encoding of information with visual frames presented on a screen, and the retrieval of that information by a device equipped with a camera. Screen-camera links operating within the visible light spectrum provide interference-free out-of-band communication. Screen-camera communication is widely used in mobile applications due to the extremely low barrier to adoption. Unfortunately, the security of the mobile communication has largely been overlooked. The fact that visual barcodes are displayed on a screen means that they are open to eavesdropping. The ubiquity of smart devices and widespread use of surveillance cameras in public areas has only added to the danger. The fundamental principle on which barcode-based communication was designed makes it difficult to add security features. Furthermore, most existing barcode applications are designed for one-way communication, which is insufficient for the establishment of a secure communication channel. Recently, several systems are designed to stream a series of unobtrusive barcodes [2, 3], or integrating images/watermark into barcodes [1]. However, these designs can only ensure the invisibility of the *screen-to-eye* link, rather than preventing the eavesdropping attacks from illegal cameras.

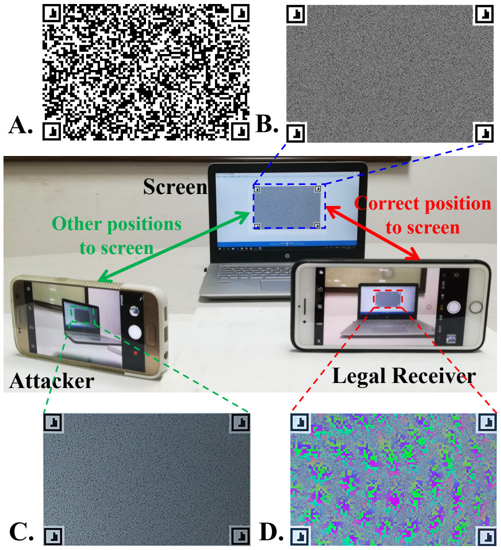
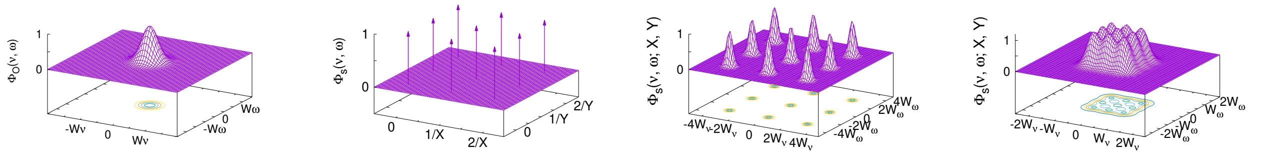


Figure 1: Camouflaged Data frames are revealed when the camera is placed in the designated viewing position: (A) original data frame, (B) being camouflaged through special spatial frequency, (C) obtained from outside the designated position, and (D) obtained from the designated viewing position.

[*] Both authors contributed equally to the paper

WiNTECH'19, October 25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6931-2/19/10…$15.00
https://doi.org/10.1145/3349623.3355724



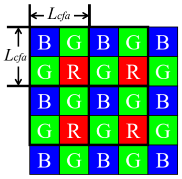
(a) Power density spectrum of a object image after sensor responese.

(b) PSD of the camera's sampling function.

(c) PSD of discrete signal $s(\nu, \omega; X, Y)$ which will occur blurring after reconstrcution.

(d) PSD of discrete signal $s(\nu, \omega; X, Y)$ which will occur aliasing after reconstrcution.

Figure 2: Examples of blurring and aliasing in the process of image acquisition and reconstruction (only neighboring sampling sidebands are shown).



B	G	B	G	B
G	R	G	R	G
B	G	B	G	B
G	R	G	R	G
B	G	B	G	B

Figure 3: Bayer CFA profile.

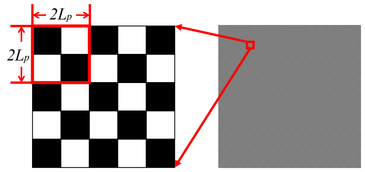


Figure 4: Pixel design for the black blocks on the original data frame.

We proposed a novel screen-camera communication system to enhance the security of communication via screen-camera links. The proposed scheme exploits the basic mechanism underlying the generation of two-dimensional aliased patterns in line-scan data acquisition systems to camouflage visually encoded frames from the communication channel. Decryption relies on the position of the camera relative to that of the image displayed on the screen. This physical limitation provides an obvious obstacle to attackers seeking to eavesdrop on the transmission of data.

2 CAMOUFLAGING IMAGES

In this section, we discuss the method used to camouflage the data frames for embedding in the form of image code (Fig. 1(A)) within a secure image (Fig. 1(B)). Assume that we already have the data frames comprising 0 data bits (white blocks) and 1 data bits (black blocks) for use in camouflaging.

We camouflage image code to enable extraction from only a designated viewing position. To achieve that, we apply *aliasing* for legal users, and *blurring* for would-be attackers.

When sampling a high frequency signal at a sub-Nyquist frequency, the frequency component is aliased or folded back. In Fig. 2(d) we present an example of aliasing in 2D. The rule of aliasing can be simplified as follows [4]:

$$f \in \{f_g | f_g = Nf_s \pm f_a, N = 0, 1, 2, \cdots, f_g \geq 0\}. \qquad (1)$$

where f_g is a candidate estimation of f, f_a is the aliasing frequency, f_o is the frequency of original signal, f_s is the sampling frequency, and $N \in \{0, 1, 2, \cdots\}$. Therefore, given f_s, we can derive candidates of f from the measured f_a.

Based on the image acquisition and reconstruction model, f_s corresponds to the sampling frequency of a camera: $(\frac{1}{X}, \frac{1}{Y})$, f_o corresponds the spatial frequency of $s(x, y)$, and the aliasing frequency of f_a is the spatial frequency of $s(x, y; X, Y)$. In this work, $O(x, y)$ comprises black and white blocks. Take one black block as an example - the spatial frequency of the black block is $(0, 0)$. If its aliasing image were revealed using a camera, then $s(x, y; X, Y)$ should equal $(0, 0)$. According to Eq. 1, the spatial frequency of $s(x, y)$ is the integral multiple of the spatial sampling frequency:

$$\{f'_g | f'_g = (\frac{N}{X}, \frac{N}{Y}), N = 1, 2, \cdots\},$$

where f'_g is a candidate estimation of the spatial frequency of $s(x, y)$, X and Y are the sampling interval in the x and y directions. As shown in Fig. 3, X and Y are equal to L_{cfa}.

Hardware pixels are physical elements of a screen, which cannot be stretched, skewed, or subdivided, and therefore set the maximum spatial frequency of the screen $(\frac{1}{2L_p}, \frac{1}{2L_p})$, where L_p indicates the length of one pixel. Fig. 4 presents this spatial frequency, in which each cell represents a pixel. When the spatial frequency of the object projected onto the camera equals the spatial frequency of the sampling frequency, $(\frac{1}{L_{cfa}}, \frac{1}{L_{cfa}})$, the emerging pattern corresponds to the original black block. Based on the camera pinhole theory and the physical parameters of the camera and screen, it is possible to calculate the distance between the receiver and sender as follows: $Distance = \frac{2L_p \times L_{focal}}{L_{cfa}}$. When the camera is placed at multiples of *Distance*, the spatial frequency of the object projected onto the camera equals $(\frac{N}{L_{cfa}}, \frac{N}{L_{cfa}})$, where $N \geq 2$. In this situation, the camera can capture only a blurred pattern, rather than the desired pattern.

REFERENCES

[1] W. Huang and W. H. Mow. Picode: 2d barcode with embedded picture and vicode: 3d barcode with embedded video. In *MobiCom*, pages 139–142, 2013.

[2] V. Nguyen, Y. Tang, A. Ashok, M. Gruteser, K. Dana, W. Hu, E. Wengrowski, and N. Mandayam. High-rate flicker-free screen-camera communication with spatially adaptive embedding. In *IEEE INFOCOM*, pages 1–9, 2016.

[3] A. Wang, Z. Li, C. Peng, G. Shen, G. Fang, and B. Zeng. Inframe++: Achieve simultaneous screen-human viewing and hidden screen-camera communication. In *MobiCom*, pages 181–195, 2015.

[4] C. Zhang and X. Zhang. Litell: robust indoor localization using unmodified light fixtures. In *ACM MobiCom*, pages 230–242, 2016.