Poster: Secure QR Code Scheme Using Nonlinearity of Spatial Frequency

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

Chuang-Wen (Bing) You
National Taiwan University
Taipei, Taiwan
cwyou@ntu.edu.tw

Yi-Chao Chen
Guangtao Xue
Shanghai Jiao Tong University
Shanghai, China
yichao0319@gmail.com
gt_xue@sjtu.edu.cn

Xiaoyu Ji
Zhejiang University
Hangzhou, China
xji@zju.edu.cn

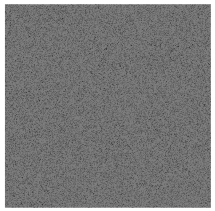
UbiComp/ISWC'18 Adjunct, October 8–12, 2018, Singapore, Singapore
ACM 978-1-4503-5966-5/18/10.
https://doi.org/10.1145/3267305.3267626

Abstract
Quick Response (QR) codes are rapidly becoming pervasive in our daily life because of its fast readability and the popularity of smartphones with a built-in camera. However, recent researches raise security concerns because QR codes can be easily sniffed and decoded which can lead to private information leakage or financial loss. To address the issue, we present *m*QRCode which exploit patterns with specific spatial frequency to camouflage QR codes. When the targeted receiver put a camera at the designated position (e.g., $30cm$ and $0°$ above the camouflaged QR code), the original QR code is revealed due to the Moiré phenomenon. Malicious adversaries will only see camouflaged QR code at any other position. Our experiments show that the decoding rate of mQR codes is 95% or above within 0.83 seconds. When the camera is $10cm$ or $15°$ away from the designated location, the decoding rate drops to 0 so it's secure from attackers.

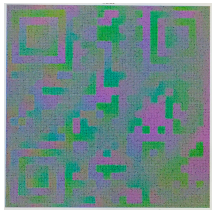
Author Keywords
QR Code; Security; Visual Encryption; Nonlinear System

ACM Classification Keywords
H.5.2 [Information interfaces and presentation (e.g., HCI)]: User Interfaces; H.4.3 [Information Systems Applications]: Communications Applications

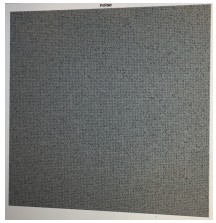
(a) Original QR code.



(b) mQR code: Encrypted QR code.



(c) Picture taken at designated position (color saturation is enhanced to make it more evident.)



(d) Picture taken at wrong position (off by $15°$).

Figure 1: mQR code can only be decrypted when the camera is put at the designated position.

Introduction

The matrix barcodes, known as Quick Response (QR) codes, are rapidly becoming pervasive around the world. QR codes are 2-dimensional barcodes that visually encode bits of information represented as black square dots placed on a white square grid. The data in a QR code can be accessed by taking a picture of the QR code and processing it with a decoder. QR codes become popular due to its fast readability and the popularity of smartphones with built-in camera. Applications include mobile payment, product tracking, item identification, time tracking, document management and general marketing.

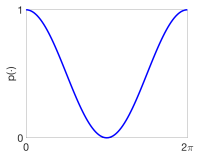
One of the security risks present with QR codes is the existence of Synchronized Token Lifting and Spending (STLS) attacks [2] where attackers take a picture of the victim's QR code and use the copied QR codes to access private information. Moreover, the sniffed QR codes can also lead to private information leakage. Encrypting messages in QR codes does not mitigate the concern because attackers don't need to decrypt the messages in STLS attacks.

Therefore, we propose *m*QRCode which exploits the nonlinearity of spatial frequency in light to camouflage and recover QR codes. Because *m*QRCode only relies on the existing physical property of camera and display for camouflage, no additional communication channel is required. When a QR code is generated, *m*QRCode encrypts it with a pattern with the designed spatial frequency, called mQR code, as shown in 1(b). When the receiver takes a picture of mQR code, mQR code is projected onto the pixel sensors of the camera . Because of the nonlinearity of spatial frequencies between the mQR code and the color filter array (CFA) of the camera, when the camera is positioned at the designated distance and angle, the original QR code is revealed due to the Moiré phenomenon and can be decrypted as shown in Fig. 1(c). When the encrypted QR code is taken by an attacker, the physical limitation naturally prevent the attacker from decrypting the mQR code.

Our experiments show that *m*QRCode can decrypt mQR codes in 25 frames (i.e., 0.83 seconds for $30fps$ camera). Moreover, when the camera is $10cm$ or $15°$ away from the designated location, the decoding rate drops to 0 so it's secure from malicious attackers.

Related Work

Existing techniques of visual cryptography (VC) [6] encode a secret image into share images such that stacking a sufficient number of shares reveals the original secret image. Among them, techniques of hiding images with Moiré patterns [1], which occur when digital repetitive structures are overlapped or viewed against each other, are explored in various research projects [3–5, 7]. [5] explored ways to superimpose various patterns of gratings to create the Moiré patterns of face images to be visualized by human eyes. [4] creates moving Moiré components running up and down at different speeds and orientations upon translation of the revealing line grating while [3] create secret sharing schemes whose shares are realistically looking images. [7] enables the creation of Moiré art and allows visual decoding by superimposing grating images printed on separate transparencies. These works require two semi-transparent layers and overlap one on the other to reveal the hidden image. Different from these works, *m*QRCode exploits the nonlinear optical interaction between a camera (specifically, color filter array) and a camouflaging pattern to hide QR codes. Because color filter array has a fixed pattern, it imposes additional constraint on the design of camouflaging patterns. Moreover, the simple black and white blocks in QR codes make it hard to directly apply existing approaches without being visually observable.



(a) $p(u) = 0.5 + 0.5cos(u)$

(b) $\phi(x, y) = x$.

(c) $m(x, y) = p(\phi(x, y))$.

Figure 2: Example of periodic and phase function.

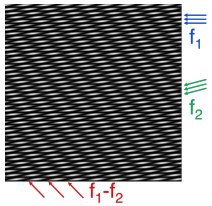


Figure 3: Nonlinear interaction of two patterns with frequency f_1 and f_2.

Background

Spatial Frequency

Spatial frequency is a pattern of any structure that is periodic across position in space. In this paper, we consider a curvilinear pattern which can be described by a frequency term and a phase term:

$$m(x, y) = p(\phi(x, y)) \quad (1)$$

where $m(x, y)$ represents the magnitude at a 2D coordinate (x, y) (i.e., color of the image), $p(\cdot)$ is a periodic function representing the frequency of the pattern, and $\phi(x, y)$ is a phase function representing the angle of the pattern. For example, Fig. 2(a) shows using a cosine wave as the periodic function with the frequency $1/2\pi$. When the phase function is set to $\phi(x, y) = x$, we can get a pattern with repetitive horizontal lines as shown in Fig. 2(c).

Nonlinearity of Spatial Frequency

When two spatial patterns overlap, the nonlinear optical interaction of the patterns creates additional visible pattern, called Moiré pattern, on top of the original patterns. Assume m is the superposition generated by the nonlinear interaction of two layers m_1 and m_2:

$$m(x, y) = m_1(x, y) \times m_2(x, y) \quad (2)$$

When m_1 and m_2 use cosine functions with frequency f_1 and f_2 as periodic functions:

$$\begin{aligned} m_1 \times m_2 &= (a_1 + b_1 cos(2\pi f_1 t)) \times (a_2 + b_2 cos(2\pi f_2 t)) \\ &= a_1 a_2 + a_1 b_2 cos(2\pi f_2 t) + a_2 b_1 cos(2\pi f_1 t) \\ &\quad + b_1 b_2 cos(2\pi (f_1 + f_2) t) + b_1 b_2 cos(2\pi (f_1 - f_2) t) \end{aligned}$$

We can see combining two cosine functions results in two additional frequencies $(f_1 + f_2)$ and $(f_1 - f_2)$. Because human eyes are more sensitive to low frequency patterns, frequency $(f_1 - f_2)$ is easier to observe as shown in Fig. 3.

Method

System Overview

*m*QRCode is designed to guarantee the high security of transmitting information using QR Code. The system architecture comprises two parts: encryption and decryption. In the encryption step, we model the spatial pattern of the color filter array (CFA) and use the phase modulation to generate the encrypted QR code image. In the decryption step, we use a smartphone's built-in camera to capture the image at the designated distance and angle and extract the message from the QR code.

Encryption

*m*QRCode exploits the nonlinear optical interaction between the color filter array (CFA) and the camouflaging pattern to hide QR codes. From Eq. 2, without loss of generality, we assume the spatial pattern of CFA is $m_1(x, y)$ and the QR code is $m(x, y)$. The goal of the encryption is to compute $m_2(x, y)$ such that $m = m_1 \times m_2$.

Model CFA

We first model color filter array (CFA) by formulating $m_1(x, y) = p_1(\phi_1(x, y))$ in Eq. 1. In photography, CFA is a mosaic of tiny color filters placed over the pixel sensors of an image sensor to capture color information. The Bayer filter is the most common filter which gives information about the intensity of light in red, green, and blue in a 2×2 array as shown in Fig. 4. We model the green layer using cosine waves as the periodic function: $p_1(u) = 0.5 + 0.5cos(u)$, and use $\phi_1(x, y) = ((x + y + 1) \mod 2) \times \pi$ as phase function.

Phase Modulation

To compute $m_2(x, y) = p_2(\phi_2(x, y))$, we let $p_2(u)$ equal to $p_1(u)$ so the resulting Moiré pattern has larger contrast in color [7]. We apply phase modulation by mapping black and white blocks in a QR code to different phases:

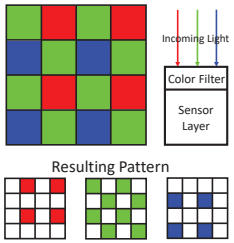


Figure 4: Profile of sensor with the Bayer arrangement of color filters.

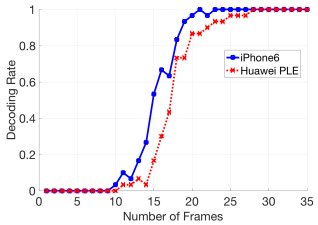
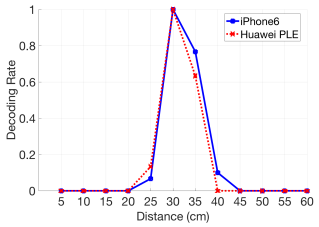
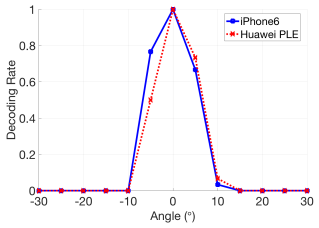


Figure 5: The number of frames required to decrypt a mQR code.



(a) Impact of distance.



(b) Impact of angle.

Figure 6: The decoding rate of mQR code designed for $30cm$ and $0°$.

$$\begin{cases} \phi_2(x,y) = ((x+y) \mod 2) \times \pi & \text{, for white blocks} \\ \phi_2(x,y) = ((x+y+1) \mod 2) \times \pi & \text{, for black blocks} \end{cases}$$

Decryption

As shown in Fig. 1(c), the Moiré pattern naturally reveals the original QR code when the picture is taken at the designated position. However, because of the distortion at the edge of the camera and the difficulty to put the camera at the exact position, the Moiré pattern may not be obvious at part of the picture. Therefore, we record a video at $30fps$ and use a series of frames for decryption. For each frame, we use the quiet zone to identify the position of mQR code, convert it to black and white, remove noise using the median filter, and detect edges. Then we combine edges from multiple frames to remove blur part. Finally, we perform block padding to fill in black and white from the edges.

Evaluation

We generate a QR code with the error correction level "M" and use *m*QRCode to encrypt it. The generated mQR code is designed for the receiver positioned at $30cm$ and $0°$ to it. The mQR code is displayed using a Samsung S7 Android phone. We use built-in camera of two phones (iPhone6 and Huawei LPE) to record a video at $30fps$ for 5 seconds at various positions. Each experiment is repeated 30 times and we report the average rate that we can correctly extract the message in the QR code.

Decoding Time

We first show that when the camera is positioned at the correct position, the number of frames it takes to decode the mQR code. From Fig. 5, we can see that for both phones, the decoding rate is 95% or higher when we use 25 or more frames. It shows that user can get the message from the mQR code within 1 second.

Working Range

*m*QRCode is designed to guarantee the high security. Fig. 6(b) shows the decoding rate when the camera is positioned at the correct distance but various angles. Fig. 6(a) shows the decoding rate when the camera is positioned at the correct angle but various distances. We can see that when the camera is $10cm$ or $15°$ away from the designated position, the decoding rate drops to 0.

Acknowledgements

The work is supported by the Joint Key Project of the NSFC (U1736207), NSFC (61572324), China NSFC Grant 61702451 the Fundamental Research Funds for the Central Universities 2017QNA4017, and in part by the Ministry of Science and Technology of Taiwan (MOST 106-2221-E-002-061 and 107-2221-E-002-148-MY2).

REFERENCES

1. I. Amidror. *The Theory of the Moiré Phenomenon: Volume I Periodic Layers*. Springer, 2nd edition, 2014.
2. X. Bai, Z. Zhou, X. Wang, Z. Li, X. Mi, N. Zhang, T. Li, S.-M. Hu, and K. Zhang. Picking up my tab: Understanding and mitigating synchronized token lifting and spending in mobile payment. In *USENIX Security Symposium*, 2017.
3. Y. Desmedt and T. van Le. Moiré cryptography. In *ACM Conference on Computer and Communications Security*, 2000.
4. R. D. Hersch and S. Chosson. Band moiré images. *ACM Trans. Graph.*, 2004.
5. G. Lebanon and A. M. Bruckstein. Variational approach to moiré pattern synthesis. *J. Opt. Soc. Am. A*, 2001.
6. P. Punithavathi and S. Geetha. Visual cryptography: A brief survey. *Information Security Journal: A Global Perspective*, 26(6):305–317, 2017.
7. P. H. Tsai and Y. Y. Chuang. Target-driven moire pattern synthesis by phase modulation. In *IEEE International Conference on Computer Vision*, 2013.