# CypherEye™: A Robust, Secure and Versatile Optical Code

The combination of the natural advantages of CypherEye frame encoding, the dynamic nature of the code (making it hack resistant) and the out-of-band non-IP channel that this optical encoding represents, make the use of this technology a significant advantage for authentication.

## QR Codes are Problematic

In the industry today we see a lot of polemics around methods of direct surface data reading. It is used in product marketing, point of sales terminals and even airplane ticketing. One of the more popular techniques for transmitting digital information optically is encoding web addresses (urls) with a QR code. Unlike barcodes that appeared in the 1960's, QR Codes are a more ecent (late 80's) invention of the Japanese Automotive industry. Automobile producers in Japan needed to code more information per unit of area than that of what barcodes could allow.

While the technology is mature enough for commercial use the QR code technology has three major sets of problems:

1. Lack of Standardization
2. Recognition Challenges
3. Phishing Challenges

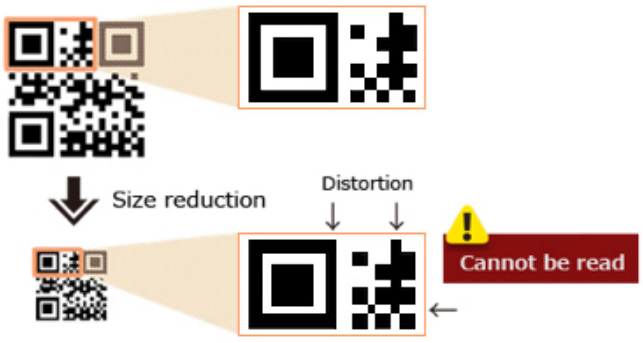
### 1. Lack of standardization

QR Codes consist of four different types and many additional variations. The ISO/IEC standard 18004:2000 that appeared 14 years ago was first attempt to standardize. in 2006 it was replaced with updated standard. The mobile phone industry is using NTT DoCoMo, a substandard implementation (that became the standard de-facto) for URL coding. There are also open source projects that tend to maintain their own standards. For instance, ZXing tries to maintain all but with some modifications.

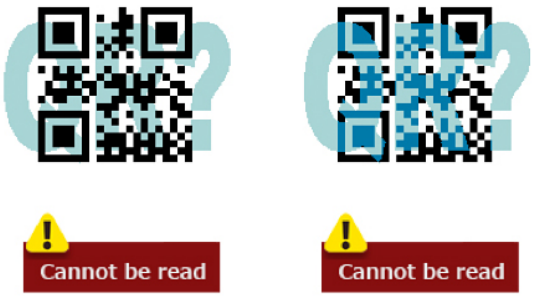
### 2. Recognition Challenges

Here are 3 major groups of technical recognition challenges:

a. Distortion and intolerance to affine transformation (skew for instance). Small distortion or even scaling up or down may render a normally looking QR Code unrecognizable.




b. Intolerance to partial obscurity. Even if a small portion of the QR Code is covered with a graphic or image the underlying QR code becomes unrecognizable. In some cases if a pattern is printed below QR Code it becomes unrecognizable as well, because the contrast of elements is lost.




c. With many QR code implementations other problem appears. Many algorithms do not tolerate frames or even patterns drawn around QR Codes. If QR Code is near or included in the border, the recognition mechanism often fails.


## 3. Phishing challenges

Phishing is the main security issue involved with QR codes. It is sometimes referred to as QRishing. QR codes are generally scanned by a mobile phone to get redirected to a website. This is where scammers try to trick users by changing the QR code in the ad or the referencing URL. They can also publish similar looking fake ads as a misdirect. Most people judge a website by its look and feel, and fake QR codes can send them to sites that look similar to legitimate websites. On mobile devices, browsers do not show the full address due to limited space, therefore making bad redirects even harder to detect. When user then login to these page, their passwords and other credentials are compromised.

Drive-by download to distribute ransomware. By using QR codes to point to drive-by download websites, hackers easily trick users. Users cannot see the URL, so there is no point at which the user feels concern for security. Because QR codes do not require entering a URL manually, this gives hackers a perfect opportunity to gain valuable information.

Websites with exploits. Sometimes websites have vulnerabilities that can launch their own attacks. Browser exploits can send bad email, enable Remote Code Execution, access microphone/camera access, hijack data and more. All these actions occur in the background, so users never know about it. They only see a website, but their QR codes are putting them in peril.

## Introducing CypheEye™

The way QR Codes work is based on matching of high-contrast patterns. This is a reasonable approach that was designed for use on old digital cameras. This method does not require much computing power or high-resolution sensory pads within the cameras and can work on relatively low-cost devices.

CypherEye is built to work on color dispersion instead. The encoding scheme includes at least three colors arranged in an arc (along a portion of the inner circle) which are used for calibration. The calibration region which is executed with a green “eye”, is used for color calibration and orientation. The first inner ring is composed of 16 colored arc segments the second ring is composed of 20 colored arc segments. Accordingly, 36 colored arc segments are arranged on the two rings. Three arcs of the inner ring can be used as an additional calibration elements or a calibration region. These elements set an encoding palette for CypherEye. During a recognition or imaging process, the colors of coding arcs

are compared with calibration colors. In this view of the CypherEye, the colors of the calibration arcs correspond to the numbers “2”, “I”, “0”.

For detection, the recognition is based on the search of closed elliptical contours in mask images. For example, four masks are used for contour searching: a) a variance mask that shows distribution of overthreshold variance of intensity over image, b) a green mask that indicates presence of green color, c) an adaptive binarization (ada-bin) mask that shows distribution of high-value intensities over image, and d) a white mask indicating the presence of white color.

This method is what makes CypherEye tolerant to geometric transformations and loss of contrast. The background variances are not a problem at all and CypherEye’s method of recognition will tolerate partial covering of the image of CypherEye. Here is a comparison of CypherEye v.s. QR codes:

| Parameter | CypherEye | QRCode |
|---|---|---|
| AT Tolerance | YES | NO |
| Background Pattern Tolerance | YES | NO |
| Information redundancy | YES | NO |
| Partial obscuring | Possible | Impossible |
| Ability to work with modern equipment | Good | Probable |
| Frames per second for recognition average | 6 | 12 |
| Does user need training to use the code? | NO | YES |
| Probability of correct recognition | 85% | 60% |
| Standardization | 1 standard | 7 standards |

## Use of CypherEye in the Context of Security

CypherEye authentication system relies on using elements of security distributed across multiple distribution points in the protocol.

A dynamic CypherEye code is used as a CypherEye authentication session identifier and a one time password. The dynamic nature of the code allows encoding of a higher level number. Additionally, the code provides resistance to replay and man-in-the-middle attacks due to its dynamic nature. It is divided into multiple sub numbers for each encoded CypherEye frame. These CypherEye codes are shown at 4fps speed one after another. When CypherEye is recognized, its code is sent back to the server where it is matched with actual session identifier.

What’s encoded is a transaction ID, a time-limited one-time password (TOTP), and some service information to strengthen the process of encoding as a part of the authentication protocol. Only third-parties who are authenticated can initiate transactions. The dynamic nature of the optical code provides sufficient encoding depth and channel robustness for high level password security.

To complete a transaction, the code is read through a mobile phone camera. The optical nature of the code recognition creates an out-of-band transaction verification channel that is air-gapped from the network and over which the digital service is provided.

The combination of CypherEye’s frame encoding, the dynamic nature of the code, and the out-of-band non-IP channel that this optical encoding represents, make the use of CypherEye technology a significant advantage for both user authentication and resistance to password hacking.