April 2021

VISUAL FIDUCIALS FOR PRIVACY AND SECURITY

Kevin Redmon

Bradford Ingersoll

Konrad Reszka

VISUAL FIDUCIALS FOR PRIVACY AND SECURITY

AUTHORS:
Kevin Redmon
Bradford Ingersoll
Konrad Reszka

ABSTRACT

It can be difficult and time-consuming to maintain personal security and privacy while participating on-line video experiences. Many modifications can be provided post-production but this is unrealistic in the real-time world in which video/camera systems are often utilized. Presented herein is a technique for using a Quick Response (QR) code or other similar encoding mechanism within the field of view of a video/camera solution as a means to provide real-time/in-stream configuration of privacy and security zones. The encoding mechanism would contain all information necessary to define these zones. Once detected within the field of view, these zones would remain in effect until actively disabled.

DETAILED DESCRIPTION

In the remote secure workforce situation involving many professionals today, there are an increasing number of video experiences, such as videoconferences, social media, online training resources, etc. It can be difficult and time-consuming to maintain security and privacy concerns from both a personal and a professional perspective while a person is participating in a professional role. Many modifications can be performed post-production but this is unrealistic in the real-time world in which many people operate.

For instance, in most videoconference applications, a meeting "host" will have an account via a video conference solution/application. Other users can join the host's meeting for the scheduled meeting time. In some instances, the meeting "owner" may choose to modify their background—possibly using a pre-defined privacy zone/area on the video stream. However, some/many of the meeting invites may be "guests" on such a system. Currently, guests may not have the ability to configure settings that persist for each meeting on the system and, thus, may need to reconfigure such settings during a later meeting. This can have a significant impact on the usability of such solutions and, therefore, the ongoing

privacy and security of such systems as well as a potentially diminished user experience. This problem can be further aggravated if the user (host or guest) is forced to use multiple vendor solutions.

Beyond business sensitive data that may need to be obscured, if a user is participating in a video call from their home, they may have decorations, displays, doorways, shelves, or other personal items they do not wish to be shared during a video session (e.g., inappropriate work decorations or posters, doorways to bathrooms, personal pictures, etc.). It would be unreasonable to request the user to frequently or permanently change or re-arrange their home.

This proposal provides for using a QR code or other similar encoding mechanism within the field of view of a video/camera solution as a means to provide real-time/in-stream configuration of privacy and security zones. Once detected within the field of view, these zones would remain in effect until actively disabled. The content of the encoding mechanism would contain all of the necessary information to properly implement–relative to the encoding mechanism's position within the field of the view–the size and location of the privacy zone. Figure 1, below, illustrates an example of the video/camera solution in which QR codes can be physically placed at different areas at which privacy zones are desired and used as the encoding mechanism for such privacy zones.

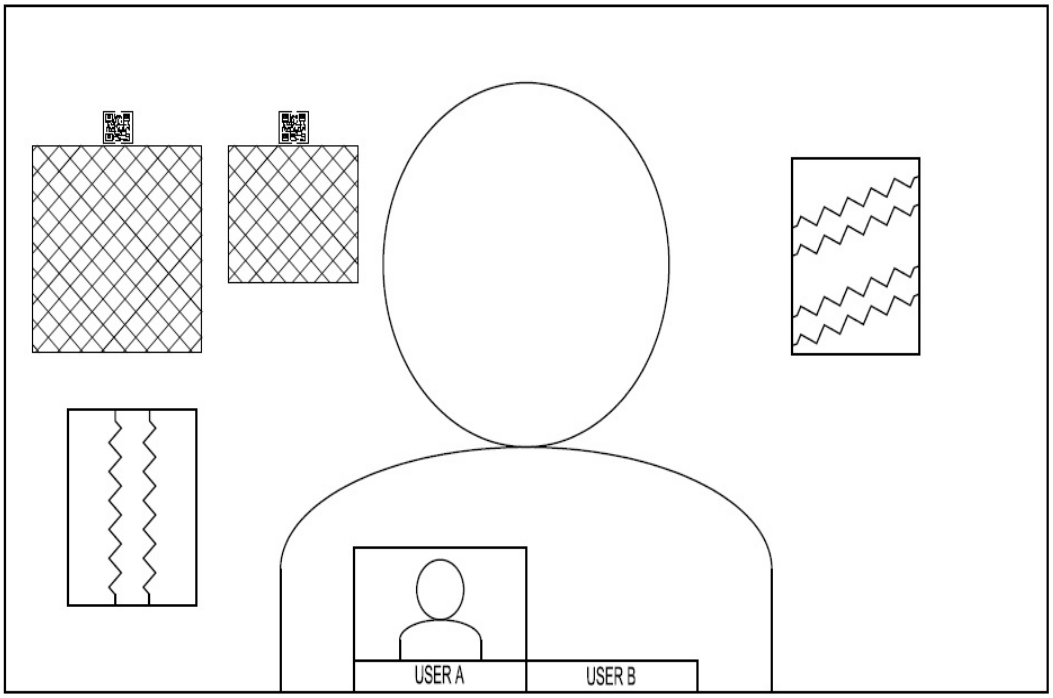

Figure 1: Privacy Zones based on QR Codes

Such a solution as illustrated in Figure 1 is better than existing privacy solutions because current solutions require static pre-configuration and/or post-processing to achieve a similar outcome as described and depicted above. It is often not feasible to remove private or sensitive data before every video call. This is further exacerbated if the user is in a home setting in which there may be certain decorations, shelves, doorways, displays, monitors, or other items that cannot be easily relocated. The technique of this proposal provides for a non-permanent, or at least a minimally invasive, solution to protect user privacy and confidential data. Small QR codes as illustrated in the example of Figure 1 can be left up, or quickly placed/taped wherever they need to be used.

Virtual and blurred backgrounds are another option to mask or hide the area behind a user; however, these do not always have a professional appearance. Many backgrounds can be highly distracting due to unnatural lighting or lighting conditions that don't match the foreground. Furthermore, these blurred/virtual background solutions often replace the entire background, which may be overreach for certain applications in which only a small portion of a scene needs to be obscured.

In some instances, the technique presented herein may build upon other potential solutions by providing greater flexibility with what is obscured, does not require central processing unit (CPU) intensive processing to erase or otherwise use a 'content aware fill' to obscure an image, and does not rely on Optical Character Recognition (OCR), which can be less than optimal for handwritten characters/text.

To implement the privacy zones of this proposal, a QR code or other encoding mechanism can be physically placed at a location and encode strings of text that define the privacy zone. Thus, QR codes/encodings can be generated to encode information necessary to describe/define a privacy zone. Consider an example as illustrated via Figure 2, below.

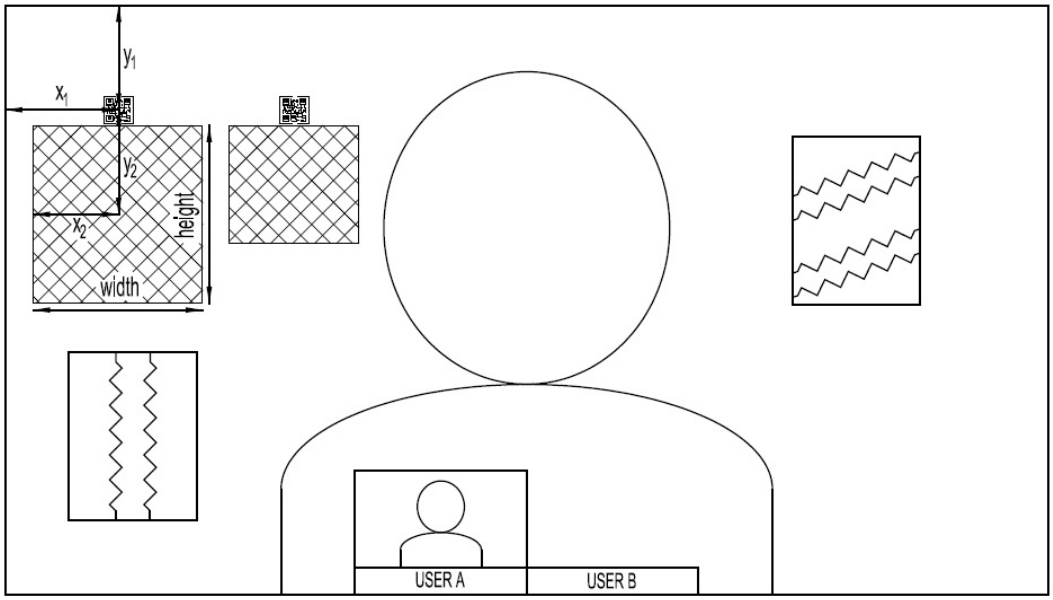

Figure 2: Privacy Zone Size and Position Details

For the example as illustrated in Figure 2, consider that a given privacy zone involves a size ('WIDTH' and 'HEIGHT') and position ('X' and 'Y'). These four parameters can be encoded in a pattern, such as X_2, Y_2, WIDTH, HEIGHT in which this sequence contains the necessary information to superimpose the privacy zone on top of the video. The position, denoted by X_2 and Y_2, can indicate (e.g., in pixels) the horizontal and vertical offset of the center of the privacy zone relative to the center position of the QR code itself (determined by X_1, Y_1). The WIDTH and HEIGHT (which can also be in pixels) determines the size of the zone, with the zone centered on the X_2 and Y_2 coordinates

(translated from the center of the QR code centered at X_1 and Y_1). The privacy zone can, thus, be defined relative to the QR code.

Various physical constraints involving QR codes may be considered. For example, in order to detect and read a QR code, a camera must have a high enough resolution and the QR code must be sufficiently close to the camera. These two parameters are vague, as real-world implementations can vary greatly and are highly dependent on camera lens and sensor factors. The size of QR code position markers, as illustrated for the QR code in Figure 3, below, can also be a factor (e.g., the larger the position markers, the easier for a camera to detect).

Figure 3: Example QR Code

QR codes were originally designed for a 10:1 distance to size ratio, but that is not a hard requirement nor reflective of many real-world implementations. Current tests indicates that a 1.5" square QR code encoded with privacy zone data can be successfully read from a distance of 13' using a small camera of a mobile phone. Cameras used in video endpoints are likely to have a larger sensor and possibly greater optical zoom capabilities.

Thus, conference rooms, home offices, and other private areas that may appear within the frame of a video conference would generally fit within this distance. If sensitive or private content is visible and legible for a camera, there is a good chance the QR code would also be legible. Furthermore, camera and imaging capabilities advance yearly, and these improvements will increase the scaling-ratio at which this the technique of this proposal could be implemented (e.g., smaller QR codes and greater distances to detection).

Various implementation factors may also be considered. For example, consider that a user has a personal computer monitor, doorway, or other photos that they do not wish to be seen on a video conference. In one instance, the user could navigate to a website or an

application that could assist in determining an appropriate width and height of a privacy zone. This could be performed by uploading a picture from a webcam/video endpoint, or if integrated with a collaboration solution, utilize a live video endpoint to assist in the privacy zone dimensioning and placement.

In one instance, the user could identify, simply with a cursor placement, a location at which the QR code can be placed. The user could then "drag" a rectangle around an area that would define the size of the privacy zone. Based on such a selection, the website/application could determine the appropriate X, Y coordinates for the center of the privacy zone based on the location of the QR code itself. In one instance, the application may even ask how far away the QR code is from the camera in order to determine an ideal size for printing the QR code. The application could either generate the QR code or present the necessary text string that the user could paste into another QR code generating application (e.g., to utilize a fun shape or design). QR code generating applications are widely available. Once generated, the user would print (and potentially cut out) the QR code and place the QR code in the position that was previously designated.

When starting a video conference, the video/camera system would scan the image for QR codes and, if detected, decode the contents and super-impose the privacy zone onto the video stream before transmitting. If the QR code moves during the video conference, the privacy zone would move with it (with the position always relative to the QR code position as detected by the camera). Whether this update occurs in real time, or through a manual update, would depend on the processing power of the video endpoint. The same QR code can be reused multiple times.

In some instances, the technique of this proposal could involve presenting an image in the specified area of a privacy zone rather than a white/blacked out area. In such instances, a Uniform Resource Locator (URL) for an image could be encoded as a fifth parameter within a QR code.

Although various measurements/physical activities are discussed herein involving the use of QR codes that can be customized based on specific users environments, use of QR codes does not need to be manual/explicit in nature. Rather, the technique of this proposal enables a battery of implementation options. To minimize/mitigate any manual process, vendors may also choose to provide branded content "hand-outs" that include a

QR code (e.g., at a trade show, bundled with a hardware endpoint, etc.) with pre-configured privacy content/"policy" as an alternative to webcam privacy covers.

In one instance, the contents of a QR code may contain Extensible Markup Language (XML) data, JavaScript Object Notation (JSON) data, and/or the like such that the "QR code Fiducial" can be used to convey a relative focal point of a background environment from where all measurements can be made (i.e., absolute measurements are not imperative). Alternatively, in the provided contents of the QR code, the privacy area may be measured relative to the QR code Fiducial or given as absolute measurements of the physical environment (as perceived by the video endpoint). The XML/JSON content may allow various capabilities, such as:

- With the use of XML/JSON payload, the QR code may contain an image URL that may be used as a branded virtual background (e.g., the trade show example, noted above);
- Providing for the placement of an embedded image at a prescribed location.
- Blocking out a prescribed shape relative to the position of the QR code by identifying a rectangle of L x W relative to the QR code that would auto-adjust based on the field of view (FOV);
- Showing a URL at a particular location; and/or
- Presenting the QR code as:
    - A Printout;
    - A digital device or "picture frame" in view of the video conference solution; and/or
    - A branded hand-out (e.g., from a trade show via a "post card" hand-out, a sticker, etc.).

Accordingly, the technique of this proposal may provide various advantages, such as being:

- Quick – a custom or branded/curated QR code can be printed/provided, placed at a location, and privacy can be enabled;
- Simple – no custom hardware or membership to the conferencing solution is required;

- Flexible – not everyone may have a designated area reserved for "professional" interactions and it is not always palatable for people to blend their professional and personal lives (i.e., some users may prefer to not share their personal preferences/life with professional contacts); and
- Non-destructive – taking down or easily removing items for every meeting may not be possible nor desirable and may conflict with a work/life balance (i.e., sharing an environment with roommates, personal effects may indicate religious/cultural affiliations, etc.); further, some people may be willing to share a personal environment with peers but not with a professional contact.

If a more involved filtering process and/or additional customizable features were to be utilized, a more advanced configuration interface may be utilized in addition to and/or in lieu of the interface described herein. Such an advanced interface is likely to also involve advanced tools, expertise, and/or subscription to the video collaboration service (i.e., available only to a member of the service versus joining as a guest).

Other potential solutions involving cameras blocking out defined areas, however, such areas are often statically configured as part of a management dashboard and, thus, involve access to such a dashboard. In contrast, the technique of this proposal provides for making the privacy zone configuration a part of the environment, which can be dynamically detected and accessible to all platform users (e.g., both paid users and guests).

For instances in which lighting may change and/or a QR code may not be read, a default policy can be configured to update the privacy area only upon a rescan of the QR code. Otherwise, the privacy area could be configured to remain static for duration of a current call. If the camera FOV were to change intentionally or unintentionally, the expectation would be that the QR code could be rescanned in order to re-instantiate the privacy area. As a function of the QR code, the version, size, and error correction employed within the QR code may help to mitigate accidental blocking of some of the image. A rescan could be performed whenever the camera has an opportunity to re-process the contents of the QR code.

For instances in which an endpoint may move or be moved, as long as the QR code is still visible and readable, the privacy zone will remain in effect. Recall, the QR code

includes the zone definition (as noted above, the QR code may contain JSON/XML data) and may employ any combination of relative measurements, absolute measurements, augmented reality information, etc. as contained within the QR code, thereby enabling a more dynamic adjustment (e.g., blacking out a rectangle of a length and width) of the privacy zone.

In summary, this proposal provides for using a QR code or other similar encoding mechanism within the field of view of a video/camera solution as a means to provide real-time/in-stream configuration of privacy and security zones. The encoding mechanism would contain all information necessary to define these zones. Once detected within the field of view, these zones would remain in effect until actively disabled.