November 2022

Embedding Invisible Fingerprints in Displayed Content to Facilitate Seamless Sharing

D Shin

Embedding Invisible Fingerprints in Displayed Content to Facilitate Seamless Sharing

ABSTRACT

Participants in a physical meeting are often interested in accessing content that is presented on a display during the meeting. However, to enable participant access, the presenter needs to obtain their contact information and share a link to the contact to all participants. This manual approach is cumbersome, inefficient, and error prone. This disclosure describes techniques for seamless and dynamic sharing of content by augmenting the user interface (UI) of presented content by embedding spatial and/or temporal fingerprints. The fingerprints are invisible to the human eye, but detectable by device cameras of participants. Meeting participants can capture a photo of the screen that displays the content. The captured image is processed on-device to detect the embedded fingerprint that is linked to the content and an option to access the content is displayed to the user. The techniques described in this disclosure provide a distributed user experience (UX) for content sharing triggered by actions taken by interested participants and avoid unnecessarily broadcasting the content link to others.

KEYWORDS

- File sharing
- Invisible fingerprint
- Embedded fingerprint
- Content sharing link
- High Dynamic Range (HDR)
- Region-proposal network
- Code modulation

BACKGROUND

Users often present material from shared documents (e.g., word processing documents, slide presentations, etc.) during in-person meetings held in a physical space such as a meeting room. In many situations, users wish to share the file(s) being presented with those attending the meeting. Currently, the common way of sharing the file(s) is to compile a list of email addresses of everyone with whom the content is to be shared and to send a link to the content via email. Gathering the requisite email addresses requires the sharer to search one or more sources, such as emails, calendars, online directories, etc. and/or ask others to send contact information electronically or on paper. Such a manual approach is cumbersome, inefficient, and error prone.

DESCRIPTION

This disclosure describes techniques for seamless and dynamic content sharing by augmenting the user interface (UI) by embedding content fingerprints that are invisible to the human eye, but detectable by a digital camera, such as on a smartphone, tablet, wearable device, or any other device. The content fingerprints for a given piece of content include a suitably crafted unique digital code, analogous to the functionality of the well-known quick response (QR) codes.

When a user presents content with such embedded fingerprints on a publicly visible display, e.g., a large screen in a meeting room, audience members can obtain a link to the content by taking a photo of the screen with their devices such as smartphones. If an embedded fingerprint is detected in the captured photo, it can be recognized with backend parsing. Since the fingerprint maps uniquely to a piece of content, such as a document, presentation, etc., the link to the content can be surfaced automatically on the device via any appropriate mechanisms such as pop-ups, notifications, (silent) text message, etc.

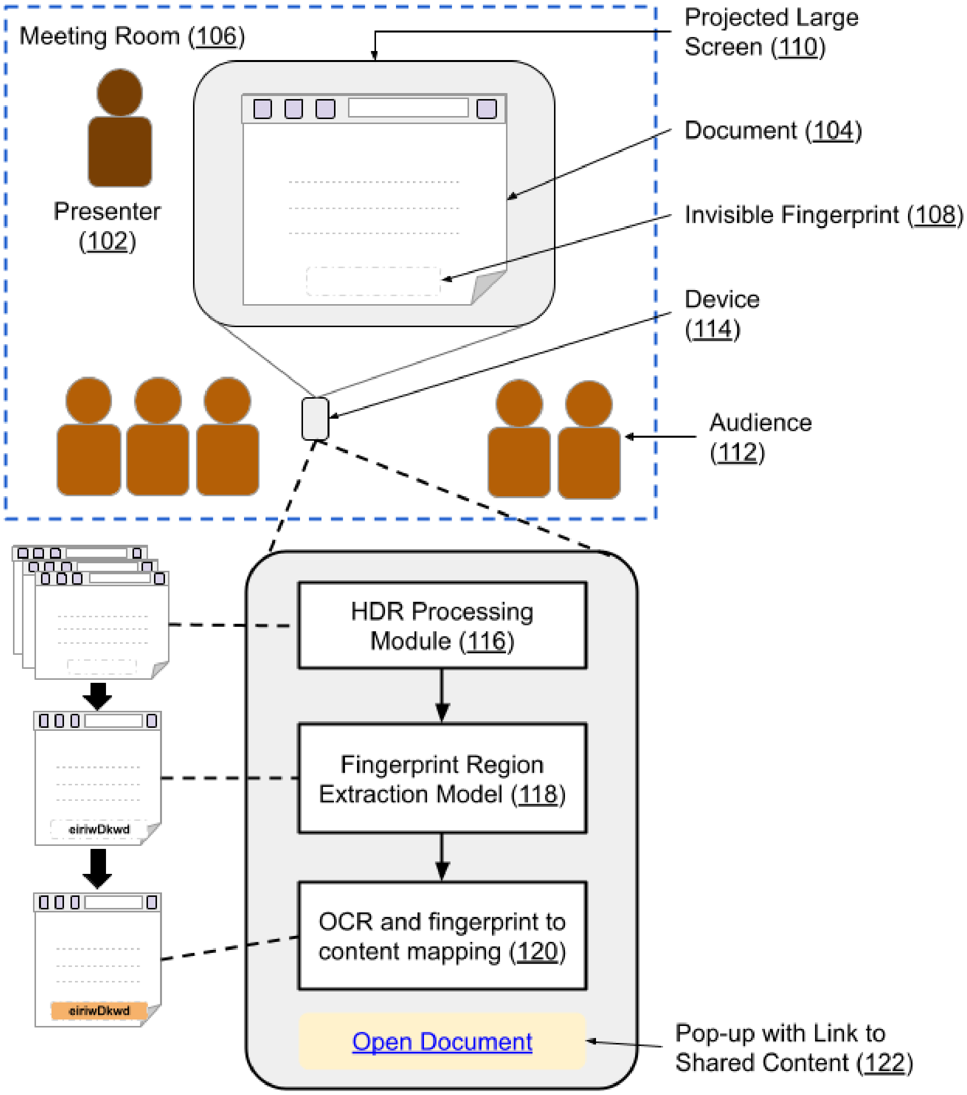
Meeting Room (106)
Projected Large Screen (110)
Presenter (102)
Document (104)
Invisible Fingerprint (108)
Device (114)
Audience (112)
HDR Processing Module (116)
Fingerprint Region Extraction Model (118)
OCR and fingerprint to content mapping (120)
eiriwDkwd
eiriwDkwd
Open Document
Pop-up with Link to Shared Content (122)

Fig. 1: Obtaining a link to a document via photos of content displayed on a screen

Fig. 1 shows an example of operational implementation of the techniques described in this disclosure. A presenter (102) is displaying a document (104) on a large screen (110) to an audience (112) of participants in a meeting room (106). With permission, a meeting participant in the audience uses the camera of a device (114) to capture a photo of the document as displayed on the screen, e.g., in the form of a raw burst of a few photos taken within a subsecond.

Upon processing (116) the captured burst, a custom high dynamic range (HDR) image obtained using the captured set of burst images reveals the embedded fingerprint code that is invisible to the human eye. Since a photo of the document with the revealed fingerprint includes the document, a suitable trained machine learning model (118) is employed to extract the portion of the image that includes the local region within the document margins where the embedded fingerprint is located.

The extracted local region that includes the fingerprint image is processed using standard optical character recognition (OCR) techniques to obtain the unique fingerprint as a text code. The code can be a unique hash ID based on attributes such as file owner, creation time, file content, etc. such that it ensures a 1:1 relationship between the code and the content file. The code is transformed using a suitable hash function to obtain the unique stored mapping to the document (120). The user is then shown a pop-up user interface element with a link to open the content (122) on the device.

The region that includes the fingerprint within an HDR-processed image can be identified using a region-proposal network that is trained offline on labeled photos of content (training data) that include a fingerprint within it. The region-proposal network can take the form of a convolutional U-Net that takes as input a raw HDR image. The output of the network is a heatmap that indicates the areas within the input image that have a high likelihood of containing a fingerprint. A heuristic that takes a convex hull (e.g., a translated/rotated rectangle) around the heatmap is applied to the heatmap image output by the U-Net.

Spatial fingerprints based on dynamic range described above take advantage of the few-photon sensitivity of the cameras in current devices. The high sensitivity of the cameras permits detection of codes that have been embedded using subtle coloring that is invisible to the human eye but that is detectable with HDR boosting on the camera. The HDR boosting can be performed using a suitable number of burst images, e.g., five to ten images.

The embedded fingerprints can also be temporal. Temporal fingerprints are based on the observation that human vision is such that a human user is unable to perceive 60-cycle alterations of lighting that can however be captured by cameras on modern devices. Therefore, code modulation that exploits aliasing on high-frequency displays can be employed to construct temporal fingerprint codes that are invisible to humans but that can be detected by a device camera.

Unlike the current approach of content sharing that involves a central host user broadcasting material manually to other users, the techniques described in this disclosure provide a distributed user experience (UX) for content sharing. Moreover, content sharing via the techniques described in this disclosure is triggered by the receivers of the shared content. The resulting pull model of content sharing permits interested users to access the material on their devices while avoiding unnecessarily broadcasting content links to others.

With user permission, the embedded fingerprint can be provided in any type of content that is suitable for sharing among a group of users. The content to be shared can be hosted within any service, application, or platform via which users can create, display, and share content. The fingerprint invisible to the human eye can be embedded within the displayed content at any suitable place, such as margins, toolbars, status bars, etc. Implementation of the techniques can make it seamless and efficient to share access to content projected for display in shared gatherings, such as meetings, conferences, etc., thus enhancing the user experience.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user’s documents or other content, profession, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques for seamless and dynamic sharing of content by augmenting the user interface (UI) of presented content by embedding spatial and/or temporal fingerprints. The fingerprints are invisible to the human eye, but detectable by device cameras of participants. Meeting participants can capture a photo of the screen that displays the content. The captured image is processed on-device to detect the embedded fingerprint that is linked to the content and an option to access the content is displayed to the user. The techniques described in this disclosure provide a distributed user experience (UX) for content sharing triggered by actions taken by interested participants and avoid unnecessarily broadcasting the content link to others.