September 2021

ENHANCING WEB CONFERENCING PRIVACY PROTECTION

Karthik Babu Harichandra Babu

Akaash Dev Sc

Amit Kumar

ENHANCING WEB CONFERENCING PRIVACY PROTECTION

AUTHORS:
Karthik Babu Harichandra Babu
Akaash Dev Sc
Amit Kumar

ABSTRACT

With the prevalence of remote work, it is possible that a significant amount of highly confidential or restricted data may be shared and discussed over virtual meeting applications. The most vulnerable point during a highly confidential (or casual, off-the-record) meeting is each individual's client, which could allow a user to record the screen or take a series of screenshots. Presently, solutions exist that either allow complete recording of the screen, including the meeting windows, or no recording at all. However, there is no solution that enables the complete functionality of other windows or applications while blocking the meeting content alone. To address the types of challenges that were described above, techniques are presented herein that support selectively blocking only the vulnerable sections of a screen in a non-intrusive way thus ensuring both user convenience and privacy protection.

DETAILED DESCRIPTION

With the prevalence of extensive remote work, a significant amount of highly confidential or restricted data may be shared and discussed over virtual meeting applications. However, all of the protection for such streams is at the host's side (e.g., the sharing of specific windows, screens, etc.). There is little to no protection on an attendee's side, with respect to the handling of confidential data or avoiding a direct screenshot or screen recording. While there are solutions in the area of proctored online tests that address aspects of such a lack, those solutions take things to the other extreme where, for example, other activities on a device are hindered.

The issue of sharing screenshots online without the consent of a presenter (or in the case of a video stream, the individual) is a very widespread problem. There is no non-

intrusive digital rights management (DRM) -like approach to preventing a direct screen grab when either confidential data is being shared or casual video calls are being held.

To address the sorts of challenges that were described above, techniques are presented herein that support needed protection mechanisms. Aspects of the presented techniques will be described and illustrated in the narrative below. In brief, the elements of the presented techniques include:

1. A non-intrusive filter for screen recording or screenshots. In essence, this element is all about protecting the meeting stream at the attendee's side.
2. The greying-out of a window (or the parts of a meeting window) in such a way that it does not impact any other windows and the storing of a screenshot (or recording).
3. A simple three-way split and a two-rectangle cover that supports aspects of the presented techniques and protects against screenshots (or recordings).
4. The conveyance by a meeting application to the operating system (OS) of the coordinates that are to be greyed-out so that the OS may then capture, modify, and store a greyed-out screenshot.

As noted above, a first element of the techniques presented herein encompasses a non-intrusive filter for screen recording or screenshots.

Such a non-intrusive filter works, according to aspects of the techniques presented herein, by capturing a screenshot or a recording and storing the same with a greyed-out meeting window (or parts of such a window). In support of this capability are two important constructs – a meeting window interpretation and a two-rectangle filter.

A meeting window interpretation considers that every meeting window may be split into (or viewed as a combination of) three panels – a presentation section (e.g., the display of shared content), a video stream, and an interaction panel. Consequently, a fully-customizable filtering mechanism will involve no more than two non-overlapping rectangles to cover any screenshot involving such a window. It is important to note that for interactive panels that may reside all over a screen, an extension of aspects of the techniques presented herein is possible and such an extension is discussed in the narrative below.

Based on the above interpretation, a two-rectangle filter involves two sets of coordinates for the covering rectangles. There are two different techniques through which such rectangle filters may be used.

A first technique involves non-overlapping rectangles where both rectangles are opaque. In the usual meeting scene, if the three panels mentioned above are represented in a flat, independent manner, it is obvious that two rectangles can offer a completely customizable option for the filters.

A second technique involves fully overlapping rectangles where an inner rectangle is transparent. While the non-overlapping, two opaque rectangle approach is straightforward, such an approach may not cover all possible layouts, particularly those involving an interaction panel that runs all around a presentation window. In such cases, the addition of a simple Boolean variable to each set of coordinates, indicating the transparency of a rectangle, can add enormous value.

Two observations regarding the implementation details of such an approach are important. A first observation emphasizes that an inner, transparent, rectangle allows for the creation of a window that supports, among other things, a video stream alone or the presentation alone (e.g., in the case where it is a fun activity). A second observation emphasizes that an outer, opaque, rectangle allows for the covering of any surrounding or 'fancy' interaction panel implementations without blocking the content that is intended to be shared.

Under aspects of the techniques presented herein, the sequence of steps on an attendee's side (assuming that a host has disallowed screenshots from or the recording of the complete window), may include, for example:

1. A host schedules a meeting, and, possibly among other things, disallows screenshots or screen recordings.
2. When an attendee joins the meeting, the application (on the attendee's side) registers with the OS at the start of the meeting.
3. A screenshot attempt is made by an attendee.
4. The OS sends a notification to the application requesting the set of coordinates (of the two rectangles, along with the transparency Boolean value for each) that are to be blocked.

5. Using the coordinates, the internal screenshot (or recording) application programing interface (API) captures a screenshot (or recording) with the sections of the rectangles represented by the coordinates greyed-out (depending upon the transparency Boolean value).
6. The greyed-out screenshot is then stored in the regular format along the pre-defined path in the OS.

Aspects of the techniques presented herein offer a number of benefits. For example, a first benefit considers that all of the existing protection mechanisms at the attendee's side are highly intrusive. For example, one can either completely disallow all key-based inputs and force the device to stay in full-screen mode or completely allow all such activity.

Additionally, a second benefit considers that the selective protection that is supported by aspects of the techniques presented herein does not affect a user's ability to employ other applications, while at the same time protecting the shared content. Further, a third benefit encompasses the fact that the simple two rectangle approach that is supported under aspects of the techniques presented herein is a lightweight, yet robust, implementation of a privacy or confidentiality filter. Moreover, a fourth benefit considers that a vendor’s implementation of aspects of the techniques presented herein would add to the vendor's story of privacy and trust without completely disrupting a client device's capabilities.

Figure 1, below, presents a sequence diagram that encompasses aspects of the techniques presented herein.

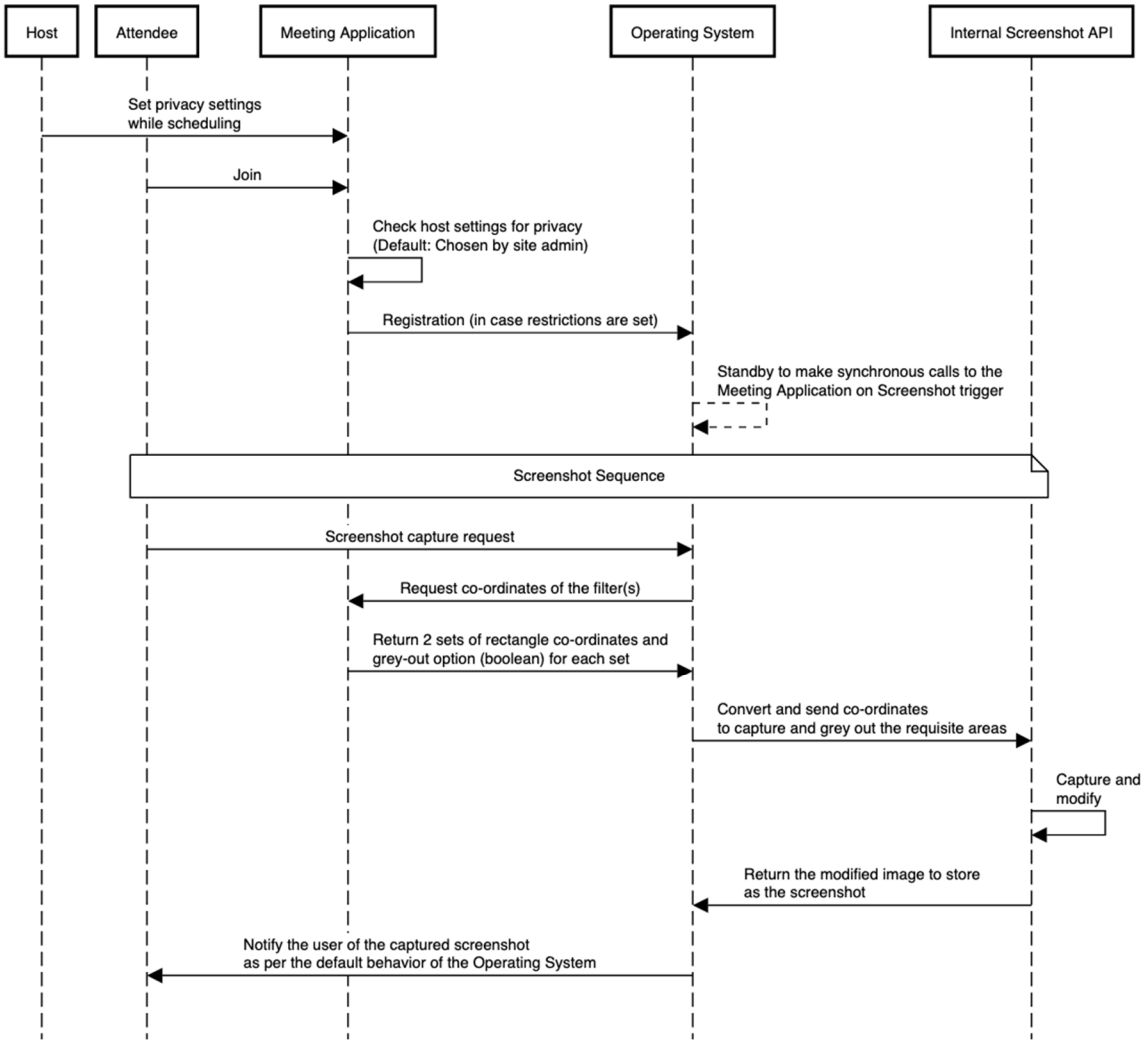

Figure 1: Sequence Diagram for Non-Intrusive Privacy-Enhanced Screenshots

Aspects of the techniques presented herein may be explicated with the aid of four illustrative use cases, will be described and illustrated in the following narrative.

A first illustrative use case encompasses a host that wishes to block only confidential data that is being presented (e.g., screen sharing). This is the most common use case, an example of which could include a discussion of confidential customer data. Figure 2, below, depicts a portion of an unprotected display screen that is to be captured.

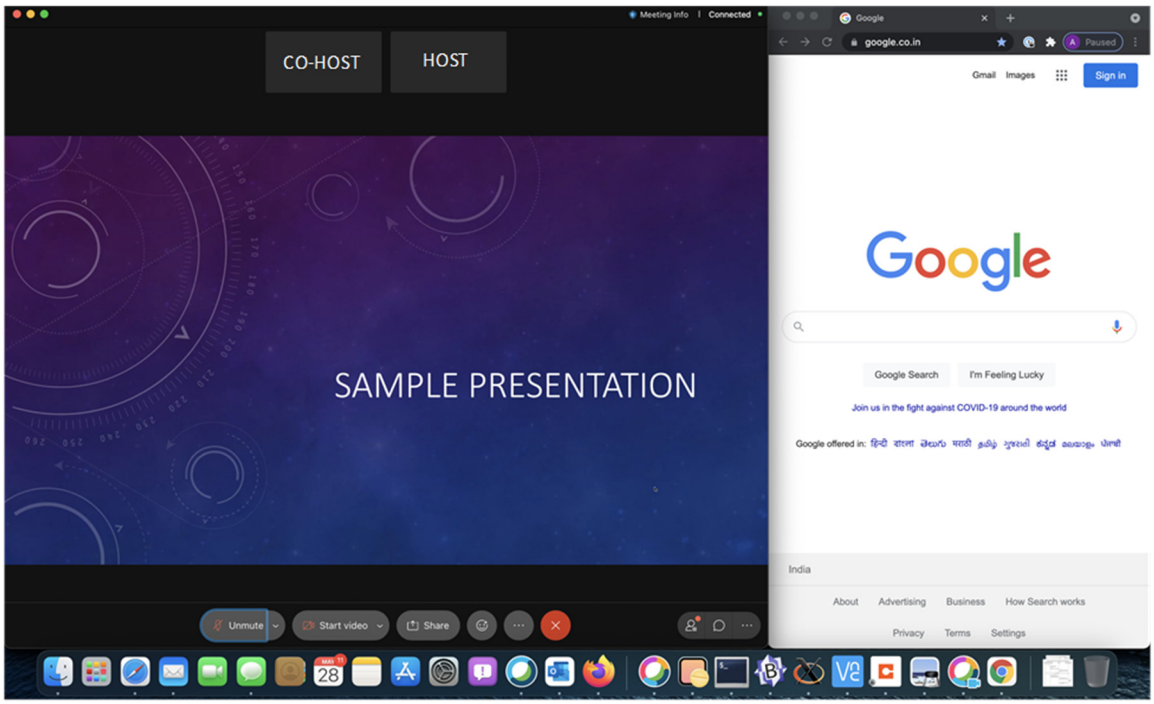

Figure 2: Illustrative Unprotected Display Screen

Figure 3, below, depicts the display screen from Figure 2, above, following the capturing and blocking of confidential data according to aspects of the techniques presented herein.

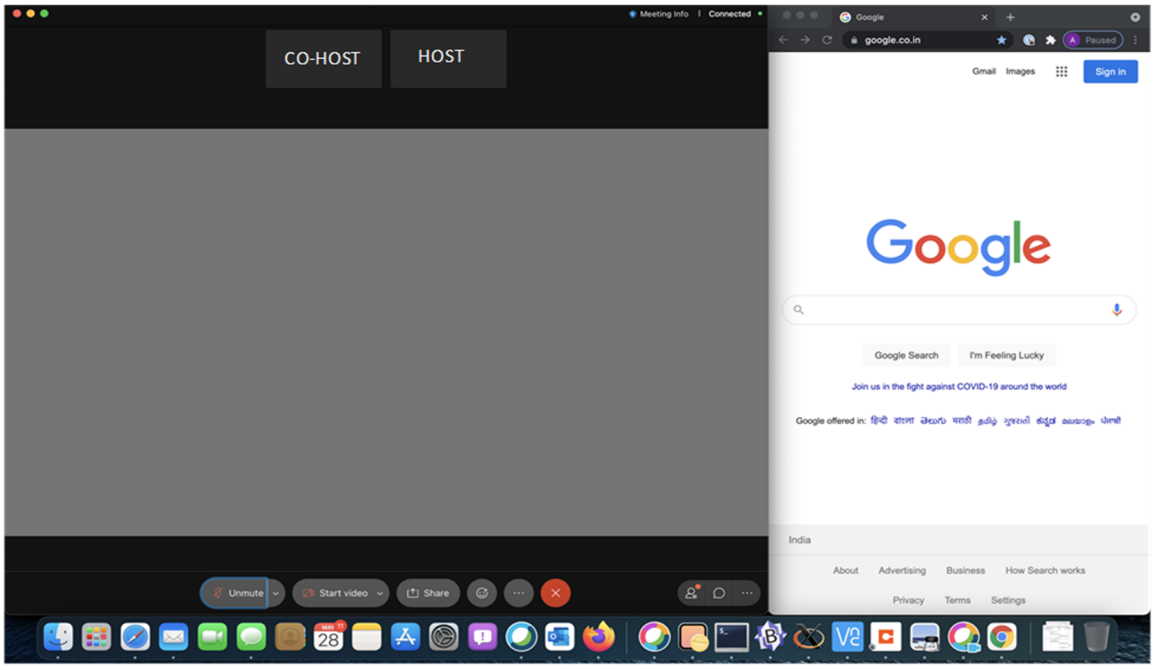

Figure 3: Illustrative Privacy-Enhanced Screen Capture

A second illustrative use case encompasses a host that wishes to block the confidential data that is being presented along with a chat window. An example of such a scenario may include an internal all-hands meeting in which video steams alone are not confidential. Figure 4, below, depicts a portion of an unprotected display screen that is to be captured.

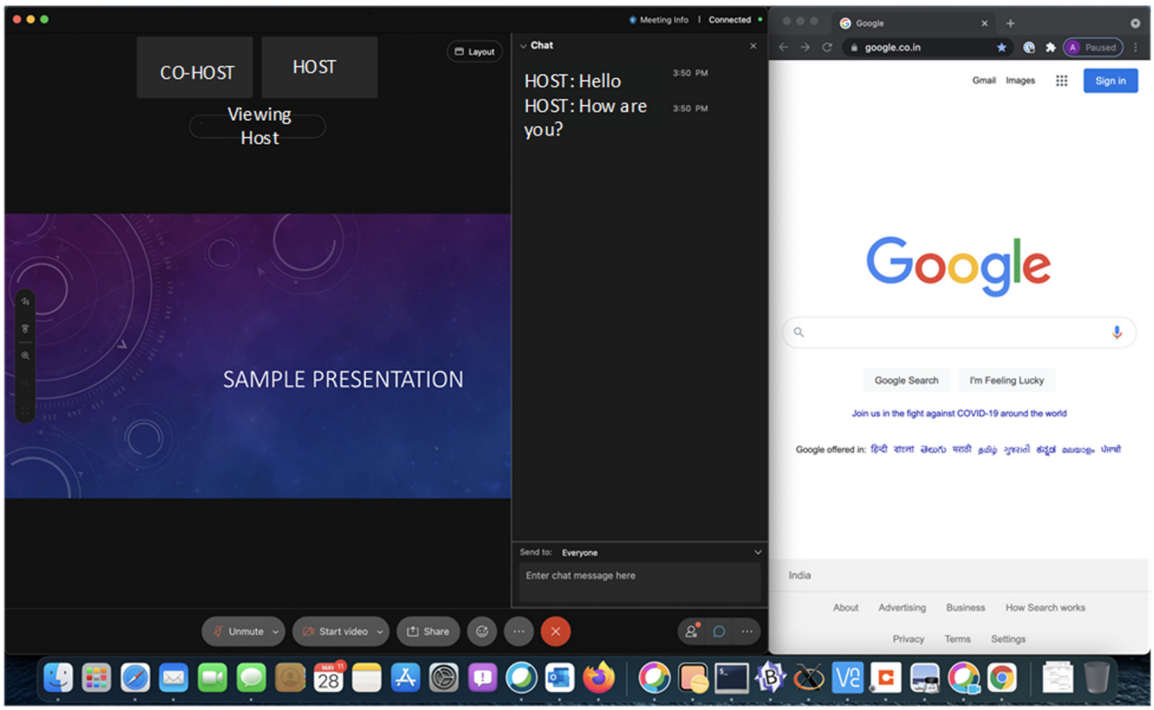

Figure 4: Illustrative Unprotected Display Screen

Figure 5, below, depicts the display screen from Figure 4, above, following the capturing and blocking of confidential data according to other aspects of the techniques presented herein. In particular, Figure 5 illustrates an application of the two non-overlapping rectangle approach for blocking confidential data, as discussed previously.

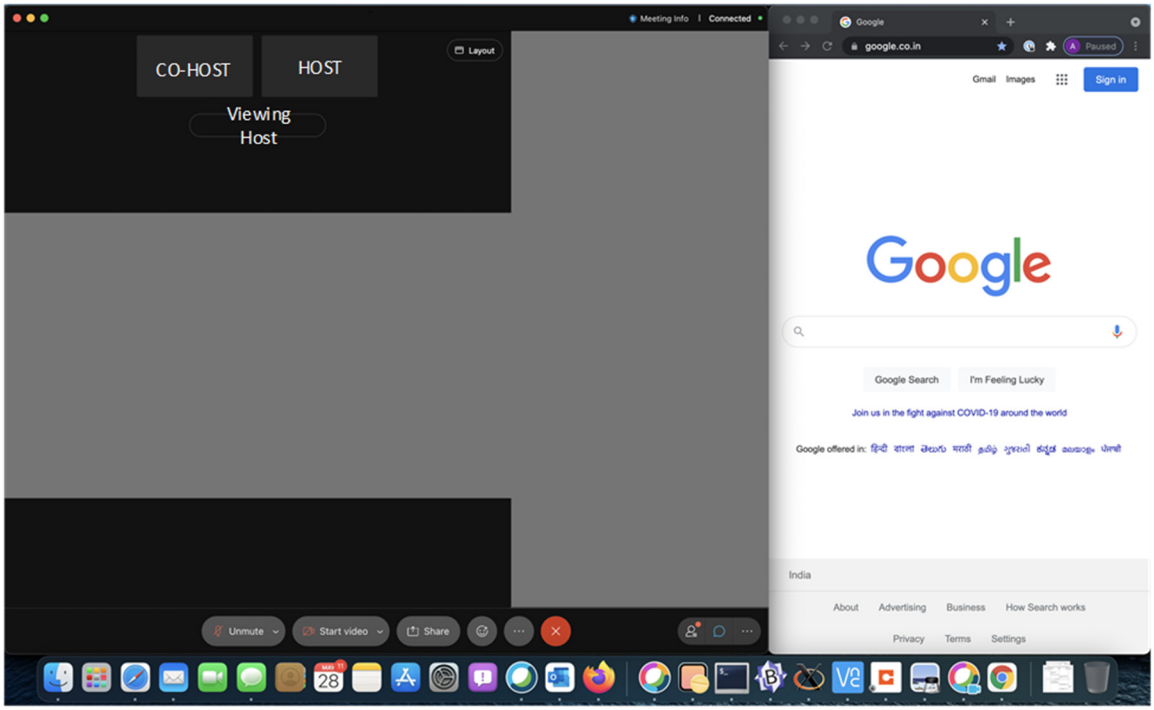

Figure 5: Illustrative Privacy-Enhanced Screen Capture

Figure 6, below, depicts the display screen from Figure 4, above, following the capturing and blocking of confidential data according to further aspects of the techniques presented herein. In particular, Figure 6 illustrates an application of the two overlapping rectangle approach for blocking confidential data involving multiple interaction panels. It is important to note that the visible video stream resides within the transparent inner filter.

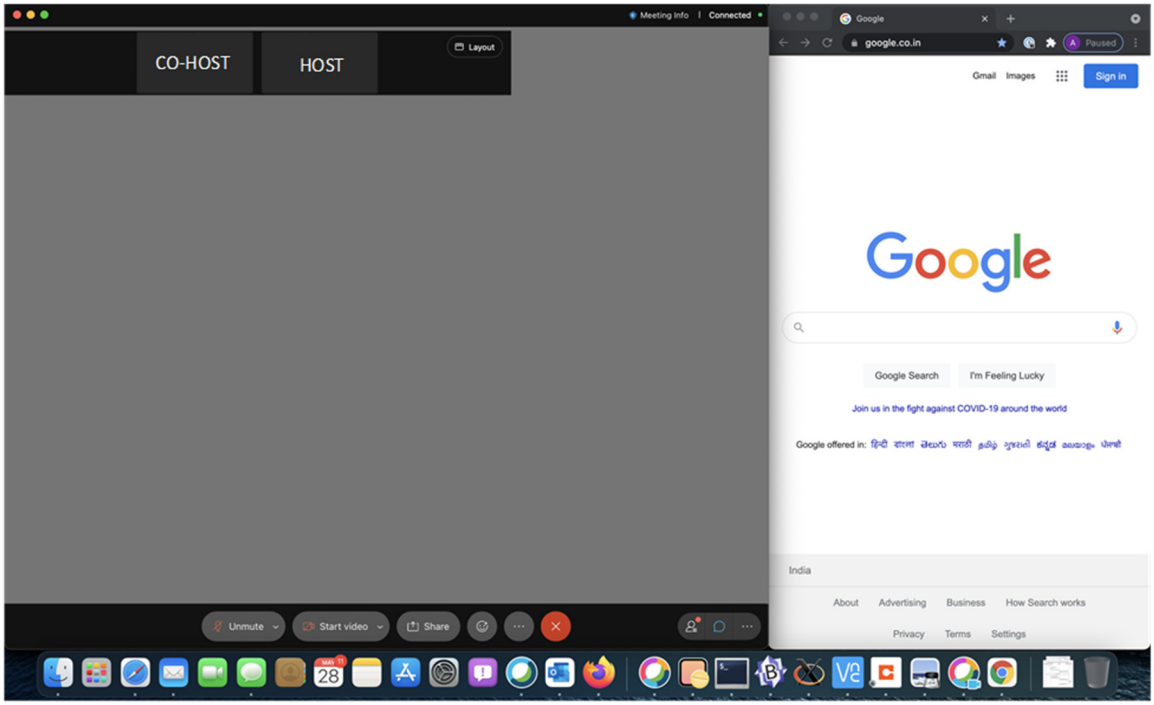

Figure 6: Illustrative Privacy-Enhanced Screen Capture

A third illustrative use case encompasses a host that wishes to block everything on the meeting window. Examples of such a scenario may include highly-confidential design discussions, human resources (HR) meetings, etc. Figure 7, below, depicts a portion of an unprotected display screen which is to be captured.

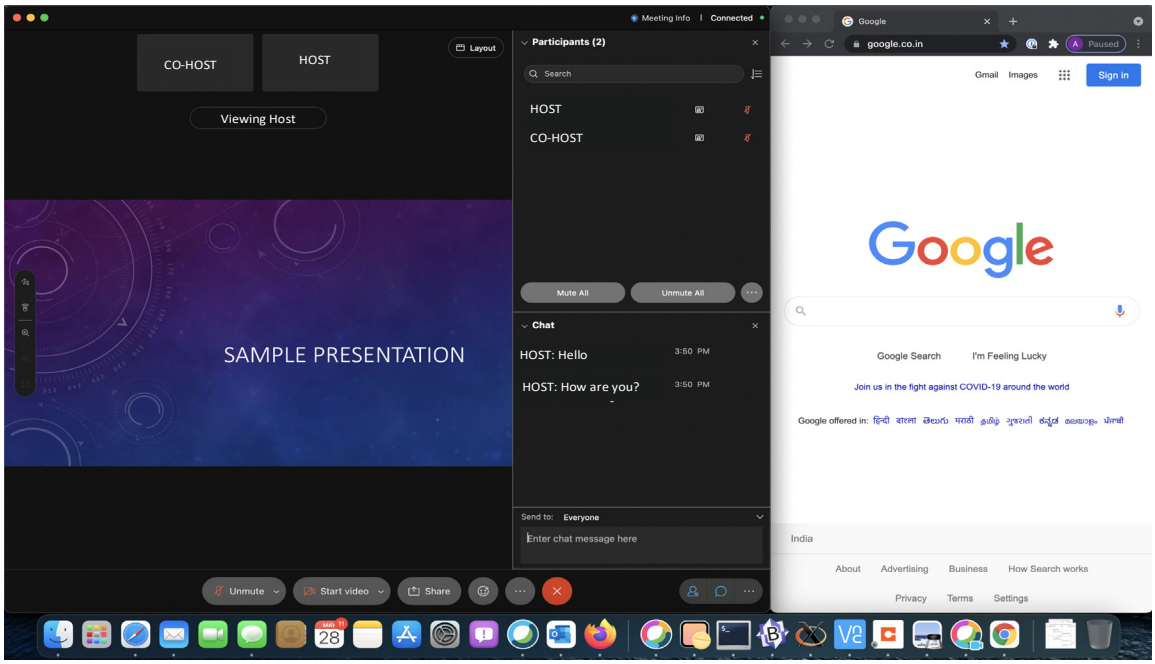

Figure 7: Illustrative Unprotected Display Screen

Figure 8, below, depicts the display screen from Figure 7, above, following the capturing and blocking of confidential data according to additional aspects of the techniques presented herein.

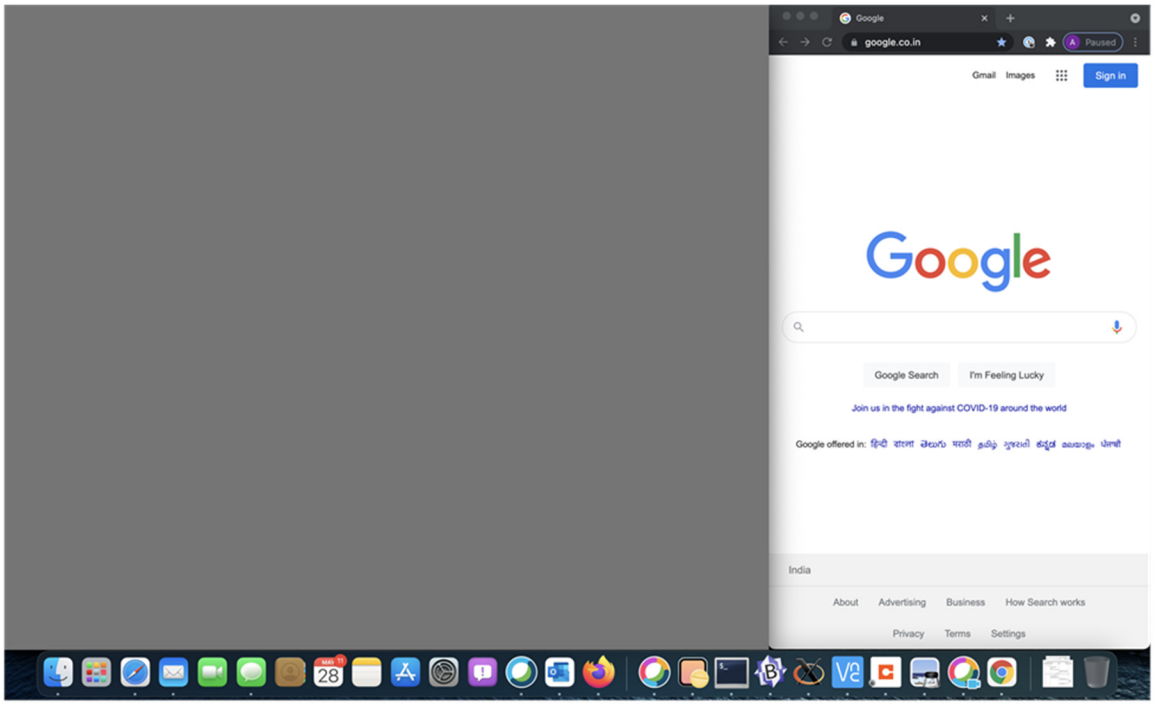

Figure 8: Illustrative Privacy-Enhanced Screen Capture

A fourth illustrative use case encompasses a casual video call where video streams are the only source that needs to be blocked. An example of such a scenario may include casual coffee table discussions. Figure 9, below, depicts a portion of an unprotected display screen which is to be captured.

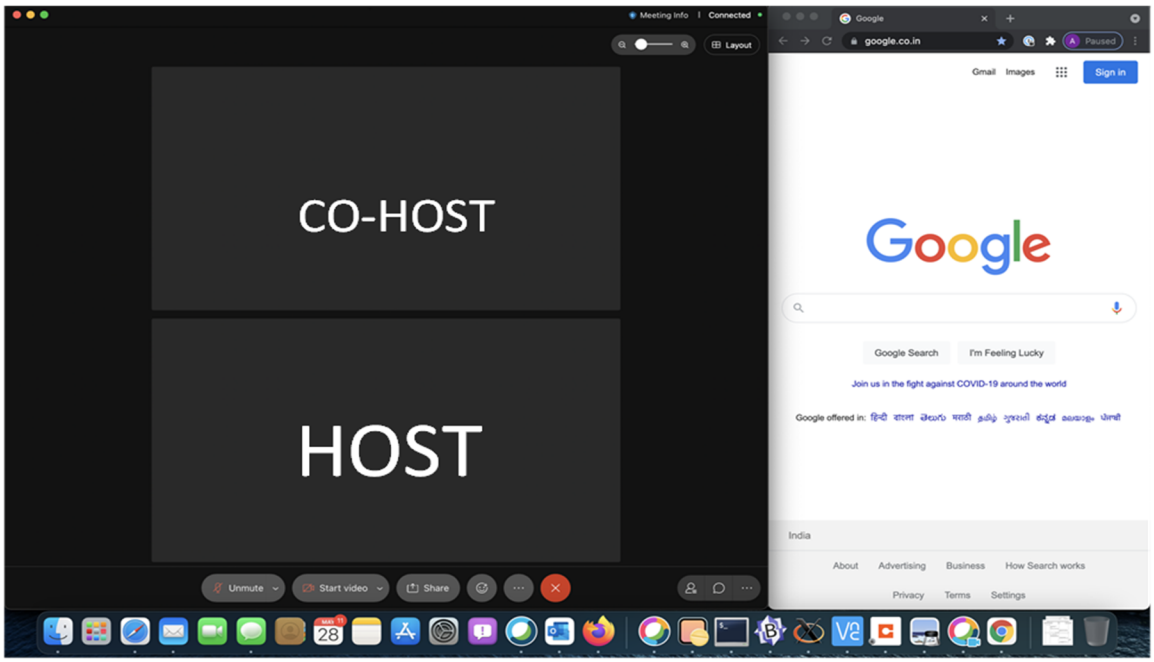

Figure 9: Illustrative Unprotected Display Screen

Figure 10, below, depicts the display screen from Figure 9, above, following the capturing and blocking of confidential data according to further aspects of the techniques presented herein.

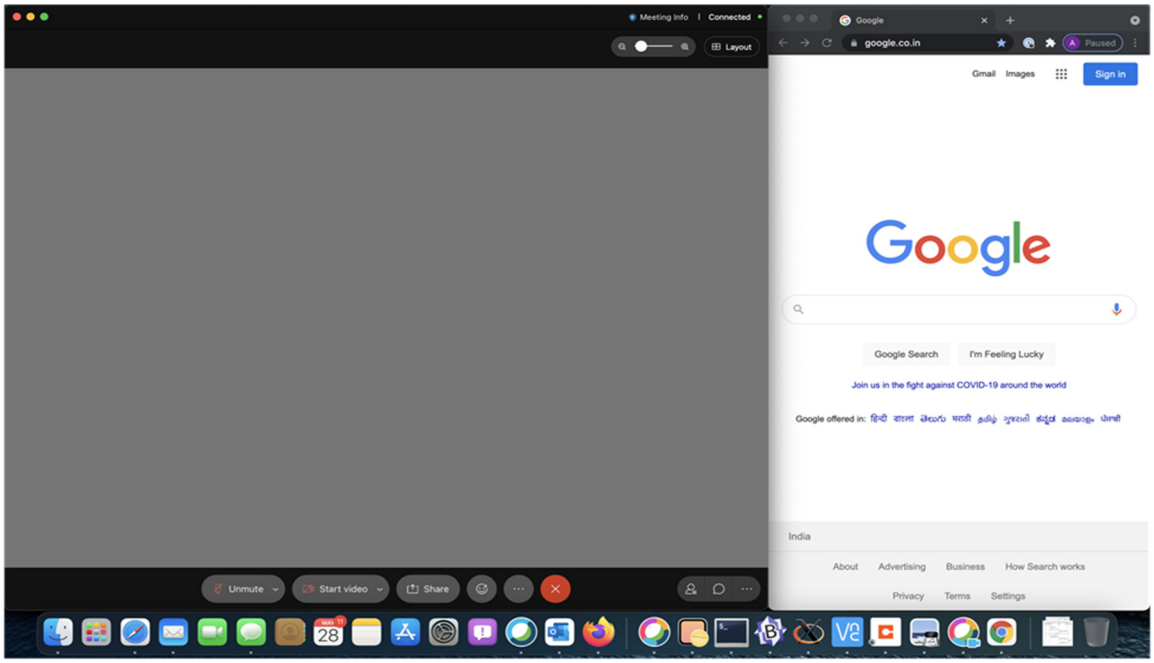

Figure 10: Illustrative Privacy-Enhanced Screen Capture

In summary, techniques have been presented that support selectively blocking only the vulnerable sections of a screen in a non-intrusive way thus ensuring both user convenience and privacy protection, which may provide for enhancing web conferencing privacy protection from an attendee's standpoint. Aspects of the presented techniques employ, among other things, a meeting window interpretation, a two-rectangle filter, and an exchange of rectangle coordinates in support of the non-intrusive greying-out of portions of a screen.