November 22, 2017

Automatic content backup and allocation to native applications

Thomas Escobar

Mark Rivera

Charles Goran

Spencer Syfrig

Automatic content backup and allocation to native applications

ABSTRACT

This disclosure describes techniques to automatically prioritize backup of content on a user device and matching of such content with appropriate software applications. The techniques described enable automatic detection and backup of user generated and other content. With user permission and express consent, new content is detected, classified and matched to a suitable application. Backup of different content is prioritized based on factors such as file size and recency, importance of the file to a user, availability of the file from other sources, and quality of the available network connection.

KEYWORDS

- Cloud backup
- Content synchronization
- Automatic backup
- User generated content
- Online storage

BACKGROUND

Automatic backup of content from a device over a network, e.g., to cloud storage, is a feature provided by modern operating systems and software applications. Users need to be able to find and retrieve the stored content at a later time, with native software (e.g., part of an operating system) or other appropriate software applications. Further, backup of content may be constrained in some instances, e.g., due to low network bandwidth, battery life of user device, etc. In these instances, prioritization of content back is needed.

DESCRIPTION

Techniques described in this disclosure intelligently predict a suitable native application to which stored content is sent to, and prioritize the order in which content is uploaded for storage. Backup of content, e.g., by transmission over a network to online storage, is performed with express user permission and consent. Only such content for which the user has provided permission is backed up. The prediction of native applications and prioritization for backup is performed based on analysis of content upon user permission for such analysis for this purpose.

Various factors including the file type, file details, file content, and available native applications, are analyzed. For example, consider a sound file that is automatically uploaded and stored. Analysis of the sound file is performed to determine e.g., that the file is a music file, an audiobook, or a voicemail recording. The file is automatically provided to a music playback application, a book application, or a native file storage application respectively, based on the analysis.

Fig. 1 illustrates classification (106) of detected content (104) based on attributes (108). The techniques are implemented when users enable automatic detection of user generated and downloaded content for backup. The content is analyzed to determine that it is new and has not previously been uploaded, e.g., to avoid duplicate storage. Upon identification of new content, various analyses are performed:

1. Attributes of the content file, e.g., type (MP3, Document, spreadsheet, etc.), content, and metadata are analyzed. For example, during such initial sorting, the file is classified by matching the file extension with a known database of extensions.
2. With user permission, the file content is compared with known content in a database, e.g., a music or movie database, to determine whether the content matches a known song or movie, etc.

3. File details, including metadata, e.g., creation date, file size, length, author, and other attributes are examined.
4. With user permission, the file contents are analyzed, e.g., using machine learning techniques. The content of the file is analyzed for categorization. For example, with user permission, it may be determined whether an image file includes a person, or a receipt, and the file is classified accordingly.

Based on the analysis, the classified content (210) is matched to an appropriate destination application (212) as illustrated in Fig. 2. The matching is based on file compatibility information. Further, when users provide permission, the application is identified based on previous user behavior, e.g., a user preferred music playback application. User feedback, e.g., acceptance or rejection of automatic content classifications and history of user selection of applications to store or access similar content are used for matching.

After the matching, content is prioritized for backup based on the source of the content and learned user behavior. For example, user generated content is given higher priority over downloaded content. Content that is not known as stored in locations other than a user device is prioritized, e.g., photos captured with the user device. The prioritization criteria can also include recency, file size, and quality of the available network connection.

The described techniques intelligently prioritize the order in which content is uploaded over a network with limited bandwidth or performance. For example, recently captured photos are prioritized over a recently downloaded e-book file. Further, it is ensured that both user generated and other content is appropriately classified and matched to the relevant applications. Although the content classification and matching is typically performed before upload, matching

can also be performed before a user accesses content. This is particularly useful if users download new applications that can access already classified content.

In situations in which certain implementations discussed herein may collect or use personal information about users (e.g., user data, information about a user's social network, user's location and time at the location, user's biometric information, user's activities and demographic information), users are provided with one or more opportunities to control whether information is collected, whether the personal information is stored, whether the personal information is used, and how the information is collected about the user, stored and used. That is, the techniques discussed herein collect, store and/or use user personal information specifically upon receiving explicit authorization from the relevant users to do so.

For example, a user is provided with control over whether programs or features collect user information about that particular user or other users relevant to the program or feature. Each user for which personal information is to be collected is presented with one or more options to allow control over the information collection relevant to that user, to provide permission or authorization as to whether the information is collected and as to which portions of the information are to be collected. For example, users can be provided with one or more such control options over a communication network. 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. As one example, a user's identity may be treated so that no personally identifiable information can be determined. As another example, a user's geographic location may be generalized to a larger region so that the user's particular location cannot be determined.

CONCLUSION

Techniques described enable automatic detection and backup of user generated and other content. With user permission and express consent, new content is detected, classified and matched to a suitable application. Backup of different content is prioritized based on factors such as file size and recency, importance of the file to a user, availability of the file from other sources, and quality of the available network connection.

FIGURES

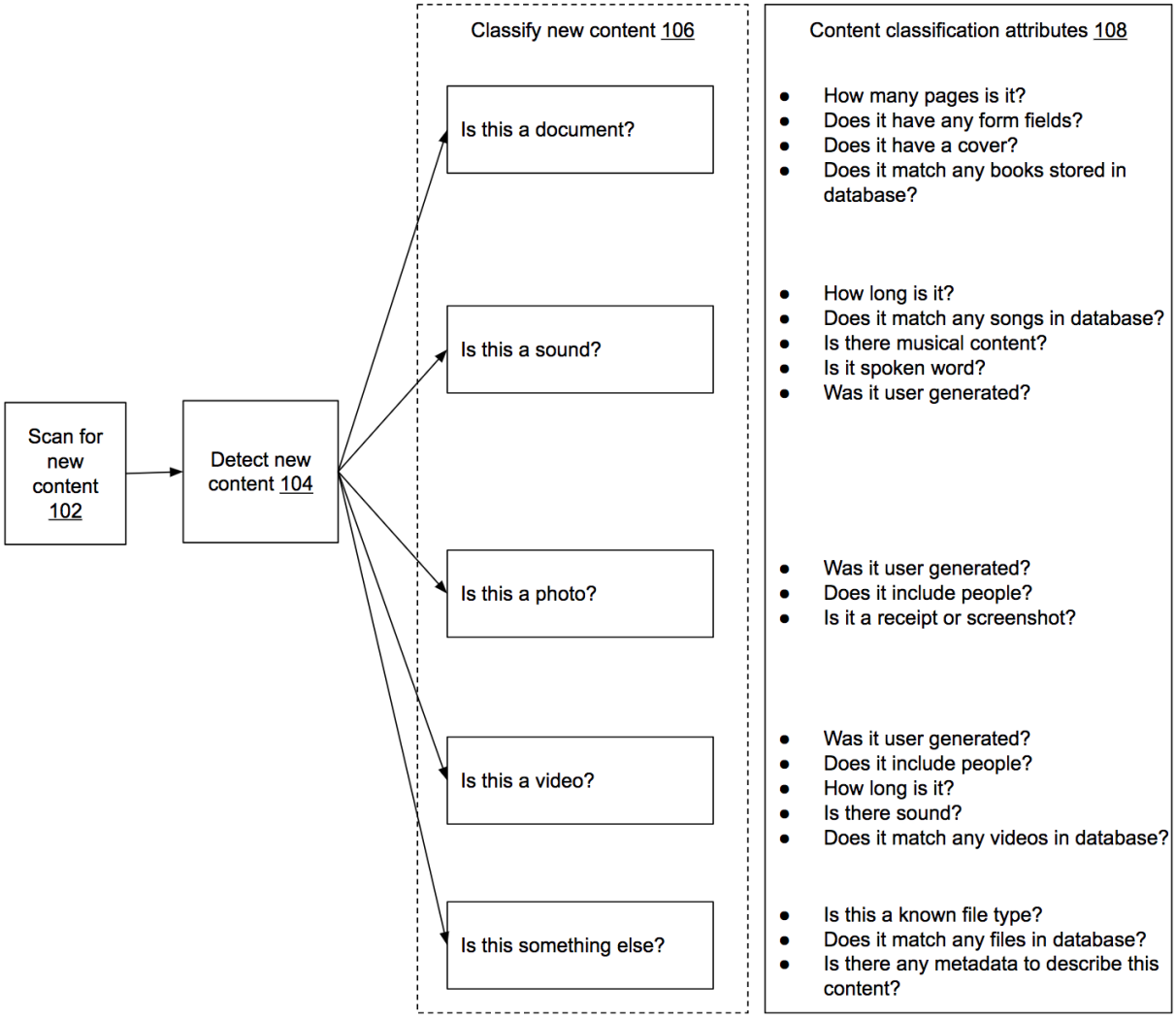

Fig. 1 Classification of content based on attributes

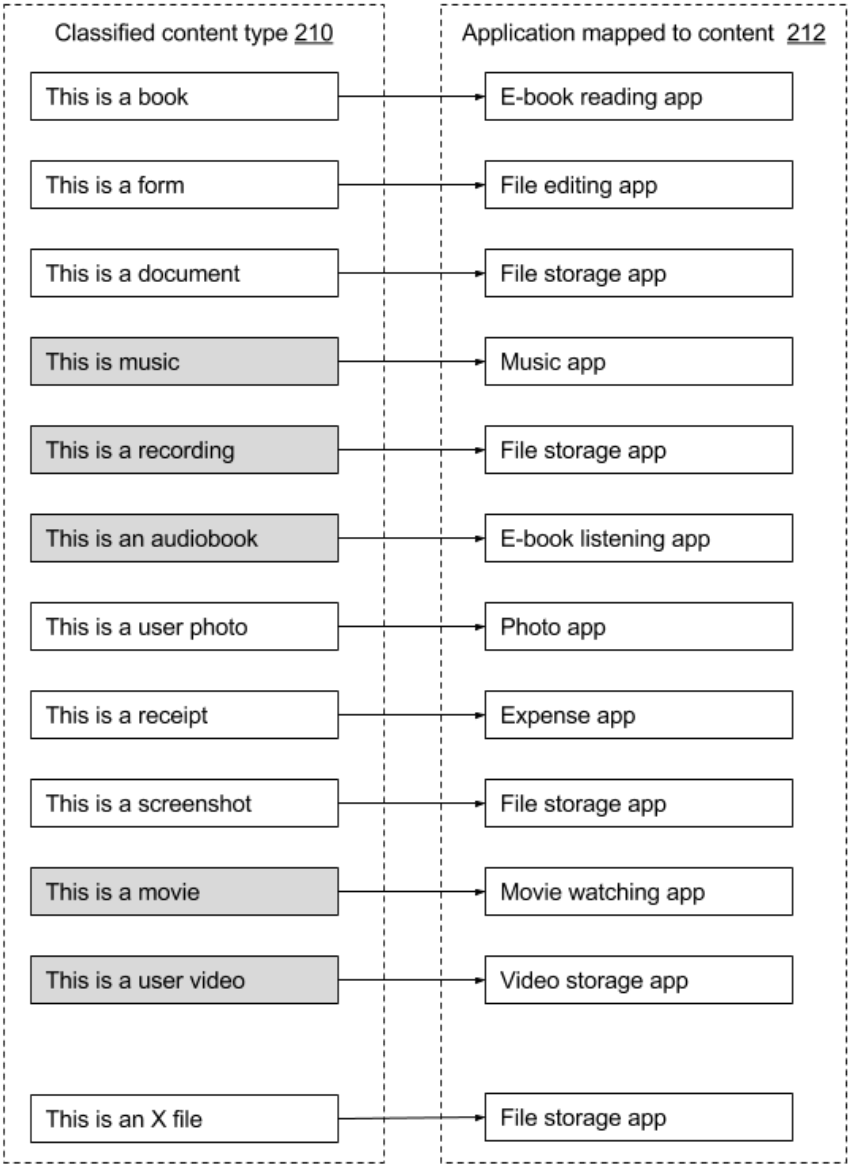

Fig. 2 Mapping of classified content to applications