Technical Disclosure Commons

Defensive Publications Series

August 17, 2017

Automatic correction of timestamp and location information in digital images

Thomas Deselaers

Daniel Keysers

Automatic correction of timestamp and location information in digital images

ABSTRACT

Image storage and sharing services permit users to store and share images. Such applications typically organize images chronologically. However, chronological organization fails if the timestamp or location information stored in the image metadata (e.g., EXIF) is incorrect. Incorrect information is a common problem, e.g., when images are shared via messaging or social media, the shared image may have the time of sharing, not the time of capture. In another example, geolocation data may be deleted when an image is shared. Further, image timestamps can be inaccurate when multiple users contribute images to a single shared album from cameras that are not time synchronized. This disclosure describes techniques to determine the time and/or location of image capture by evaluating the image in the context of other images. Images with trustworthy time information are identified. Images with less trustworthy information are analyzed for content, and a determination is made as to whether they are ahead or behind a trustworthy image. In this manner, techniques of this disclosure enable chronological ordering of images.

KEYWORDS

- Image timestamp
- Image location
- Digital camera
- Metadata correction
- Photo sharing

BACKGROUND

Images uploaded to an online image-sharing service often have timestamps of uncertain accuracy. This inaccuracy in timestamps arises due to several reasons, such as:

- **Unsynchronized cameras**: Multiple users upload to a single image library. There is no guarantee that the different cameras used to capture and upload images have synchronized clocks. This results in images within the library having timestamps that do not reflect their true chronological order.
- **Images with erased or overwritten metadata**: When sharing an image over a messaging or social media applications, the timestamp and geolocation data are sometimes erased or overwritten. For example, a shared image can include the time and date of sharing, not the time and date of capture. Similarly, images that are uploaded or downloaded to/from a server sometimes lose their geolocation data. The erasure of geolocation data amounts to the loss of intrinsically valuable information. However, it also affects the accuracy of the timestamp, as certainty regarding time-zone is lost.
- **Cameras with no geo-tagging or time-zone stamping functionality**: Some cameras do not include global positioning or wireless networking functionality. Images captured with such cameras include a timestamp based on a locally configured time. If the user did not set camera time, the timestamp is based on factory setting. Further, if the user travels across time zones, the camera is unable to detect and adjust for a changed time zone. This results in inaccurate timestamps on captured images.

The lack of accurate timestamps on images is problematic during chronological ordering, since image library applications and storage services use date/time information included within

images, e.g., embedded as EXIF or the timestamp of the image file in the file system for chronological ordering.

DESCRIPTION

Techniques of this disclosure predict time, date and possibly geographical location of digital images based on the context of other images of a user. When a user permits use of images for the purposes of determining time and/or location information, a stream of images, originating possibly from multiple cameras, is taken as input. Certain images from the stream are identified as having trustworthy time information. The remainder of images, with less trustworthy timestamps are arranged in time around the trustworthy images.

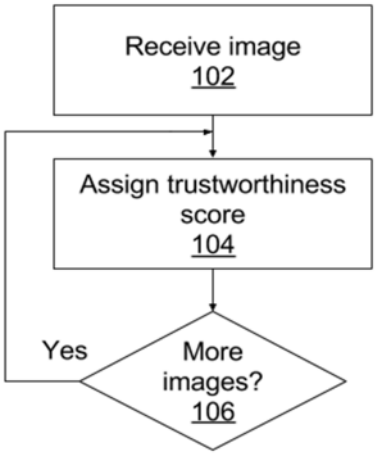

Fig. 1: Obtaining trustworthy images from an album

Fig. 1 illustrates the steps involved in filtering out images with trustworthy timestamps from the set of images in an album. Images with trustworthy timestamps are selected by assigning a trustworthiness score (also referred to as confidence) score to each image. An image is received (102) and a trustworthiness score is assigned to the received image (104). If there are more images (106), the assignment of trustworthiness score is until all images have been assigned a score.

An image is regarded as having a trustworthy timestamp if the image-sharing service can verify that the user's smartphone (or camera) has the correct time set. For example, this can be verified through the metadata of the image that the smartphone has onboard GPS, and that the GPS reported time and location to sufficient accuracy. Further, if the timestamp for a device were found trustworthy for prior images, the timestamp of an image is deemed trustworthy. Additionally, if a user of the device indicates that a particular timestamp for an image, or timestamps for a particular device are trustworthy, such user indications of trustworthiness are used.

If an image scores high on the trustworthiness scale, then the timestamp is taken as a groundtruth timestamp, e.g., it is given an absolute time value. An image with less reliable metadata scores low on the trustworthiness scale. Images that are evaluated for trustworthiness scores can originate from multiple distinct devices. If the user denies permission to access certain images, those images are excluded from the determination of trustworthiness score.

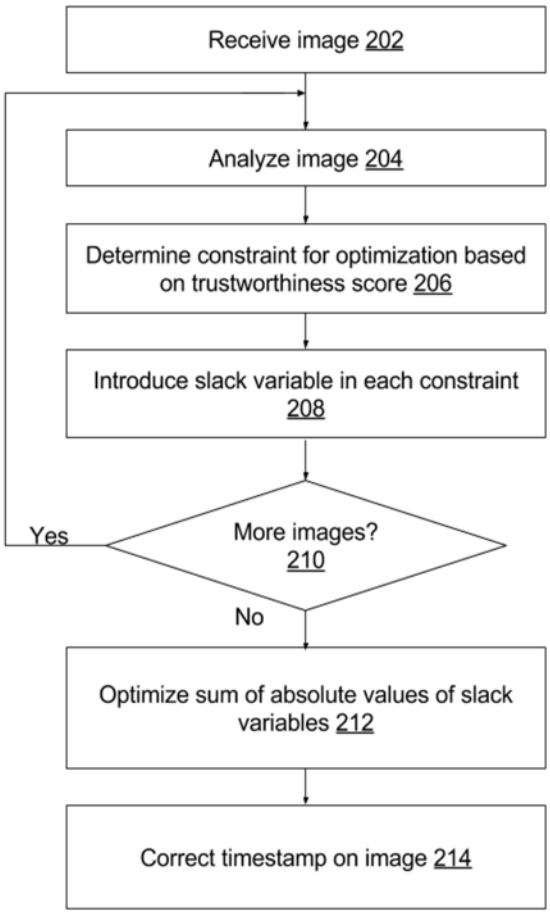

Fig. 2: Correcting timestamps of images

After trustworthiness scores have been assigned for the images, timestamp correction is performed, as illustrated in Fig. 2 and a global chronological order of the images is determined. An image is received (202) and analyzed (204) when users provide consent for such analysis. The analysis is based on the content of the image as well as the metadata of the image, e.g., the device identifier, the camera model, the application used to capture the image, geolocation information, the order of the images taken on each of the devices, the filename of the image (especially if it includes a timestamp or serial number), etc. The content of the image is analyzed to infer time of day, e.g., based on lighting, sunlight, or weather conditions, etc. The content of the image is further analyzed to determine similar images or scenes. For example,

when users permit use of facial recognition techniques, the presence of anonymized faces of the same people in multiple images taken from different devices establishes similarity between the images.

With an assumption that all images, e.g., within an image album, were taken during the same time span, image ordering is determined using the image analysis. For example, images taken during the night are taken after images taken in the dusk; images taken at dusk are taken after images taken in bright sunlight; images taken in bright sunlight are taken after images taken during dawn, etc. The change in appearance of objects in a group of images can also be used to determine an ordering of the images. For example, an image depicting a half-eaten cake is determined as having been taken after images that show a complete cake.

Pairs of images taken at nearly the same moment are identified based on image analysis. For example, at many gatherings, multiple people often take images of the same key event. Each such piece of information about an image leads to a constraint, with a confidence score, on the relative ordering (206). For example, images from trustworthy devices give absolute (groundtruth) time values. As another example, images of the same event lead to a "taken within a short timespan" constraint, where the length of the timespan depends on the type of event, e.g., kissing at a wedding is a few seconds long; pictures of a developing eclipse are spread apart by a few minutes; etc. Images from the same device establish an identical time-shift constraint, e.g., "shift in time on two images from the same device should be the same." The order in which images were taken on a device leads to a constraint of type "image X was taken T seconds before image Y with probability P" for each pair X and Y of images. While the foregoing description refers to different types of image analysis, only such analyses are

performed as permitted by the user. For example, facial recognition techniques are not used if the user has not provided consent for such use.

Mathematically, the problem of ordering is posed as an optimization problem. A slack variable is introduced in each of the constraints (208), thus making each constraint soft. The process of image analysis, setting of constraint, and introduction of slack variable is repeated for each image (210). The sum of the absolute values of the slack variables is minimized (212) while fulfilling all constraints to obtain a correct timestamp for each image (214).

Location information is corrected in a similar manner. For example, if an image is similar in content (same objects, similar lighting, etc.) to and within the same time span of a trustworthy image, then location is established for the less trustworthy image based on the location associated with the trustworthy image.

Techniques of this disclosure can also use publicly available information, e.g. about events, or from other publicly shared pictures.

The user is given a choice for timestamp and location correction, e.g., the correction can be fully automatic for images with high corrected-timestamp confidence, or the user can be prompted for confirmation each time a timestamp is corrected. For example, the image-sharing service may ask of the user: “We believe the following ordering of images is more accurate; do you wish to use the suggested ordering?”

The disclosed techniques can be applied to any type of images, e.g., static images, images with motion (e.g., cinemagraphs, live photos, animations, etc.), video clips, video, 360-degree images, etc.

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 systems and methods 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

Chronological ordering of digital images depends on accurate timestamps on the images. The time of image capture, as marked by the camera, can be inaccurate for a variety of reasons. Techniques of this disclosure correct the timestamps of images by considering each image in the context of a stream of images. Images with trustworthy timestamps are identified. Images with less trustworthy timestamps are arranged around trustworthy images based on an

analysis of the image and of its metadata. The problem of timestamp correction is posed and solved mathematically as a global optimization problem in which information from multiple sources is fused.