Privacy-enabling technologies in video surveillance

Frederic Dufaux

We define a framework that demonstrates how video scrambling techniques can effectively foil facial recognition.

Privacy is a cornerstone of our civilization and is essential for many societal functions. However, this fundamental principle is eroding because of ubiquitous modern information technologies, such as video surveillance. While benefiting society by suppressing crime, widespread use of security cameras has led to well-documented forms of abuse. Moreover, its ‘big brother’ nature is hindering its wider social acceptance. Increasingly powerful analytical tools combined with pervasive networks of high resolution cameras further threaten loss of privacy. New privacy-enabling technologies (PETs) are emerging, which are potentially capable of protecting privacy without hampering video surveillance tasks. However, thorough performance analysis and validation of these technologies is still lacking.

One such video surveillance privacy threat is automatic person identification by facial recognition techniques. Here, we define a framework to assess various PETs in concealing distinguishing facial information and identity.

We used the Face Identification Evaluation System (FIES) to evaluate the performance of facial recognition algorithms applied to images altered by various PETs. The FIES provides standard facial recognition algorithms—including a recognition algorithm based on principal components analysis—and standard statistical methods for assessing performance. It is composed of four main components: image preprocessing, training, testing, and performance analysis (see Figure 1). In

Figure 1. The framework for facial identification and evaluation, which includes facial recognition algorithms based on principal components analysis (PCA).
preprocessing we reduced detrimental variations between images. In the training phase we used a set of images to create the subspace into which test images were subsequently projected and matched. In the testing step, we computed a distance matrix—using the Euclidian distance—in the transformed subspace for all test images. At this stage, two image sets were defined—the gallery (known faces) and probe (faces to be recognized) sets. Finally, we analyzed performance by computing recognition rank to generate a cumulative match curve. A rank 0 is given when the facial recognition algorithm matched the PET-altered image to the correct subject. A rank 1 is defined as when the best match is of another person, but the second best match is of the correct subject. We compared recognition rate for a given rank when evaluating the results.

We assessed two naive PET approaches (pixelization and Gaussian blur) and a more sophisticated region-based transform-domain scrambling method (see Figure 2).\(^7\) Pixelization reduces image resolution by substituting a square block of pixels with its average, where Gaussian blur removes detail by applying a Gaussian low-pass filter. Scrambling inverts the sign of transform coefficients, driven by a pseudo-random number generator. We evaluated the capacity of each PET to foil

*Figure 2. Examples of privacy-enabling technologies. (a) Original image, (b) pixelization, (c) Gaussian blur, and (d) scrambling.*

*Figure 3. Performance comparison of privacy-enabling technologies using cumulative match curve for PCA-based facial recognition algorithms using Euclidian distance.*
facial recognition using the grayscale Facial Recognition Technology database. In our simple attack, training and gallery sets were comprised of unaltered images, whereas the probe set corresponded to images with applied PETs. Figure 3 shows our resultant cumulative match curves. We observed that the recognition rate of original images was greater than 70% at rank 0. After we applied pixelization or Gaussian blur, recognition rate remained high at 56% and 26% success at rank 0, respectively. Finally, scrambling successfully concealed identity, and displayed a recognition rate of nearly 0% at rank 0, and below 10% at rank 50.

In summary, we designed a framework to verify PET effectiveness in concealing identity. We showed that, while naive techniques are ineffective, a more sophisticated scrambling approach successfully concealed identity. Our results challenge the common conjecture that increased security necessarily incurs a loss of privacy. Our future work will concentrate on further analyzing the performance of various PETs. In particular, larger and more realistic data sets will be tested. It is also imperative to better understand user and system requirements regarding privacy issues. Finally, performance analysis should also include the impact on compression efficiency, complexity, and security against attacks.

Author Information

Frederic Dufaux
Telecom ParisTech
French National Center for Scientific Research (CNRS)
Paris, France

Frederic Dufaux is a CNRS Research Director at Telecom ParisTech and editor-in-chief of Signal Processing: Image Communication. He received his PhD in electrical engineering from the Swiss Federal Institute of Technology (EPFL). His research interests include video analysis and coding, visual quality assessment, video surveillance, and privacy protection.

References