CCTV-Exposure: System for measuring user's privacy exposure to CCTV cameras

Hannu Turtiainen[1⋆] , Andrei Costin[1⋆⋆], and Timo Hämäläinen[1]

Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, Jyväskylä, 40014 Finland {turthzu,ancostin,timoh}@jyu.fi https://jyu.fi/it/

Abstract. In this work, we present CCTV-Exposure – the first CCTV-aware solution to evaluate potential privacy exposure to closed-circuit television (CCTV) cameras. The objective was to develop a toolset for quantifying human exposure to CCTV cameras from a privacy perspective. Our novel approach is trajectory analysis of the individuals, coupled with a database of geo-location mapped CCTV cameras annotated with minimal yet sufficient meta-information. For this purpose, CCTV-Exposure model based on a Global Positioning System (GPS) tracking was applied to estimate individual privacy exposure in different scenarios. The current investigation provides an application example and validation of the modeling approach. The methodology and toolset developed and implemented in this work provide time-sequence and location-sequence of the exposure events, thus making possible association of the exposure with the individual activities and cameras, and delivers main statistics on individual's exposure to CCTV cameras with high spatio-temporal resolution.

Keywords: privacy, privacy measurements, privacy-enhancing technologies, PET, video surveillance, CCTV surveillance, CCTV exposure, experimentation, open-source, GPS location track, GPX

1 Introduction

In the modern world, public spaces of many cities are being surveilled by closed-circuit television (CCTV) cameras to a considerable extent. It is estimated that globally there are around 1 billion CCTV cameras in use today [3,5].In the United States, people are likely recorded by a CCTV camera over fifty times per day [11]. In 2019, a person documented 49 CCTV cameras on the way to work in New York City [15] and described it as dystopian.

The discourse on CCTV surveillance has ethical dimensions. Von Hirsch argues that CCTV surveillance is sometimes covert, and often people believe that they are not under CCTV surveillance when they are [9]. Furthermore, according to a 2016 survey, an average citizen of the United States is assumed to be recorded by four or fewer CCTV cameras per day, while the actual figure is

⋆ An extended version of our paper is also available [18].

⋆⋆ Corresponding and original idea author.

likely over ten times larger [11]. Considering the amount of CCTV cameras having been installed globally and the fact that people can be detected and recorded by them, adding face recognition to the pattern opens up an unsettling possibility to also automatically identify people by CCTV cameras [10,20,1]. Moreover, CCTV cameras, Digital Video Recorders (DVRs), and Video Surveillance Systems (VSSs) are notoriously known to be vulnerable to cybersecurity attacks and hacks [6]. Therefore, it is reasonable to assume that the CCTV cameras overlooking public places may be under the control of unauthorized persons hence posing a direct threat to privacy.

In this context, we argue that it is essential to create *CCTV-aware* solutions and technologies that allow people the discretion to be under surveillance or not in public places. We approach the question from the perspective of estimating individual users' exposure to CCTV cameras based on their real-time or historical geo-location (e.g., position, tracks, routes). While there is a substantial amount of studies related to exposure to various "harmful environments" [7,17,2,4,14,8], to the best of our knowledge, none of the existing works focuses on the exposure to privacy invasion by CCTV cameras when this is seen as a "harmful environment" for individual privacy.

Nevertheless, when shared responsibly and for practical purposes, the users' GPS data can also be used for Privacy Enhancing Technologies (PET), as we present in this paper. In this paper, we propose one such *CCTV-aware* solution, namely `CCTV-Exposure`. When compared to exposure to "harmful environments" such as exposure to radiation, the `CCTV-Exposure` system is intended to act like a "CCTV dosage meter" for travel activities of privacy-minded individuals.

Our contributions with this work are:

1. We propose, implement, and demonstrate a system aimed at measuring individuals' privacy exposure to CCTV cameras using analysis of historical and real-time GPS data
2. For evaluation and further improvements, we release (upon peer-review acceptance) the relevant artifacts (e.g., code, data, documentation) as open-source: https://github.com/Fuziih/cctv-exposure

The rest of this paper is organized as follows. We briefly introduce related work in Section 2. We present in Section 3 our algorithms as well as design and implementation details. Then, in Section 4 we introduce results and their evaluation. Finally, we conclude this paper with Section 5.

2 Related Work

To date, to the best of our knowledge, none of the works (systems, implementations, surveys) have addressed the research question related to individuals' privacy exposure to CCTV and video surveillance, as we do in this paper. However, we briefly introduce closely related state-of-the-art and related work in adjacent fields below.

Turtiainen et al. [19] were the first to propose and develop a dedicated computer vision (CV) model – CCTVCV – designed specifically to detect CCTV cameras from street view and other images, with the primary intended purpose of building various privacy-enhancing technologies (PET), tools, and large-scale datasets (e.g., global mapping of CCTV cameras in public spaces). Building on the applicative ideas from Turtiainen et al. [19], Sintonen et al. [16] developed and proposed OSRM-CCTV, which is the first of its kind route planning and management. PET solution offers pro-active route planning optimized for individual privacy and public safety. Subsequently, Lahtinen et al. [12] applied and validated an early prototype of OSRM-CCTV to demonstrate the feasibility of OSRM-CCTV in real cities (e.g., Jyväskylä, Finland), and to study the impact of CCTV cameras on users' route planning when privacy or safety is a crucial factor. Our present work is different yet complementary to these studies [16,12].

Using GPS data to measure human exposure in different cases is nothing new to the general research field. Dias and Tchepel [7] used GPS data collected from test subjects' mobile phones to measure the users' exposure to air pollution. Their study was conducted in the Leiria area in Portugal, and their pollution data were estimated via Transport Emission Model for Line Sources (TREM) model and meteorological data. Dias and Tchepel claim that due to pollution concentration variation within "microenvironments", their exposure model will yield a meaningfully better understanding of individual's pollution exposure in urban areas in contrast to traditional background pollution measurements. Correspondingly, Tchepel et al. [17] measured human exposure to benzene in the Leiria area in Portugal. Several other studies (such as [2,4,14]) have also measured exposure to air pollutants using GPS data. Global positioning system data are also valuable for creating large datasets of human mobility data. These datasets can be used in conjunction with machine learning and artificial intelligence technologies, for example, to predict crowd flows. Luca et al. [13] surveyed on that subject. However, they concluded that at the time of publishing in December 2020, state-of-the-art models for predicting human mobility suffer from several limitations, for example, data privacy concerns and the geographical constraints for the trained models.

Global positioning system devices and data sending units are also used in tracking wildlife. Hinton et al. [8] measured Cesium-137 exposure on wildlife in the Chornobyl exclusion zone in Ukraine from November 2014 to May 2015. They attached a GPS monitoring unit and a dosimeter to eight free-ranging wolves in the area for data gathering. The gathered dosage data was used to analyze the soil Cesium-137 levels in relation to the temporal and spatial data collected from the GPS units.

3 Design and Implementation

Our `CCTV-Exposure` system is written in Python3 with minimal requirements, as only GPXpy [1] and NumPy [2] are used to reduce any code and dependency overhead. We also implemented the module in Rust (v. 1.60). The Rust implementation is similar and equivalent to our Python3 counterpart; however, it does not allow the use of non-timestamped GPX files due to parser limitations.

At present, and for this paper's evaluation, our system accepts only GPX files as input. However, an application programming interface (API) input is an option that we leave to be implemented in future work. A required argument for the module is the camera database file. For our testing, we used the camera coverage radius and the field-of-view specified in the camera database file; however, these values can be overridden with input arguments by the user.

We decided to use Euclidean distance to perform faster computations instead of the more accurate Haversine distance. However, the module allows option specification to easily switch between Euclidian and Haversine distances and add alternative distance measurement implementations. The core module performs all calculations in meters (for distance) and seconds (for time). For this reason, we ignore the curvature of the earth to quicken the calculations, as well as simplify the model. Our synthetic tests show that for GPX tracks of several kilometers, the cumulative error is negligible when assuming realistic (e.g., hundreds of meters to several kilometers) human geo-location tracks within CCTV-fitted public spaces.

The gist of the module is to loop over all tracks and segments read from the GPX input file. It is important to note that the input GPX file can (and should) be wholly anonymized and scrubbed of any Personally-Identifiable Information (PII), as `CCTV-Exposure` aims to enhance and preserve privacy as one of its core principles. A GPX file can have multiple tracks, which can have multiple segments, and each segment is specified in the GPX file via a set of points (i.e., exact GPS locations, with optional timestamp). We refer to these points throughout the rest of this paper as *GPX points*. The core module loops over each GPX point and identifies "in-range cameras" for each iterated point. An "in-range camera" for a GPX point means a CCTV camera (from the available and loaded database of geo-location mapped CCTV cameras) whose field-of-view (whether directed or 360) covers or intersects with the GPX point. Afterward, the module:

- loops all GPX points which we concluded above to be "within the visual reach" of their "in-range cameras."
- splits the distance between the point and their adjacent point for more granular inspection and calculation (see Section 3.1)

For output interoperability, we use JavaScript Object Notation (JSON) formatted output. We provide distance and time exposure metrics as well as per camera information to the user.

[1] https://pypi.org/project/GPXpy/, https://github.com/tkrajina/GPXpy
[2] https://numpy.org/

For this proof-of-concept module, we loaded our database of geo-location mapped CCTV cameras from a comma-separated values (CSV) file and then looped over all of them for each point.

3.1 Interpolated points - points between GPX points

To increase the accuracy of our calculations, for each GPX point that a camera is in range of, we split the distance to *interpolated points*. *Interpolated points* are not present in GPX data and are a result of our internal calculations to increase both the granularity of analysis and accuracy of the exposure estimate. A variable splits the distance we call *resolution*. The default resolution for our experiments was 0.5 meters; however, the resolution can configure into the system for lower or higher granularity and accuracy purposes. This value is a critical parameter to adjust due to the inherent uncertainty of the GPS data and the variability of data accuracy (GPS drift). The interpolated points are illustrated in Figure 1a. We go through the GPX points with cameras and calculate how far back from the present GPX point the field-of-view of the camera in question reaches (i.e., how many interpolated points). From the answer, we can accurately (within resolution) calculate the distance and time spent in the field-of-view of the individual camera.

After the backward iteration, we loop the GPX points again but focus on going forward from the GPX points, where each camera stops in range. This way, we cover the whole union of camera field-of-view and the route in the process. Figure 1c stages the idea behind the back-and-forth coverage system. Also in Figure 1b, calculated interpolated points are demonstrated. In the example, both blue GPX points are in the red camera's range; therefore, there's no need for granular calculation between the points.

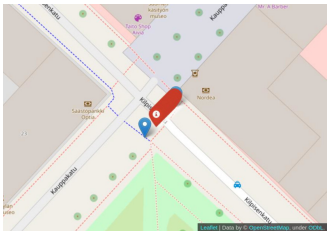
4 Evaluation and Results

The Jyväskylä city area in Central Finland was chosen as the experiment location for this study. As of writing, it is the seventh-largest city in Finland by population. The immediate city center area is relatively compact and rather CCTV congested. The camera mapping was conducted in the summer of 2020 [12,16], and the routes for this study were captured in early 2022.

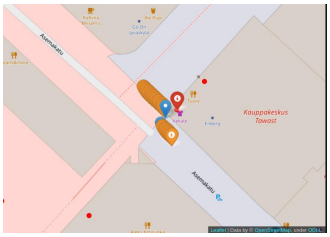
4.1 Evaluation Methodology

We tested four tool-generated 'synthetic' GPX files, and four Garmin recorded 'real-world scenario' files as routes for evaluation of `CCTV-Exposure`. Map examples of the routes are depicted in Figure 3. The 'synthetic' GPX files were created using GPSVisualizer [3], and timestamps were added to them using GoToes GPX editing tool [4]. Our Garmin EDGE 810 recorded the files in Garmin's

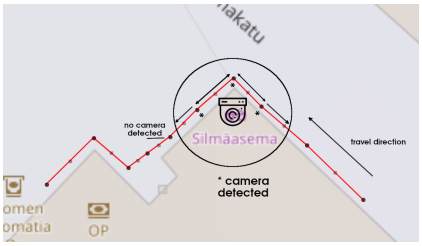
[3] https://www.gpsvisualizer.com
[4] https://gotoes.org



(a) `CCTV-Exposure` interpolated point system: blue markers are GPX points and red markers are interpolated points between them.



(b) `CCTV-Exposure` interpolated points measured: interpolated points in yellow, camera in red, GPX points in blue.



(c) `CCTV-Exposure` granular calculation

Fig. 1: Interpolated point depiction.

FIT format, which were subsequently converted into GPX using a converter from AllTrails [5]. The real-world scenario files provide a bit more exciting data as the timestamps are more varied due to changes in the recorded speed of the person; therefore, the exposure time and distance will yield differing results. However, the Garmin device used in this test had some accuracy issues during recording.

Certain Assumptions and Limitations In our current test setup, we were limited by our camera dataset containing only 450 cameras [12] around the city center of Jyväskylä (Finland). However, there is an active work-in-progress to expand this dataset rapidly in various parts of the world.

For our testing, for all the cameras in our database, we set by default ten (10) meters for the camera "privacy invasion" radius, i.e., the radius on which we assume any CCTV camera in the database can successfully record hard- and soft-biometrics of an individual with subsequent potential recognition or identification. This radius setting is highly conservative and emulates the "worst-case scenario" (i.e., limited visibility range from a CCTV camera perspective).

Moreover, our CCTV camera dataset (and any other public dataset we have seen) has limitations as these datasets do not have 100% accurate characteristics

[5] https://www.alltrails.com/converter

of each camera in the dataset. One core reason for this is that we can detect the presence of the camera (e.g., using CCTVCV [19] or crowdsourcing); however, we (and any similar third-party project) will not know certain information about each camera, such as:

1. exact camera model – this would also be challenging to perform visually by humans (due to low resolution and lack of markings) and via computer vision (as this would require the equivalent of "face recognition" accuracy and system, but for CCTV cameras).
2. exact owner/operator of the camera(s) – these contacts are generally missing but could (or perhaps **should**, as required by GDPR?) provide much more meta-information about the camera; we have a work-in-progress towards achieving this meta-information collection via crowdsourcing; however, we leave this challenge as future work.

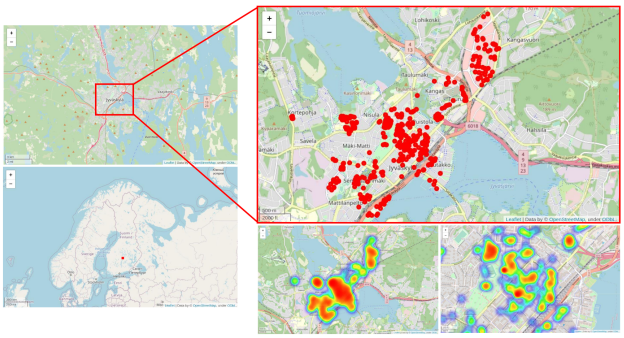


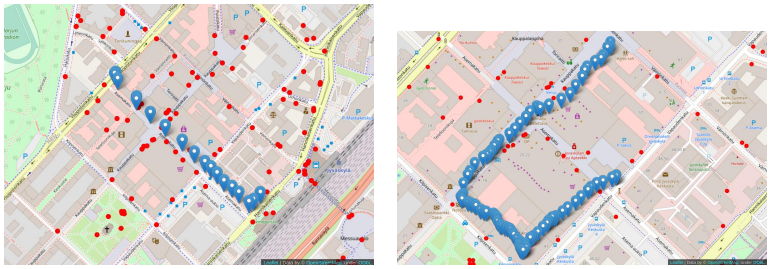
Fig. 2: CCTV cameras dataset mapped in the city of Jyväskylä [12], and used for evaluation of `CCTV-Exposure`.

4.2 Exposure results

In Table 1, we disclose the exposure metrics for the test routes. Our synthetic routes' average CCTV exposure distance and time were 3.7% of the total routes. Our real-world routes (captured by the authors with Garmin devices in the city center of Jyväskylä) indicated an average CCTV exposure of 12.5% relative to segments' distance, and 15.1% close to segments' time, respectively.

Our synthetic routes had a more sparse point distribution, thus resulting in lesser exposure metrics. Our real-world recordings, however, produced more accurate data.

Based on these results, and especially on the real-world recorded routes, it is pretty safe to say that avoiding CCTV cameras around the city center of



(a) Example of a synthetic route traveling through the narrow side of the city.

(b) Example of a recorded route in the city center.

Fig. 3: Example routes used in evaluation of `CCTV-Exposure`.

Route	**Distance – m**	**Unique cams – num**	**Exposure dist. – %**	**Exposure time – %**
syn1.gpx	1538	2	2.6% (41m / 1538m)	2.6% (0:00:29 / 0:18:29)
syn2.gpx	497	1	3.7% (18m / 497m)	3.7% (0:00:20 / 0:09:15)
syn3.gpx	571	1	3.5% (20m / 571m)	3.5% (0:00:14 / 0:06:50)
syn4.gpx	897	3	4.8% (43m / 897m)	4.8% (0:00:32 / 0:11:08)
real1.gpx	633	13	25.4% (161m / 633m)	36.0% (0:02:55 / 0:08:05)
real2.gpx	614	14	17.4% (107m / 614m)	17.4% (0:01:16 / 0:07:15)
real3.gpx	597	9	4.7% (28m / 597m)	4.5% (0:00:18 / 0:06:41)
real4.gpx	775	1	2.3% (18m / 775m)	2.6% (0:00:15 / 0:09:17)

Table 1: Exposure results for the routes used during preliminary evaluation.

Jyväskylä (Finland) proves to be a challenge. These observations are in line with the conclusions from Lahtinen et al. [12], where the authors implemented and studied CCTV-aware route-planning for "preventive privacy analysis".

It is important to note, however, that due to the systematic lack of previous works, ground truth datasets, and baseline recommended exposure levels related to "CCTV privacy invasion", the evaluation numbers should be interpreted with care because they represent a best-effort estimate of the privacy exposure to the CCTV cameras based on the limited CCTV camera datasets and the error-prone GPS tracks.

5 Conclusion

In this paper, we presented `CCTV-Exposure` – an open-source system for measuring users' privacy exposure to mapped CCTV cameras based on geo-location, GPX, and historic tracks. We evaluated the `CCTV-Exposure` on multiple GPS tracks in Jyväskylä, where we also had a comprehensive CCTV camera mapping database of 450 cameras. Our evaluations demonstrate the effectiveness, performance, and practicality of `CCTV-Exposure` when tasked with measuring CCTV

exposure of users based on their real-time or historical geo-location and GPS tracks.

As this is some early yet promising implementation and evaluation, certain limitations and challenges have been identified. They present a fertile ground for further research that we leave as future work. First, performance optimization and accuracy validation of `CCTV-Exposure` will benefit from collecting more extensive and more complete CCTV databases while being validated on larger and more diverse datasets. Second, `CCTV-Exposure` will benefit from being validated with larger and more diverse user-base and stakeholders' scenarios. Third, `CCTV-Exposure`, as well as OSRM-CCTV, would both benefit from a holistic integration into an end-to-end CCTV-aware system.

For evaluation and further improvements, as well as to encourage researchers and practitioners to explore this digital privacy-related field, we release (upon peer-review acceptance) the relevant artifacts (e.g., code, data, documentation) as open-source: https://github.com/Fuziih/cctv-exposure

Acknowledgement

Part of this research was supported by a grant from the *Decision of the Research Dean on research funding within the Faculty (17.06.2020)* of the Faculty of Information Technology of the University of Jyväskylä (The authors thank Dr. Andrei Costin for facilitating and managing the grant). Hannu Turtiainen also thanks the Finnish Cultural Foundation / Suomen Kulttuurirahasto (https://skr.fi/en) for supporting his Ph.D. dissertation work and research (under grant decision no. 00221059) and the Faculty of Information Technology of the University of Jyvaskyla (JYU), in particular, Prof. Timo Hämäläinen, for partly supporting and supervising his Ph.D. work at JYU in 2021–2022. Map images in Figures 1a, 1b, 2, and 1 are generated with Folium (for Python) library (https://python-visualization.github.io/folium/) using OpenStreetMap data (https://www.openstreetmap.org). Map image in Figure 1c is generated in GPSVisualizer.com (https://www.gpsvisualizer.com) also using OpenStreetMap data.

References

1. Axis: Identification and recognition. https://www.axis.com/files/feature_articles/ar_id_and_recognition_53836_en_1309_lo.pdf
2. Beekhuizen, J., Kromhout, H., Huss, A., Vermeulen, R.: Performance of gps-devices for environmental exposure assessment. Journal of exposure science & environmental epidemiology 23(5), 498–505 (2013)
3. Bischoff, P.: Surveillance Camera Statistics: Which City has the Most CCTV Cameras? https://www.comparitech.com/blog/vpn-privacy/the-worlds-most-surveilled-cities/ (May 2021)
4. Breen, M.S., Long, T.C., Schultz, B.D., Crooks, J., Breen, M., Langstaff, J.E., Isaacs, K.K., Tan, Y.M., Williams, R.W., Cao, Y., et al.: Gps-based microenvironment tracker (microtrac) model to estimate time–location of individuals for air

pollution exposure assessments: Model evaluation in central north carolina. Journal of exposure science & environmental epidemiology 24(4), 412–420 (2014)
5. Cosgrove, E.: One billion surveillance cameras will be watching around the world in 2021. https://cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html
6. Costin, A.: Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In: 6th International Workshop on Trustworthy Embedded Devices (TrustED) (2016)
7. Dias, D., Tchepel, O.: Modelling of human exposure to air pollution in the urban environment: a gps-based approach. Environmental Science and Pollution Research 21(5), 3558–3571 (2014)
8. Hinton, T.G., Byrne, M.E., Webster, S.C., Love, C.N., Broggio, D., Trompier, F., Shamovich, D., Horloogin, S., Lance, S.L., Brown, J., et al.: Gps-coupled contaminant monitors on free-ranging chernobyl wolves challenge a fundamental assumption in exposure assessments. Environment international 133, 105152 (2019)
9. von Hirsch, A.: The ethics of public television surveillance. Ethical and Social Perspectives on Situational Crime Prevention. Hart Publishing (2000)
10. Hu, W., Tan, T., Wang, L., Maybank, S.: A survey on visual surveillance of object motion and behaviors. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 34(3), 334–352 (2004)
11. Karas, B.: Americans Vastly Underestimate Being Recorded on CCTV. https://ipvm.com/reports/america-cctv-recording
12. Lahtinen, T., Sintonen, L., Turtiainen, H., Costin, A.: Towards CCTV-aware Routing and Navigation for Privacy, Anonymity, and Safety-Feasibility Study in Jyväskylä. In: 28th Conference of Open Innovations Association (FRUCT). pp. 252–263. IEEE (2021)
13. Luca, M., Barlacchi, G., Lepri, B., Pappalardo, L.: Deep learning for human mobility: a survey on data and models. arXiv preprint arXiv:2012.02825 (2020)
14. Ma, J., Tao, Y., Kwan, M.P., Chai, Y.: Assessing mobility-based real-time air pollution exposure in space and time using smart sensors and gps trajectories in beijing. Annals of the American Association of Geographers 110(2), 434–448 (2020)
15. Pasley, J.: I documented every surveillance camera on my way to work in New York City, and it revealed a dystopian reality. https://www.businessinsider.com/how-many-security-cameras-in-new-york-city-2019-12 (Dec 2019)
16. Sintonen, L., Turtiainen, H., Costin, A., Hamalainen, T., Lahtinen, T.: OSRM-CCTV: Open-source CCTV-aware routing and navigation system for privacy, anonymity and safety (Preprint). arXiv preprint arXiv:2108.09369 (2021)
17. Tchepel, O., Dias, D., Costa, C., Santos, B.F., Teixeira, J.P.: Modeling of human exposure to benzene in urban environments. Journal of Toxicology and Environmental Health, Part A 77(14-16), 777–795 (2014)
18. Turtiainen, H., Costin, A., Hamalainen, T.: CCTV-Exposure: An open-source system for measuring user's privacy exposure to mapped CCTV cameras based on geo-location (Extended Version). arXiv preprint arXiv: (2022)
19. Turtiainen, H., Costin, A., Lahtinen, T., Sintonen, L., Hamalainen, T.: Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision. Applications and implications for privacy, safety, and cybersecurity.(Preprint). arXiv preprint arXiv:2006.03870 (2020)
20. Wheeler, F.W., Weiss, R.L., Tu, P.H.: Face recognition at a distance system for surveillance applications. In: Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE (2010)