Summary of applied biometrics TG activities: October 2015 to August 2016

ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure

Dr Peter Waggett
IBM, United Kingdom

2016

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Joint
Research
Centre

Summary of applied biometrics TG activities: October 2015 to August 2016

This publication is a technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

JRC103172

ISBN 978-92-79-62218-2

doi:10.2788/909340

.

Contents

Acknowledgements

The author gratefully acknowledges the contributions and reviews of the other members of the ERNCIP Thematic Group: Applied Biometrics for Security of Critical Infrastructure and the ERNCIP Office.

Abstract

This report has been generated by the ERNCIP Thematic Group: Applied Biometrics for Security of Critical Infrastructure.

Biometrics allows for the automated identification of individuals based on their biological and behavioural characteristics and provides the promise of the unique identification or classification of individuals interacting with critical infrastructures. The thematic group was established to provide a forum for experts to drive the direction of standards development and generate advice to aid critical infrastructure stakeholders to understand and use biometrics successfully.

This report outlines the work of the thematic group between October 2015 and August 2016.

1. General description of the thematic group

1.1. Purpose

Since the previous phase of activity covered by this thematic group (TG) from 2012 to 2014, biometric identity technologies, such as fingerprint, iris or face recognition, have become more common technologies in use for control of access to critical infrastructure (CI). In particular, the technologies are more widely used for border control and travel documentation.

Some technologies, such as facial recognition, have become much more accurate and are now thought to be capable of achieving useful results using data from closed-circuit television (CCTV) systems. The number of such systems deployed has increased rapidly and they are increasingly seen as a vital asset to protect CI and the wider society. These factors have led the thematic group to look in particular in this phase of work at helping the efforts to standardise the use of CCTV imagery for biometric recognition.

A particular challenge to the successful use of biometric technologies is still the testing and evaluation of wide-scale deployments of disparate sensors. This is because the required correct identification rates are often high and the acceptable false alarm rate needs to be low, so very many tests must be run to determine the performance of individual sensors and systems. In this phase of the TG's work there was also an emphasis on helping standardisation of biometric systems to support physical access control within a secure area.

The improving capabilities of biometric systems mean that a lot of data that is currently being captured (particularly CCTV facial images) that in the past would not have been considered suitable for biometric processing are now within scope and therefore need to be included in privacy and data protection considerations. In addition, the increasing use of biometrics in consumer devices such as mobile phones have increased the need for coordinated actions to ensure that privacy and data protection issues are fully considered.

The TG has had a focus on privacy issues during this phase of the work and will be continuing with its activities prior to the next phase of activity. The outputs of this workshop will be used to finalise the results of an initial investigation that was performed in this phase of the TG's work.

The utility of biometric technologies is largely unquantified. In particular, the following criteria are often unknown or impossible to compare against competing systems:

- the performance of the underlying biometric system;
- the robustness to vulnerabilities such as direct (spoofing) or indirect attacks;
- the strength of privacy preservation techniques.

The lack of involvement from user groups is the reason that we cannot measure the utility of biometric technologies. Some initiatives exist in Europe, the United States and Asia. However, these initiatives are isolated and the ERNCIP programme has provided valuable interactions to increase understanding. During this phase of the TG's work there

have been interactions with users through wider ERNCIP meetings and these interactions will continue prior to the start of the next phase.

1.2. Objectives

A series of objectives for the TG were identified for this phase of the activity:

- to continue the contribution to the standardisation, evaluation, testing and certification initiatives in key application areas for critical national infrastructures;
- to promote and validate the resources developed in the previous phases of the TG's work and seek to extend them through initial investigations on areas such as privacy.

The work programme for this phase of work was approved by the ERNCIP Office on 13 November, 2015.

Group structure

Coordinator: Peter Waggett, IBM UK Ltd

Participating organisations (October 2015 to August 2016):

Denmark: DBI
France: Safran Morpho

France: Thales

Germany: Franhofer Institute for Computer Graphics Research

Netherlands: European Association of Biometrics Group

Poland: Naukowa i Akademicka SiećKomputerowa (Research and Academic Computer Network)/Warsaw University of Technology

Spain: Universidad Carlos III

Switzerland: Idiap Research Institute (former Institut Dalle Molle d'Intelligence Artificielle Perceptive)

United Kingdom: CAST - Home Office Centre for Applied Science and Technology

United Kingdom: CESG (former Communications-Electronics Security Group)

United Kingdom: IBM

United Kingdom: National Physical Laboratory

United Kingdom: University of Surrey

The members of the group met five times between October 2015 and August 2016. Members of the TG also participated in the first ERNCIP/Improver operator workshop and two of the ERNCIP Group of EU CIP Experts meetings.

2. Way of working

The TG decided to split its technical work into a number of work packages, organised under two broad work headings, namely:

- standardisation, evaluation, testing and certification to meet the requirements of operators of CI's and other stakeholders;
- work on awareness, elicitation of priorities and promotion of appropriate use of biometrics in CI's

In its work in this phase the group identified the following applications where biometrics can support security processes and considered them in its responses:

- automated border controls;
- physical access control (particularly to special zones within a restricted area of operation of critical infrastructure);
- logical access control (additional security for access to IT systems);
- mobile identity checks ('on-the-spot challenge'/virtual zones in restricted areas of operation of critical infrastructures);
- biometric recognition of individuals from CCTV (noting a link to the TG on video analytics and surveillance).

3. Results and deliverables 2015-2016

3.1. Standards development

The main achievements of the Group in the standardisation area were the consolidation of input to:

- ISO/IEC JTC 1/SC 37 Technical Committee for Biometric Standards, regarding Biometrics in CCTV;
- CEN Technical Committee 224 Working Group 18 — Biometrics, regarding Biometrics for Physical Access Control.

3.1.1. ISO/IEC JTC 1/SC37 Committee for Biometric Standards, regarding Biometrics in CCTV

During 2014, TG members contributed to a new work item (multipart standard ISO/IEC 30137), which was proposed to SC37 for development on biometric CCTV activities, and to a new work item for standards development on biometric physical access control activities.

At the January 2014 plenary meeting of JTC1 ISO/IEC SC37 (international standards subcommittee on biometrics), the new work item (NWI) on use of operator-assisted automated face recognition in CCTV systems was adopted, having gained the required number of votes from national standardisation bodies.

The ERNCIP Applied Biometrics TG contributed significantly in the first phase of its work to the development of one of the base documents, which complemented the submission from the South Korean national standards body and led to a combined NWI.

In this phase of the TG's work, meetings were held prior to SC37 meetings in January and July 2016 to ensure that the development of the standard was guided in a direction that ensured the standard would be an appropriate one for use and adoption by operators of CI's across Europe. This is a three-part standard but the majority of the work at this time is directed at the first two parts, as a lot of the work in the third part of the standard in terms of data formats will necessarily need the first two parts to be advanced prior to its development. The scope of the discussions held at the TG meetings focused on problematic areas (in particular finalising and agreeing schematic diagrams that will make the standard understandable in an unambiguous way across the large number of stakeholders) and requesting TG members to provide additional content via the International Standards Organisation (ISO) commenting process. It was identified that the TG needed additional expertise in this area and a new member was recruited to the TG from Thales. This also allowed the TG to cover other related standards groups and get additional insights around CCTV systems.

At each SC37 meeting the first and second parts of the standards made the expected progress and TG experts have acted as editors for them. It is expected that these documents will also need input for the January 2017 SC37 meeting and the TG experts involved will need to coordinate inputs prior to this meeting. This meeting will take place outside of the framework of the ERNCIP programme prior to the start of the next phase. It is hoped that it will be possible to cover subsequent meetings under a new phase of the TG's work.

Scope of ISO/IEC 30137

This multi-part standard is applicable to the use of biometrics in video surveillance systems (also known as CCTV systems) for a number of scenarios, including real-time operation against watch lists and in post event analysis of video data.

Part 1: Design and specification

- defines the key terms for use in the specification and testing of AFR in video surveillance systems, including metrics for defining performance;
- provides guidance on selection of camera types, placement of cameras, image specification, etc. for operation of a face recognition capability;
- provides guidance on the composition of the gallery (which may be a blacklist or a whitelist) against which face images from the video surveillance system are compared, including the selection of appropriate images of sufficient quality and the size of the watch list in relation to performance requirements;
- makes recommendations on data formats for facial images and other relevant information (including metadata) obtained from video footage, used in watch list images, or from observations made by human operators;
- establishes general principles for supporting the operator of the video surveillance system, including user interfaces and processes to ensure efficient and effective operation and the requirements for trained and motivated personnel;
- establishes best practice in supporting the operator, such as user interfaces and processes to ensure efficient and effective operation of the system and the requirements for trained and motivated personnel;
- specifies performance metrics and testing methodologies applicable to performance measurement of operational systems (addressing the nature of video, with multiple frames and multiple individuals, as well as the use of the operator in determining the final outcome);

- establishes governance processes to address requirements for security, as well as the requirements for privacy and personal data protection specific to the use o automated face recognition (AFR) in video surveillance applications (e.g. internationally recognisable signage) and societal considerations in the deployment of systems This multi-part standard is primarily applicable to the use of AFR in video surveillance systems for a number of use cases and scenarios of operation. Examples include real-time operation against watch lists and post event analysis of video data.

Part 2: Performance testing and reporting

This part of the standard:

- describes a framework for testing and reporting the performance of detecting and recognising humans in the video captured by a surveillance camera which is in general installed relatively far from the human, compared to traditional biometric systems;
- defines the key terms for use in the specification and testing of automated face recognition and other biometric recognition in video surveillance systems, including metrics defining performance;
- specifies testing methodologies applicable to performance measurement of operational systems (addressing the nature of video, with multiple frames and multiple individuals, as well as the use of the operator in determining the final outcome);
- specifies requirements for test methods, recording of data, and reporting of results.

Part 3: Data formats

This part of ISO/IEC 30137 specifies data format(s) for storing, recording and transmitting biometric information acquired via a CCTV system. It is anticipated that in most cases the biometric modality will be the face, but this standard is not restricted solely to face image data (for example it may be possible to extract iris images or perform gait analysis in some scenarios where high-resolution cameras are used. More generally, exchanges between expert groups working on ISO/IEC 30137 Part3 and on Edition 2 of IS0 22311 in ISO TC292 WG6 have been initiated to ensure that the ERNCIP needs are properly taken into account in the future Edition 2 of IS0 22311, but also that the format selected for biometry is consistent with the data formats applicable to other types of analytics, preparing for a future-proof cost-effective interoperability within the community of CCTV systems

3.1.2. CEN Technical Committee 224 Working Group 18 — Biometrics, regarding Biometrics for Physical Access Control

The ERNCIP Thematic Group on Applied Biometrics supported the response to the European Commission's Mandate M/487 to establish a roadmap for security standards with this work on biometric physical access control

Technology trends for biometric physical access control activity are leading to an increasing need for standardisation activities to ensure that their promise is met while respecting the needs for individuals' privacy and data security. These trends include:

- an increasing number of biometric modes that are becoming both practical and affordable for large-scale deployment;
- an increasing number of installations that need highly secured access;
- an increasing number of 'owners' of installations (due to outsourcing etc.);
- an increasing awareness of conflicting requirements for data sharing and privacy.

The ERNCIP stakeholders also impose significant challenges at a practical and geopolitical level. These include:

- differing legal and cultural norms around data collection, storage and privacy;
- highly varied environments for data collection including some that are environmentally challenging.

During 2014 a new work item was presented at CEN TC224 WG 18 for standard development on physical access control activities. This ERNCIP TG was represented at all of the meetings in 2015 and 2016 and its experts were able to drive the standard forward.

The standard is on course for publication in 2017 and will then be presented to ISO SC37 for further development as an international standard.

3.1.3. Other standards activity

In addition to the CCTV and access control standards, contributions were made to other standards under development by SC37. These include the biometrics vocabulary, which is seen as a major contribution to standardising the language used in CI procurement. This is being pursued in SC37 for an English version and CEN TC224 WG18 in other European languages. The increasing importance that CNI operators see in presentation attacks has meant that the TG experts have provided contributions to the progression of that multi-part standard.

TG experts are also involved heavily in ISO SC17, covering identity and travel documents, which are regarded as key elements of a CI based identification strategy.

3.2. Additional resources

The promotion and validation of the resources developed in the previous phases of the TG's work was conducted during this phase and the resources have also been extended through an initial investigation on privacy.

The two reports generated during the previous phase of the TG's work were publicised by members of the TG at a number of meetings with stakeholders at European and global events. The primary meetings were associated with the communities involved in meetings at ISO SC17 and SC37 and also CEN TC224 WG 18. The convenor of the TG also presented at the ERNCIP Expert and Operators workshops that were held during this phase of the work. The presentation given to the group is attached as Annex A. Discussions and comments on these documents were generally positive and only minor additions were suggested.

The TG's documents have been downloaded from the ERNCIP website over 600 times. They will be updated if any substantive comments are received during the next phase of the TG's activities.

Members of the TG held a privacy workshop prior to the start of the project in October 2015. This workshop confirmed the belief that an initial investigation should be performed into the impact of privacy on operators' use of biometric data and systems. The results of this initial investigation are being presented as an additional report in this phase of the TG's activities.

4. Expected future focus

4.1. Continuation of current TG activities

The activities initiated with ISO and CEN for biometric recognition with CCTV systems and for physical access control will need to be continued in 2016 in order to reach the objective of developed standards in 2017. TG experts have already committed to continue these actions prior to the commencement of the next phase of TG activity. In addition, experts from the TG will be holding a workshop in October 2016 to consult with stakeholders on their areas of concern around European norms for data privacy and biometrics. These norms are being challenged by current and proposed implementations of systems using biometric data. This workshop is one of a series that were initiated by TG experts in 2014 and are planned to continue in 2017. The network of contacts established by the experts in this phase of the ERNCIP project have provided invaluable input to the progression of the TG's objectives and this will continue during the gap between ERNCIP phases.

4.2. Potential new work items for the TG

Extended 'virtual fencing' — Biometrics at a distance

Recent security incidents that have been directed at 'soft targets' and those that have caused damage at access control points have highlighted the need to identify threats at a distance. Successful identification of these threats could provide alerts and allow for the deployment of measures to counter or reduce the impact of these threats.

Biometrics provides the promise of such identifications through a number of methods. Standard CCTV systems can now provide imagery that can be analysed and used for direct biometric analysis via face or gait recognition or indirect recognition through behavioural biometric approaches. These can provide an identification at a relatively long range from the sensor.

Other biometric modalities such as 'iris on the move', gait recognition and face recognition can provide alerts at a distance via sensors that have been deployed ahead of boundaries.

This is an area of work that the thematic group would seek to address during a future work period in 2017. This work has the potential to overlap in content and interest with other thematic groups and this will be explored by members of the biometric theme prior to the start of the next phase of work using contacts and introductions identified by the JRC ERNCIP management team.

Recent incidents indicate that this is a high-priority item for work at EU level but it may require significant funding to make much progress and is therefore only rated as of medium level with respect to the ability of the TG to progress rapidly.

Presentation attack detection

Over the duration of this phase of the thematic group an awareness of the potential for biometric mechanisms to be subject to a variety of attacks and attack methods has become apparent. At the ISO level this awareness is driving standards development but it has also become apparent that there is a need for a mechanism to allow critical national infrastructure operators across Europe to have a method to share information about individual attacks and counter measures that have been implemented. This mechanism needs to be secure and managed to ensure that it does not itself lead to a proliferation of attacks through sharing of information with the wrong groups of individuals.

In some respects this service will provide a biometric analogue for methods currently in use to prevent or mitigate cyber and virus attacks.

The thematic group would seek to articulate the requirements for providing such a service across Europe in the next phase of the work.

The TG believes this is an area which will become increasingly important to CI operators and is an area where the TG's ability to make an impact could be high.

Disaster victim identification

Natural disasters and man-made incidents often lead to chaotic conditions and the potential for vital forensic identification and other data to be lost or confused in the early stages of a response. Lack of timely information can also lead to uncoordinated actions from first responders and others. The understanding of this problem has led to a growing realisation that best practice in this area needs to be captured and propagated. There may also be a need to allow emergency activity (e.g. the ability of security responses to include real-time control and monitoring of CCTV equipment regardless of the ownership of the equipment).

The existing activity in this area is currently being advanced under an early work item within ISO SC37. There are EU requirements (e.g. privacy) that will not be within the scope of the ISO standard. These could be activated under a parallel standard that could be progressed within CEN TC224 WG 18 with the support of this thematic group.

The TG believes this is an area which will become increasingly important to CI operators and is an area where the TG's ability to make an impact could be high.

Cyber-biometrics and social media biometrics

The aim of this investigation will be to work towards a rich understanding of identity, which will encompass aspects that we reveal both in the real world and in the cyber world. The fusion of cyber and real world measures is what will make this investigation challenging, exciting and timely. The result will be a more complete and dynamic picture of who someone is, enabling greater input into the identity decision. It is anticipated that this project will build on the concepts of super-identity outlined in previous research programmes and will require the recruitment to the TG of additional expertise.

The TG believes that this is an area of medium priority for CI operators at present but has the potential to become high priority in the future. The ability of the TG to work on

this problem in the short term is low but could become high if additional experts were able to participate in the TG.

Multi-modal biometrics

The increasing availability of biometric information in a number of biometric modes can provide operators with the potential to combine and fuse these results to make more accurate and reliable identifications. The approach to biometrics fusion needs to be carefully considered and designed as, although it seems slightly counter intuitive, poor biometric fusion can lead to increasing numbers of false alarms or misidentifications.

In the next phase of the TG the experts will seek to investigate and document best practice advice for critical national infrastructure operators.

The TG believes that this is an area of medium priority for CI operators at present but which has the potential to become high priority in the near future. The ability of the TG to work on this problem in the short term is medium but could become high if additional experts were able to participate in the TG.

Bring your own authentication and biometrics

Biometric sensors are becoming a standard part of a smart phone. At present biometrics on smart phones is mainly used to unlock the device or to unlock an application. It is to be expected that in the future the smart phone may become a biometrically enhanced identity (ID) token next to, and maybe even replacing, other accepted ID documents such as the passport. This will lead to various new applications, including physical access control. There are various options for the authentication workflow, depending on where the verification is done and where the biometric reference is stored. All these architectures have their own security and privacy risks that need to be investigated and mitigated.

In the next phase of the TG the experts will seek to investigate the aforementioned security and privacy risk and their mitigation.

The TG believes that this is an area of medium priority for CI operators at present but which has the potential to become high priority in the near future. The ability of the TG to work on this problem in the short term is medium but could become high if additional experts were able to participate in the TG.

ANNEX A — TG presentation to the ERNCIP Experts Group on 29 June 2016

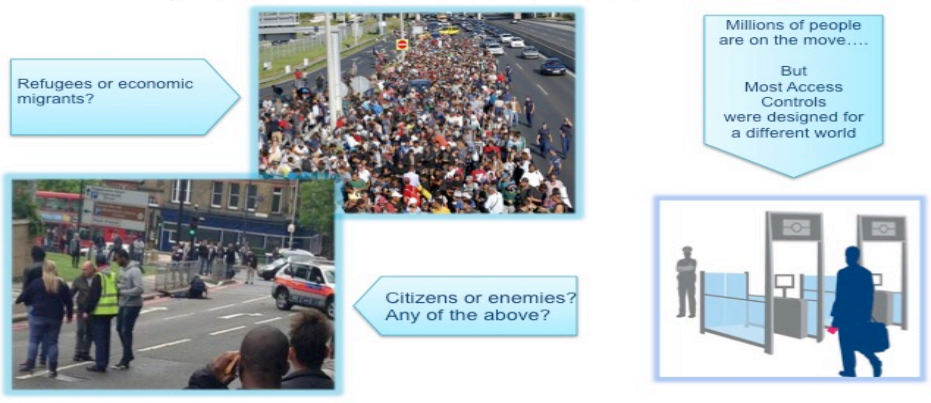
Applied Biometrics for Critical Infrastructure Protection

ERNCIP Group of CIP Experts Group Meeting
29/6/16
Dr Peter Waggett

Biometrics and Critical Infrastructures

- Critical Infrastructures need to identify for:
  - Automated border control
  - Physical access control
  - Logical access control
  - Mobile identity checks
  - Biometric recognition from images and imagery
- Critical Infrastructures face increasingly complex challenges and threats around 'identity' and always will

Biometrics are becoming increasingly important to critical infrastructure



Meeting demands for new biometric services in a timely, and cost effective manner

How do we identify someone with no passport, no ticket, no biography?

How do we recognise someone with a valid passport – but in a false identity

facial matching

4

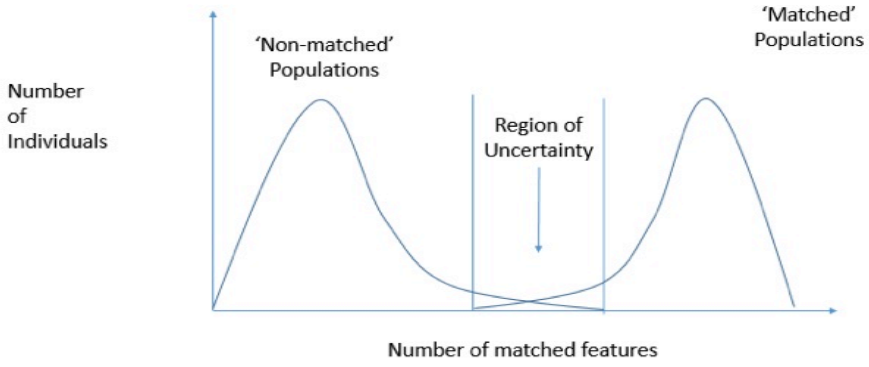
Biometrics and Critical Infrastructures

- Biometrics is defined as the automatic recognition of individuals through biological or behavioral characteristics
- Biometrics encompasses multiple modes
  - Fingerprint
  - Face
  - Iris
  - Voice
  - Key stroke dynamics
  - etc

Identity Management

- Need to provide comprehensive and complete coverage for a population - no one can be excluded
- Two major tasks:
  - Biographic analysis to establish an 'identity'
  - Biometric analysis to associate an individual to that 'identity'
- Exception handling processes and procedures needed for False Matches and Non-Matches

Biometric Matching Challenge



Citizens are seeing biometrics as their preferred authentication method

Selfies to protect digital identities of users Paris,February 18, 2016

Samsung SDS to deploy Morpho's facial recognition technology for *online authentication*

The launch of the iPhone 5s in 2013 was the largest deployment of biometric devices ever.

9 million units were sold on the first weekend of its launch.

eGates are no longer reserved for premium passengers

179 Airports in 60 countries are using biometrics to automate border control

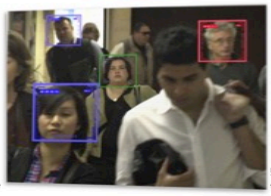
8

Familiarity with biometrics comes with raised expectations

Why can't we…..

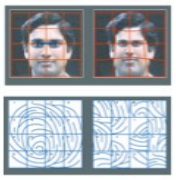
- Point a camera at a moving crowd and identify people accurately and consistently?
- Track them through a crowd?
- **Challenges**
  - Lighting
  - Occlusion
  - Movement
  - Confusion
  - Limited Capture time
  - Unwilling subjects
  - Sorting candidates
  - Eliminate False Positives
  - Uncontrolled Environment

Control the variables



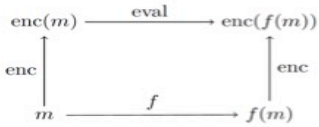
Biometric Technology is constantly evolving, predicting the winners and losers is difficult

Cancellable Biometrics



- Hacking the database is pointless.
- New Biometric identities can be created
- Use standard matching algorithms

Fully Homomorphic Encryption



Technique to send an encrypted matching request to an unencrypted database

And receive an accurate answer

The matching system is 'oblivious' to who asked what

Supports security agencies without revealing their identity

Multiple copies of databases for each agency are not required

10

Biometrics Theme

- Objectives
  - To develop resources to aid procurement and implementation of biometrics in Critical Infrastructures
  - To contribute to standardization, evaluation and testing initiatives to represent the needs of Critical Infrastructures in those activities

First Phase Highlights

- 24 contributors from 9 Countries gave us large number of views
- Document describing best practice around testing for large scale systems
- Document describing best practice for security managers of Critical Infrastructures to implementing biometric controls
- Over 600 downloads

Current Activity

- New members and contributors giving new insights to work
- Maintaining momentum in standards bodies to deliver biometric standards that are fit for Critical Infrastructures especially for CCTV
- Ensuring privacy issues and guidelines are investigated for Citizens but balanced to ensure successful operation of systems

LB-04-16-827-EN-N

JRC mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy directorates-general, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/909340

ISBN 978-92-79-62218-2