PHILOSOPHICAL TRANSACTIONS B

rstb.royalsocietypublishing.org

Research

Cite this article: Jain AK, Ross A. 2015 Bridging the gap: from biometrics to forensics. *Phil. Trans. R. Soc. B* **370**: 20140254.
http://dx.doi.org/10.1098/rstb.2014.0254

Accepted: 4 May 2015

One contribution of 15 to a discussion meeting issue 'The paradigm shift for UK forensic science'.

Subject Areas:
behaviour

Keywords:
biometrics, forensics, sketch-to-photo matching, tattoo matching, fingermarks, video surveillance

Author for correspondence:
Anil K. Jain
e-mail: jain@cse.msu.edu

Bridging the gap: from biometrics to forensics

Anil K. Jain and Arun Ross

Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 USA

Biometric recognition, or simply biometrics, refers to automated recognition of individuals based on their behavioural and biological characteristics. The success of fingerprints in forensic science and law enforcement applications, coupled with growing concerns related to border control, financial fraud and cyber security, has generated a huge interest in using fingerprints, as well as other biological traits, for automated person recognition. It is, therefore, not surprising to see biometrics permeating various segments of our society. Applications include smartphone security, mobile payment, border crossing, national civil registry and access to restricted facilities. Despite these successful deployments in various fields, there are several existing challenges and new opportunities for person recognition using biometrics. In particular, when biometric data is acquired in an unconstrained environment or if the subject is uncooperative, the quality of the ensuing biometric data may not be amenable for automated person recognition. This is particularly true in crime-scene investigations, where the biological evidence gleaned from a scene may be of poor quality. In this article, we first discuss how biometrics evolved from forensic science and how its focus is shifting back to its origin in order to address some challenging problems. Next, we enumerate the similarities and differences between biometrics and forensics. We then present some applications where the principles of biometrics are being successfully leveraged into forensics in order to solve critical problems in the law enforcement domain. Finally, we discuss new collaborative opportunities for researchers in biometrics and forensics, in order to address hitherto unsolved problems that can benefit society at large.

1. Introduction

Biometric recognition, or simply biometrics, refers to the automated recognition of individuals based on their biological and behavioural characteristics [1]. Examples of biometric traits that have been successfully used in practical applications include face, fingerprint, palm print, iris, palm/finger vasculature and voice (figure 1). There is a strong link between a person and their biometric traits because biometric traits are inherent to an individual. A typical biometric system can be viewed as a 'real-time' automatic pattern matching system that acquires biological data from an individual (e.g. a fingerprint) using a sensor, extracts a set of discriminatory features from this data (e.g. minutiae points) and compares the extracted feature set with those in a database in order to recognize the individual. It is assumed that each feature set in the database (referred to as a template) is linked to a distinct individual via an identifier, such as a name or an ID number. Comparison of the extracted feature set and the template results in a score indicating the similarity between the two feature sets. Assessment of the similarity of the feature sets may then be used to recognize the individual.

In modern society, the ability to reliably identify individuals in real time is a fundamental requirement in many applications including international border crossing, transactions in automated teller machines, e-commerce and computer login. As people become increasingly mobile in a highly networked world, the process of accurately identifying individuals becomes even more critical as well as challenging. Failure to identify individuals correctly can have grave repercussions in society ranging from terrorist attacks to identity fraud where a citizen

THE ROYAL SOCIETY PUBLISHING

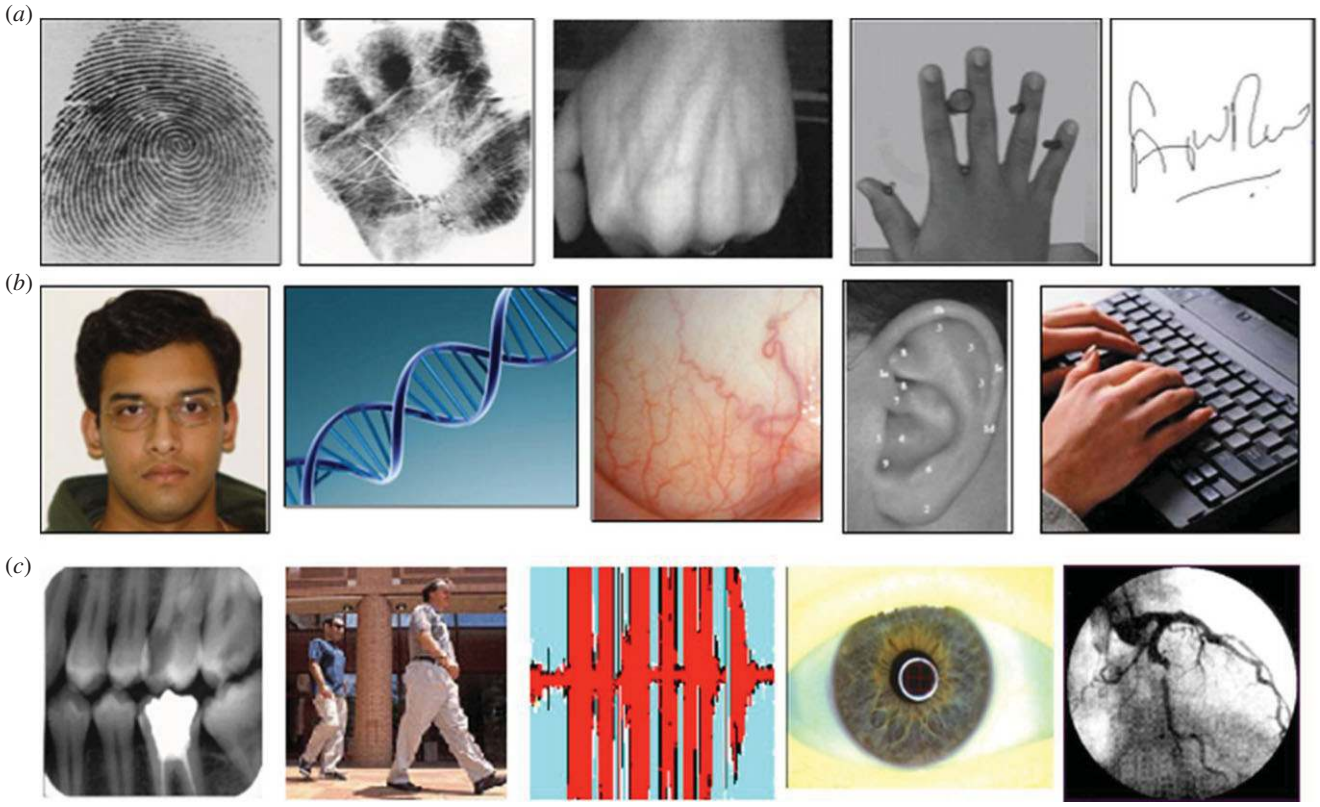


Figure 1. Examples of biometric traits. (*a*) Fingerprints, palm prints, hand vasculature, hand shape and signature. (*b*) Face, DNA, sclera (on the eyeball), ear shape and typing patterns (keystroke dynamics). (*c*) Teeth (forensic odontology), gait, voice or speech, iris and retina. Some of these traits, *viz*., fingerprints, palm prints, face, voice, teeth, ear shape and DNA, are also used in forensics. (Online version in colour.)

loses access to his own bank accounts and other personal information. The two biggest driving factors behind the emergence of biometrics are improved homeland security and curtailing financial fraud.

Indeed, the last two decades have seen a rapid adoption of biometric systems across a variety of application domains. Without a doubt, biometric technology is already creating a significant impact on our society. For example, biometrics continues to play a critical role in law enforcement applications both as an investigative tool to narrow down the suspect list and as forensic evidence in a court of law. Biometric recognition has also become an integral part of identity management systems around the world, especially in developing countries where a large number of people lack formal identity documents to prove who they are. The Aadhar project, implemented by the Unique Identification Authority of India (UIDAI), is a formidable and unprecedented effort to provide a unique 12-digit identification number to approximately 1.2 billion residents of India. Under this project, ten fingerprints and two irises are used for de-duplicating identities; as of now approximately 800 million Aadhar numbers have been issued. It is expected that such biometric identification programmes will serve as vehicles for effective delivery of healthcare, curtail fraud in welfare benefits and enable secure financial transactions [2]. Biometric systems have also changed the way we travel by enhancing security, efficiency and reliability of border-crossing systems. In the USA, biometrics-based person authentication in border control and transportation systems was implemented after the 9/11 terrorist attacks. In consumer electronics, every major mobile device vendor now has either incorporated or is in the process of introducing biometric-based authentication for phone security and mobile payment.

The first known research publication on automated biometric recognition was published by Trauring [3] in 1963 on fingerprint matching. The foundation for automated biometric systems based on other traits such as voice [4], face [5] and signature [6] were laid in the 1960s. Subsequently, biometrics systems based on traits like hand shape [7] and iris [8] were developed. Not surprisingly, the advent of biometric recognition systems coincided with advancements in other closely related areas such as artificial intelligence, pattern recognition and image processing in the 1960s, which helped in the analysis and recognition of biometric patterns.

However, the event that really triggered the systematic use of biometric traits to recognize a person happened a hundred years before Trauring's landmark paper. The event was the enactment of the Habitual Criminals Act in 1869 in the UK [9]. This Act made it mandatory to maintain a register of all persons convicted of a crime in the UK along with appropriate evidence of their identity. This register was used to identify repeat offenders, who were generally incarcerated with a higher degree of punishment compared with first-time offenders. The need for such an identification scheme was expressed by a Home Office Committee as follows [9]:

> What is wanted is a means of classifying the records of habitual criminal, such that as soon as the particulars of the personality of any prisoner (whether description, measurements, marks, or photographs) are received, it may be possible to ascertain readily, and with certainty, whether his case is in the register, and if so, who he is. (p. 257)

In order to identify such repeat offenders, Bertillon [10] introduced a system for recognizing persons based on a set of anthropometric measurements. Additionally, he used multiple descriptive attributes such as eye colour, scars and

Figure 2. Examples of biometric applications. (*a*) A Texas hospital uses palm scans to verify registered patients. (*b*) The Office of Biometric Identity Management (OBIM), formerly referred to as the US-VISIT program, uses all 10 fingerprints to verify the identity of a visa holder entering the United States; the fingerprint data is also compared against a watch-list of known identities. (*c*) The identity of ticket holders accessing theme parks in Disney Parks is confirmed using fingerprints to ensure that the tickets are not shared across customers. (*d*) An Apple Pay customer initiates payment by placing his finger on the iPhone fingerprint sensor and holding the phone near a contactless reader. (Online version in colour.)

marks (referred to as soft biometrics in contemporary literature) in order to recognize an individual. But the Bertillon system lacked automation, was cumbersome to administer uniformly (making it prone to error), and even when administered correctly, the measurements were not distinctive enough to uniquely identify individuals. Therefore, it was quickly abandoned in favour of a relatively simpler and more accurate approach involving manual comparison of human fingerprints. This was made possible by the pioneering works of Faulds, Herschel and Galton, who studied the distinctiveness of configurations of certain features in a fingerprint ridge pattern such as minutia points [11].

In 1891, Argentine police officials initiated the fingerprinting of criminals and used fingerprint as evidence in a homicide case in 1892 [12]. This is believed to be the first use of fingerprints in criminal proceedings. Starting from around 1900, Scotland Yard in the UK began using fingerprint in law enforcement applications (http://onin.com/fp/fphistory.html). Fingerprints were accepted as evidence of identity in a British criminal case for the first time in 1905. In 1924, the United States Congress authorized the Department of Justice to collect fingerprints along with the arrest information. This paved the way for the establishment of a fingerprint identification system by the Federal Bureau of Investigation (FBI) in the USA. The system started with collecting fingerprints using 10-print cards and, in the late 1970s, advanced to an automated fingerprint identification system (AFIS). Though this system is referred to as 'automated', it must be mentioned that the automation was not fully completed in the initial years of deployment. Human experts were (and to a lesser extent even now) still required to process the fingerprint-cards and identify the basic features such as minutia points, which were then matched automatically by the AFIS to retrieve a short list of most similar candidates from the database. The final match decision continued to be made by human experts. It must be noted that in many contemporary intelligence applications involving fingermarks (also referred to as latent prints), the matching process is still semi-automated.

The aforementioned discussion indicates that the origin of biometric recognition is in fact rooted in the law enforcement and forensic science domain where 'recognition' entailed the apprehension of criminals. But, as stated earlier, it is now being increasingly used in identity management systems where the principal goal is to allow an individual to access a resource (e.g. a mobile phone) or receive a privilege (e.g. entering a country). Examples are shown in figure 2.

2. Biometrics versus forensic science

Forensic science entails the application of scientific principles to analyse evidence at a crime scene in order to reconstruct and describe past events in a legal setting. It has been deeply influenced by *Locard's exchange principle* that states that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence. In his book *Crime Investigation: Physical Evidence and the Police Laboratory*, Kirk articulates the principle as follows [13]:

> Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool marks he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value. (p. 4)

A number of sources of impression evidence are used in forensic investigations, including fingermarks, tyre marks, shoemarks, tool marks and handwriting [14]. Additionally, other types of evidence such as voice and face are also used. One of the principal objectives of a forensic investigation is to associate an item

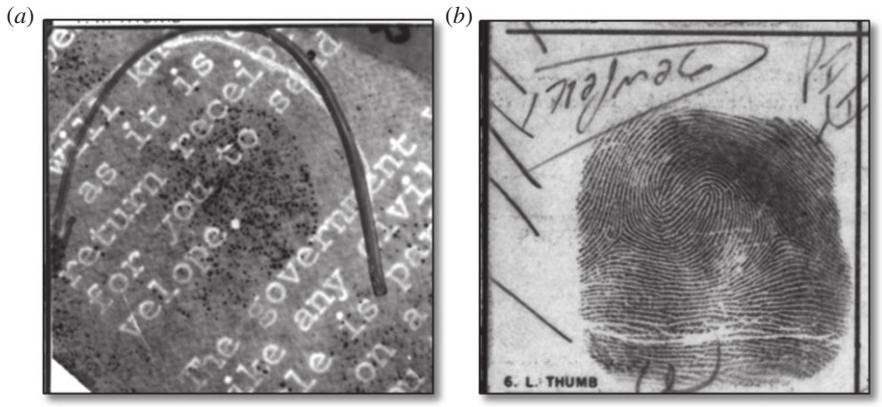


Figure 3. (*a*) The fingermark is an item of evidence retrieved, for example, from a crime scene. (*b*) The rolled fingerprint is obtained from a known source (i.e. known individual).

of *evidence* (e.g. a fingerprint) with a *source* (e.g. an individual). Consider a fingermark recovered at a crime scene (figure 3). In the context of a forensic investigation, once the fingermark is deemed to be related to the criminal activity, then the subsequent question is: *What is the source of this evidence,* i.e. *who or what generated this fingermark?* In *traditional* forensic evaluation, there were at least three possible outcomes based on the examination of the evidence: (i) individualization: no other individual on earth is source of the fingermark; (ii) inconclusive: it is not possible to reliably assert whether or not the fingermark is associated with the known individual; and (iii) exclusion: the fingermark is definitely not associated with the known individual. The *contemporary* approach, however, focuses on the strength of the evidence in favour of the pair of propositions—H1: the fingermark under examination originates from the donor suspected in the case; and H2: the fingermark under examination originates from another donor [15].

In this regard, both forensic science and biometric recognition seek to link biological data (impression evidence) to a particular individual. Despite this commonality, there are a number of differences between forensics and biometrics:

(1) Forensic science is invoked *after* the occurrence of an event and is typically used to reconstruct past criminal events by a hypothetico-deductive approach. Biometric recognition, on the other hand, is typically used *before* the occurrence of an event (e.g. accessing a laptop or entering a country).
(2) In a forensic investigation it is not possible to determine in *advance* the type of evidence that will be used to apprehend the perpetrator of the crime. The crime scene has to be carefully examined in order to glean evidence that is subsequently used for recognition purposes. This is in contrast to biometric systems where the biological traits (i.e. modalities) to be used for person recognition are known in advance.
(3) Forensic science predominantly involves the *manual* collection and examination of evidence, compared to biometric recognition which is by definition fully *automated*. Indeed, qualitative assessment schemes (as opposed to quantifiable measures) are extensively used in the context of forensics for establishing the similarity between an item of evidence and a particular source. This can lead to cognitive bias [16] where the forensic expert can be unduly swayed by external factors while examining and interpreting the evidence.
(4) Recognition decisions in biometric systems have to be rendered in *real time* and, therefore, computational efficiency is an important factor in biometric applications. In forensics, however, real-time recognition is not a requirement.
(5) In forensic science, a *false non-match* is highly undesirable since it can result in excluding the perpetrator of a crime from further consideration. In the case of biometrics, depending upon the application at hand, the consequences of false matches and false non-matches can be different. For example, in a surveillance system, false non-matches have to be minimized at the risk of increasing false matches; however, in a biometric access control system for a nuclear plant, false matches have to be minimized even if this results in an increased number of false non-matches.
(6) An *inconclusive* decision in forensics means that crime-scene evidence cannot be associated with certainty to a particular individual. But a biometric system can acquire additional samples of a biometric trait (or of additional traits) from an individual for rendering a 'match' or 'no match' decision.
(7) The *quality* of the evidence data obtained in the case of forensics is typically lower than that of biometrics. Trace or impression evidence used in forensic investigations has to be meticulously extracted from a crime scene where, unlike in biometrics, a person does not deliberately deposit the biological evidence. This is one reason why a fully automated scheme cannot always be used to establish a match in the case of forensics.
(8) The outcome of a forensic investigation process has to be often *verbally* communicated to a jury or a judge. Thus, verbal reasoning is crucial in forensics. For example, when declaring the degree of similarity between a fingermark and the defendant's fingerprint, the expert witness has to offer a verbal justification characterized by both qualitative and quantitative metrics. The outcome of biometric recognition, on the other hand, is a numerical score (or a set of scores) that is systematically used (in conjunction with a pre-specified threshold) by the automated system for declaring a match—therefore, verbal reasoning is not necessary in automated identity management systems.

For a number of years, the biometric and forensic research communities have pursued their vocation independently of each other. However, recently, there has been an increased

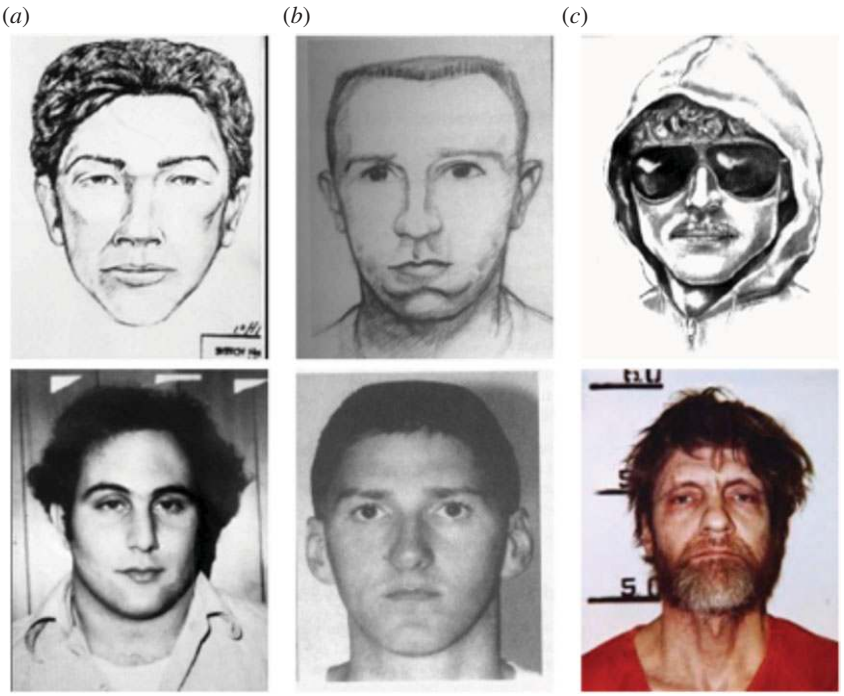


Figure 4. Examples of facial composites used in cases in which the suspect was successfully apprehended after the police received a tip from the public. Examples of composites drawn by a forensic artist and their corresponding mugshots are shown for (*a*) David Berkowitz (Son of Sam), (*b*) Timothy McVeigh (the Oklahoma City bomber) and (*c*) Ted Kaczynski (the Unabomber). (Online version in colour.)

interest in harnessing the automated approach developed in biometrics to address problems faced by forensic scientists. Two such applications are discussed below: sketch-to-photo face matching and tattoo image matching. In both applications, biometrics can be used as an investigative tool to quickly narrow down the suspect list.

3. Biometrics for forensic applications

(a) Sketch-to-photo face comparison

Facial sketches or composites are routinely used in law enforcement to assist in identifying suspects involved in a crime when no facial image of the suspect is available at the crime scene (e.g. due to the absence of surveillance cameras). After a composite of a suspect's face is created, authorities disseminate the composite to law enforcement and media outlets with the hope that someone will recognize the individual and provide pertinent information leading to an arrest (figure 4). Facial composites are particularly valuable when eyewitness descriptions are the only form of evidence available [17]. Unfortunately, this process is inefficient and does not leverage all available resources, in particular the extensive mugshot databases maintained by law enforcement agencies. Successful techniques for automatically matching facial composites to mugshots will enable faster apprehension of suspects.

Facial composites used in law enforcement can be divided into three categories:

(1) Hand-drawn composites: facial composites drawn by forensic artists based on the description provided by a witness. Hand-drawn composites have been used in criminal investigations dating as far back as the nineteenth century [18].
(2) Software-generated composites: facial composites created using software kits that allow an operator to select various facial components (e.g. eyes, nose) from a menu. Software-generated composites have become a popular and more affordable alternative to hand-drawn composites [18].
(3) Surveillance composites: facial composites drawn by forensic artists based on poor quality surveillance images. These are used in scenarios when commercial-off-the-shelf (COTS) face recognition systems fail due to poor lighting, off-pose faces, occlusion, etc.

Irrespective of the method used to generate the composite, the quality of the resulting composite (namely, its resemblance to the actual perpetrator of the crime) mainly depends on the accuracy of the description provided by the witness and the skill of the artist/operator.

Given the egregious nature of crimes committed by perpetrators depicted in forensic sketches—including murder, terrorism, sexual assault and armed robbery—failing to quickly capture them can have severe consequences. Improving forensic sketch recognition would greatly increase public safety. Under the broad umbrella of biometric recognition, a new paradigm has emerged for identifying suspects using forensic sketches. A sketch can be converted to a digital image and then automatically matched against mugshots and other face images in a database—for example, drivers' licence photos—to determine a match. This automated approach, enabled by progress in computer vision and machine learning algorithms, can offer a valuable resource to authorities seeking to accurately and quickly capture dangerous criminals.

(b) Automated tattoo image matching

Tattoos inscribed on the human body have been successfully used to assist human identification in forensic applications (figure 5). Tattoos can also contain hidden meanings related to a suspect's criminal history, such as gang membership, previous convictions, years spent in jail and so forth (e.g.

Figure 5. Tattoo images captured from suspects' bodies at the time of booking. Courtesy Michigan State Police. (Online version in colour.)

Figure 6. The output of an automated tattoo image retrieval system [19]. The image on the left is the 'query' image that is compared with a large database of tattoo images. The images on the right denote the top 7 candidate tattoo images retrieved from the database by the tattoo image retrieval system. The number below the query image indicates the number of 'keypoints' in it. The number below each retrieved image indicates the similarity (number of common 'keypoints') between the query image and the retrieved image. Note that, in this example, three instances of the same tattoo (with varying quality and size) as the query were present in the database and these are retrieved as the top three candidates. (Online version in colour.)

the importance of using scars, marks and tattoos (SMT) in FBI's Next Generation Identification (NGI) Systems has been documented at http://oag.ca.gov/sites/oag.ca.gov/files/072513_ssps_ngi_overview_0.pdf).

There is also an increasing prevalence of tattoos among the general population at large. According to a Harris Poll conducted in January 2012, 'one in five US adults now has a tattoo'. (http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/mid/1508/articleId/970/ctl/ReadCustom%20Default/Default.aspx). Tattoo pigments are embedded in the skin to such a depth that even severe skin burns often do not destroy a tattoo. For this reason, tattoos on their bodies helped identify victims of the 9/11 terrorist attacks and the 2004 Asian tsunami. Thus tattoo images, if available, can be used to identify victims as well as suspects.

Law enforcement agencies routinely photograph and catalogue tattoo patterns for the purpose of identifying victims and suspects (who often use aliases). The ANSI/NIST-ITL1-2011 standard defines eight major classes (human, animal, plant, flag, object, abstract, symbol and other) and a total of 70 subclasses (including male face, cat, narcotics, American flag, fire, figure, national symbols and wording) for categorizing tattoos. A tattoo image-based search currently involves comparing a query tattoo's class label with those in the tattoo database. This practice of matching tattoos according to the *manually* assigned ANSI/NIST class labels has the following limitations [19]:

(1) Class labels may not capture the semantic information, or meaning of symbols, in tattoo images.
(2) Tattoos often contain multiple symbols and cannot be classified appropriately into existing ANSI/NIST classes.
(3) Tattoo images belonging to the same class often exhibit large variations in content and appearance.
(4) The ANSI/NIST classes are not adequate for describing new tattoo designs.
(5) The process of assigning a class label to a tattoo image is subjective.

These shortcomings have led to the development of image-based techniques (as opposed to class-based) to improve tattoo image recognition performance. The challenge is to represent visual content of a tattoo in terms of features such as landmarks, texture and shape. These features can then be used for representing and comparing tattoo images without the use of any class labels.

Automated schemes to conduct tattoo matching have been presented in the biometrics literature [19]. A sample output of such a system is illustrated in figure 6. This application demonstrates how biometrics (i.e. 'automated recognition') can be imported into a forensic application (i.e. 'post-event investigation').

4. Bridging the gap: challenges and opportunities

Given the importance of solving crimes quickly and the need for automation to assist forensic experts, the use of biometric algorithms in law enforcement and forensic applications will indeed benefit society. Further, the outcomes based on most forensic evidence (e.g. fingermarks, tool marks, etc.) have not been scientifically validated. The 2009 National Academy of Sciences (NAS) report [20] on the current state of forensic science in the United States clearly articulates this shortcoming, *viz.*, that frequently made claims in forensic science are supported by far less rigorous research than might have been expected. The report points out: 'With the exception of DNA analysis, no forensic method has been rigorously shown to have the capacity to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source' (p. 7). In many

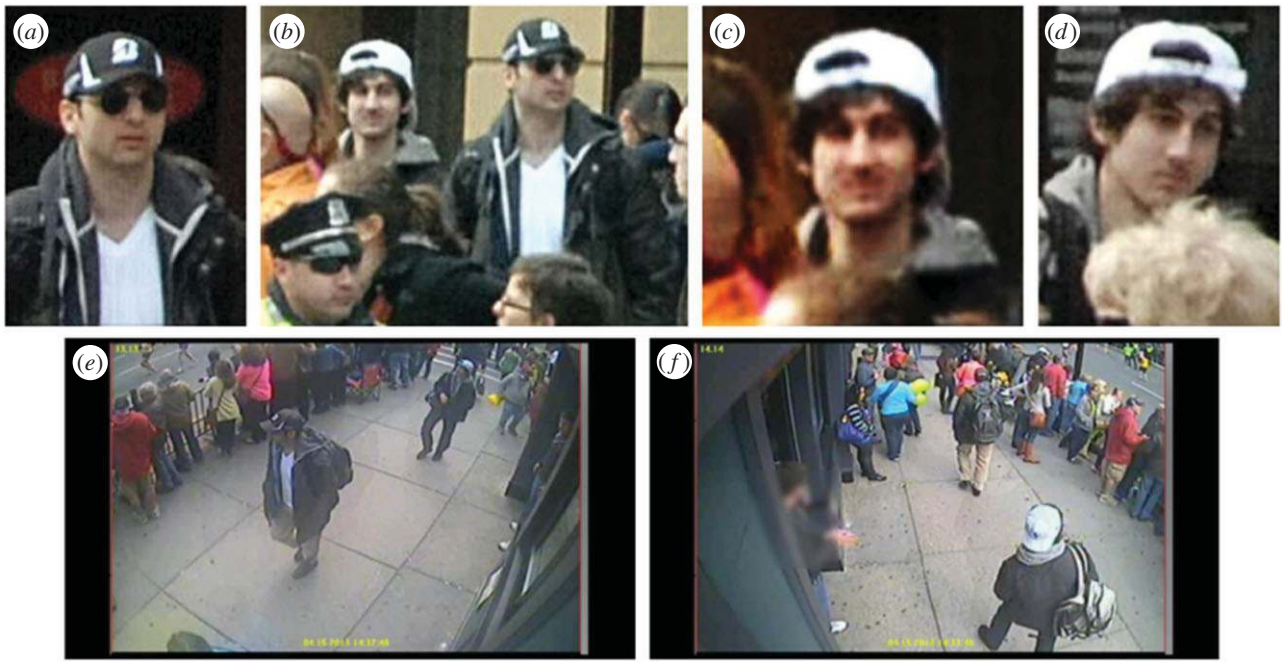


Figure 7. Facial images and videos released by law enforcement of the two suspects (brothers) in the Boston Marathon bombings. (*a*,*b*,*e*) The older brother, Tamerlan Tsarnaev, is wearing a black hat. (*c*,*d*,*f*) The younger brother, Dzhokhar Tsarnaev, is wearing a white hat. The public was asked to help identify these two individuals. (Online version in colour.)

cases, the longstanding experience of a forensic expert is assumed to be a substitute for scientifically gleaned empirical evidence. While experiential learning is important when practising forensic science, it must necessarily be imported into a scientific framework that balances 'domain knowledge' with 'empirical data'. Such a research culture is often missing from forensic science, and empirical data from rigorous studies that justify forensic scientists' opinions are scarce. Instead, the non-DNA forensic sciences (e.g. hair and bite marks [21]) have shown a disturbing tendency to treat frequently repeated opinions as scientific facts that are so well-accepted within the field that the absence of supporting data is regarded as unimportant [22]. Thornton & Peterson [23] succinctly point out: 'It is ironic that those areas of forensic science that have real underlying data offer more modest statements of individualization, while those limited to subjective or impressionistic data make the strongest statements, sometimes of absolute certainty'. Thus, there is an opportunity for biometric researchers to collaborate with forensic experts and statisticians in assembling large forensic datasets (e.g. fingermarks) and analysing the reliability and validity of forensic procedures using automated methods.

Apart from this, there are operational scenarios where biometrics and forensics can come together to solve law enforcement problems of high importance. Two such operational applications are discussed below.

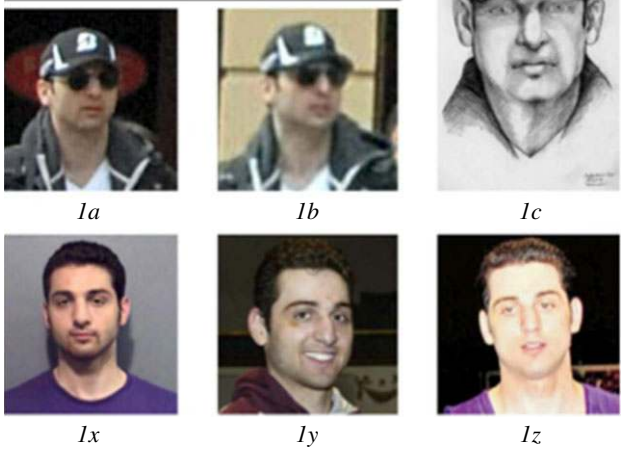
(a) Face recognition from surveillance videos

There are certain person recognition applications where it is very difficult to impose constraints on how the biometric trait should be acquired. A classic example of unconstrained sensing environment is video surveillance, where images are acquired using closed circuit television (CCTV) cameras that monitor public locations. Persistent video surveillance is deemed to be a successful deterrent against crime and, consequently, surveillance cameras have rapidly proliferated around the world, especially in large metropolitan areas. For example, it has been estimated that there are more than 1 million CCTV cameras in the city of London alone and around 4.9 million of them are spread across the UK [24]. Almost all the existing CCTV cameras in use are passive in nature in the sense that they merely record the video footage of the monitored location, and the archived video is analysed by human operators only after a crime has been committed and reported. Real-time video processing and recognition is seldom carried out either to predict or detect an incident or to identify the offender. The primary challenge in automated real-time video surveillance is how to detect 'persons of interest' in a video and then identify them using face recognition systems (also see [15]). Another related problem is person re-identification, where the objective is to track the same person as he/she passes through a network of CCTV cameras. Face recognition in surveillance applications is a very challenging problem due to the following two reasons:

(1) The poor quality of face images captured using CCTV cameras. Factors leading to this degradation in quality may include low spatial resolution of the camera, large distance between the subject and the camera, speed at which the subject is moving, illumination variations at the monitored location, and occlusion caused by other objects and people in the scene.
(2) Since the subject is not expected to be cooperative (not posing for face capture as in a mugshot scenario), there may be large pose and expression changes as well as occlusion of facial features due to the wearing of accessories like caps and sunglasses. In some cases, the subject may also intentionally hide his face from the camera to avoid detection.

(*a*)

Race: White
Gender: Male
Age: 20 to 30



1a *1b* *1c*

1x *1y* *1z*

(*b*) with demographic filtering (white male, 20–30)

	1a	*1b*	*1c*	mean
1x	5432	27 617	112	353
1y	518	25 780	1409	686
1z	3958	14 670	1142	1416
mean	424	5790	71	82

Figure 8. Importance of composite-to-photo matching if it were used in the Boston bombing investigation. (*a*) Here, *1a*, *1b* and *1c* are probe images while *1x*, *1y* and *1z* are gallery images of the older brother, Tamerlan Tsarnaev. (*b*) The table reports the rank at which the three gallery images of Tamerlan Tsarnaev match with his two probe images and the composite sketch. The use of the composite of Tamerlan Tsarnaev (*1c*) resulted in a better match with the gallery image (*1x*) than any of the probe images (*1a* and *1b*) released by the police. (Online version in colour.)

Despite the above challenges, significant progress has been achieved in unconstrained face recognition. This was demonstrated by Klontz & Jain [25], where the authors simulated the scenario of using face recognition to identify the suspects in the 2013 Boston Marathon bombings (figure 7). Three images each of the two suspects (the Tsarnaev brothers) were added to a background database of 1 million mugshot images provided by the Pinellas County Sheriff's Office (PCSO). These six images added to the gallery database included mugshots as well as face images of the brothers obtained from the social media. The images of the suspects extracted from surveillance cameras and released by the law enforcement were used as probe (query) images to search the gallery using two state-of-the-art face matchers. It was observed that one of the probe images of the younger brother (Dzhokhar Tsarnaev) matched correctly with his high-school graduation photograph included in the gallery [25]. However, due to issues such as pose, low resolution and occlusion (e.g. cap and sunglasses), the older brother (Tamerlan Tsarnaev) could not be successfully identified using the face matchers. This shows that large improvements in unconstrained face recognition accuracy would be required before 'lights-out' face recognition systems can be deployed in forensic applications that involve the utilization of surveillance data.

In a related experiment [26], when a *composite* of the older brother was generated from the surveillance video and used as the probe image, it was observed to match at a better rank with one of the gallery images of the subject (figure 8). This reiterates the importance of using surveillance composites generated by a forensic sketch artist in the context of unconstrained face recognition.

(b) Processing latent fingerprints

One of the most challenging problems in fingerprint recognition is comparing fingermarks to rolled/slap (reference) fingerprints. Comparison of fingermarks to reference prints by state-of-the-art AFIS does not typically yield satisfactory results. This is because many unknown fingermarks encountered in crime-scene investigations (i) are partial prints with relatively small friction ridge area, (ii) have poor contrast and clarity with significant distortion and (iii) have significant background noise [27]. Therefore, a fingerprint examiner is typically needed to manually mark features on a fingermark prior to submitting a query to an AFIS, and to subsequently review the top-K (usually $K = 20–50$) retrievals to determine if the unknown fingermark matches against a reference print [28].

The NIST ELFT-EFS 2 evaluation [29] reported that the likelihood of finding a match in the reference database improves when the query submitted to an AFIS has a markup. This performance gain, however, depends on the precision of the markup being input to the AFIS [30]. Imprecise markups can result in the corresponding reference print being returned at a lower rank amongst the retrieved candidates compared with when the image alone is input to the AFIS. Furthermore, markups for the same fingermark by different examiners can vary significantly [31,32]. To overcome the aforementioned limitations, it may be instructive to use a fingermark identification framework where AFIS and fingerprint examiners operate synergistically to improve the identification accuracy [28]. Such a framework is based on the following two conjectures. (i) Fingermarks that are of very good quality may not require a manual markup in order to be correctly identified; if this can be established *a priori*, fingerprint examiners can then devote more time to markup difficult fingermarks. (ii) Combining the markups of different examiners with the features extracted automatically can boost AFIS performance. The conjecture stems from the classical pattern recognition theory that, on average, a group of experts with diverse and complementary skills can collectively solve a difficult problem better than each individual expert.

5. Summary and future work

Automatic recognition of humans is an integral aspect of a multitude of daily transactions in our society. A number of

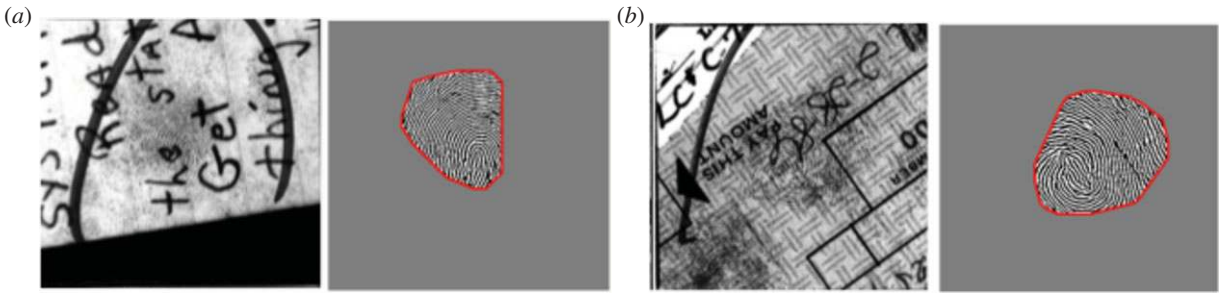


Figure 9. (*a*,*b*) Examples of two fingermarks that have been automatically enhanced using image processing techniques. Forensic experts can avail of the progress made in pattern recognition, computer vision, image processing and machine learning in order to assist in the 'identification' process where an item of evidence (in this case a fingermark) is associated with a source (i.e. an individual or a group of individuals). (Online version in colour.)

applications ranging from smartphone access to international border crossing depend on the use of authentication mechanisms to reliably identify an individual. Traditionally, ID cards and passwords have been used to verify the identity of an individual. But, the well-known shortcomings of such credentials (*what you carry* and *what you know*) has prompted the use of biological traits such as fingerprints to automatically and accurately recognize an individual. In this article, we first introduced biometrics and noted its origins in the forensic and law enforcement domain. Next, we discussed the similarities and differences between biometrics and forensics. We then presented some applications where the principles of biometrics are being successfully leveraged into forensics in order to solve critical problems in the law enforcement domain. Finally, we discussed new opportunities for researchers in biometrics and forensics to collaborate on, in order to address hitherto unsolved problems that can benefit society at large.

Although forensic science was one of the earliest applications of biometric recognition, biometric systems are yet to live up to their full potential in solving the problems faced by forensic experts. Biometric recognition can be used in forensics in two distinct ways: (i) as a tool to assist in investigation (figure 9) and (ii) to support evidence presented in a court of law. It is worth noting that these two use-cases have very different requirements. In the first case, the key requirements are the speed and accuracy of the biometric system under challenging data conditions. However, low levels of errors made by the system are tolerable in this scenario because the investigating officers can make use of other contextual information (e.g. age, gender and race of the suspect) to eliminate some of the errors. In the second scenario, the primary requirement is the scientific presentation of biometric evidence with strong statistical basis to a court of law. This in turn involves obtaining a reliable estimate of the *distinctiveness* of a biometric trait—a problem that is still unsolved in the context of biometric traits. Another related problem is the *persistence* of the biometric recognition accuracy that requires a longitudinal study of the biometric trait of interest.

One of the interesting developments in the intersection of forensics and biometrics is the advancements in real-time automated matching of DNA profiles. The current standard procedures for DNA profiling, namely polymerase chain reaction (PCR) and short tandem repeat (STR) analysis, have been in place for around two decades now. Since these procedures typically involve laboratory analysis by human operators, it may take up to several hours to obtain an STR profile from a buccal swab. However, prototype devices are now available for rapid DNA analysis. These devices fully automate the process of developing an STR profile from a reference buccal swab and have a response time of less than 2 h. In the near future, it may be possible to further speed up this process to a few minutes, thereby making DNA a feasible biometric modality even in applications other than forensics. However, one needs to be extremely cautious about the privacy issues associated with DNA-based biometric systems because the DNA samples (or templates) may contain a wealth of personal information (e.g. susceptibility to diseases). Further, issues of DNA contamination can lead to erroneous conclusions that can pre-empt the usefulness of this modality in unconstrained environments.

Finally, what can pattern recognition, machine learning and biometrics researchers bring to the forensics domain? We list four possibilities here. (i) New representations (features) extracted from forensic evidence: instead of storing a single encoding, say for fingerprints, we could generate multiple encodings. As large databases of forensic evidence become available, we could use new machine learning/pattern recognition tools such as deep networks (e.g. convolutional neural networks) to learn new representations that either may perform better than handcrafted features or could be used in conjunction with handcrafted representations to boost performance. State-of-the-art performance for unconstrained face recognition has already been achieved using convolutional neural networks. (ii) Design automated systems for forensic evidence (e.g. tool marks) that are still manually analysed by forensic scientists thereby being time consuming, costly and subjective. (iii) Use automated systems for 'triage': an automated system when presented with forensic evidence can be used to determine if a decision can be rendered in the 'lights-out' mode with no human intervention, if a forensic expert is needed to visually assess the data, or if the evidence is non-informative. (iv) Developing probabilistic models for defining uncertainty in decisions rendered by automated systems or for describing the strength of the forensic evidence [33]. This would entail analysing large databases of forensic evidence in order to glean statistically significant conclusions.

Competing interests. We declare we have no competing interests.

Funding. We received no funding for this study.

Acknowledgements. The authors are grateful to Dr Didier Meuwly, Dr Ruth Smith and Dr James Wayman for their careful reading of the manuscript and for providing valuable edits and comments. The authors also thank Dr Karthik Nandakumar and members of the PRIP Lab at Michigan State University for their assistance in preparing this manuscript.

References

1. Jain AK, Ross A, Nandakumar K. 2011 *Introduction to biometrics: a textbook*. Berlin, Germany: Springer.
2. Gelb A, Clark J. 2013 Identification for development: the biometrics revolution. Technical report 315. Washington, DC: Center for Global Development.
3. Trauring M. 1963 On the automatic comparison of finger ridge patterns. *Nature* **197**, 938–940. (doi:10.1038/197938a0)
4. Pruzansky S. 1963 Pattern-matching procedure for automatic talker recognition. *J. Acoust. Soc. Am.* **35**, 354–358. (doi:10.1121/1.1918467)
5. Bledsoe WW. 1966 Man-machine facial recognition. Technical report PRI 22. Panoramic Research, Inc.
6. Mauceri AJ. 1965 Feasibility study of personal identification by signature verification. Technical report SID65–24. North American Aviation.
7. Ernst RH. 1971 Hand ID System. United States patent number US 3576537.
8. Daugman JG. 2003 The importance of being random: statistical principles of iris recognition. *Pattern Recognit.* **36**, 279–291. (doi:10.1016/S0031-3203(02)00030-4)
9. Spearman E. 1999 Identifying Suspects, 1894. In *Crime and punishment in England: a sourcebook* (eds A Barrett, C Harrison), pp. 256–257. London, UK: UCL Press.
10. Bertillon A. 1896 *Signaletic instructions including the theory and practice of anthropometrical identification*. (Transl. RW McClaughry). New York, NY: The Werner Company.
11. Galton F. 1892 *Finger prints*. London, UK: McMillan & Co.
12. Hawthorne MR. 2009 *Fingerprints: analysis and understanding*. Boca Raton, FL: CRC Press.
13. Kirk P. 1953 *Crime investigation: physical evidence and the police laboratory*. New York, NY: John Wiley & Sons.
14. Taroni F, Champod C, Margot P. 1998 Forerunners of bayesianism in early forensic science. *Jurimetrics* **38**, 183–200.
15. Meuwly D, Veldhuis R. 2012 Forensic biometrics: from two communities to one discipline. In *Proc. Int. Conf. of the Biometrics Special Interest Group* (*BIOSIG*), *Darmstadt, Germany, 6–7 September 2012*. IEEE.
16. Kassin SM, Dror IE, Kukucka J. 2013 The forensic confirmation bias: problems, perspectives, and proposed solutions. *J. Appl. Res. Mem. Cognit.* **2**, 42–52. (doi:10.1016/j.jarmac.2013.01.001)
17. Jain AK, Klare B, Park U. 2012 Face matching and retrieval in forensics applications. *IEEE Multimedia* **19**, 20–28. (doi:10.1109/MMUL.2012.4)
18. McQuiston-Surrett D, Topp L, Malpass R. 2006 Use of facial composite systems in US law enforcement agencies. *Psychol. Crime Law* **12**, 505–517. (doi:10.1080/10683160500254904)
19. Lee J-E, Tong W, Jin R, Jain AK. 2012 Image retrieval in forensics: tattoo image database application. *IEEE Multimedia* **19**, 40–49. (doi:10.1109/MMUL.2011.59)
20. National Research Council of the National Academies. 2009 *Strengthening forensic science in the United States: a path forward*. Washington, DC: National Academies Press.
21. Eckholm E. 2014 Mississippi death row case faults bite-mark forensics. *New York Times*, 15 September 2014.
22. Mnookin JL *et al.* 2011 The need for a research culture in the forensic sciences. *UCLA Law Rev.* **58**, 725–779.
23. Thornton J, Peterson J. 2002 The general assumptions and rationale of forensic identification. In *Modern scientific evidence: the law and science of expert testimony*, vol. 34. Eagan, MN: West Publishing Company.
24. Barrett D. 2013 One surveillance camera for every 11 people in Britain, says CCTV survey. *The Telegraph, July 2013*.
25. Klontz JC, Jain AK. 2013 A case study of automated face recognition: the Boston marathon bombing suspects. *IEEE Computer* **46**, 91–94. (doi:10.1109/MC.2013.377)
26. Best-Rowden L, Han H, Otto C, Klare B, Jain AK. 2014 Unconstrained face recognition: identifying a person of interest from a media collection. *IEEE Trans. Inf. Forensics Secur.* **9**, 2144–2157. (doi:10.1109/TIFS.2014.2359577)
27. Jain AK, Feng J. 2011 Latent fingerprint matching. *IEEE Trans. Pattern Anal. Mach. Intell.* **33**, 88–100. (doi:10.1109/TPAMI.2010.59)
28. Arora SS, Cao K, Jain AK, Michaud G. 2015 Crowd powered latent fingerprint identification: fusing AFIS with examiner markups. In *Proc. of Int. Conf. on Biometrics, Phuket, Thailand, 19–22 May 2015*. See http://biometrics.cse.msu.edu/Publications/Fingerprint/AroraCaoJainMichaud_CrowdPoweredLatentIdentification_ICB15.pdf.
29. Indovina M, Dvornychenko V, Hicklin R, Kiebuzinski G. 2012 ELFT-EFS evaluation of latent fingerprint technologies: extended feature sets [evaluation#2]. NISTIR, 7859.
30. Indovina M, Hicklin R, Kiebuzinski G. 2011 ELFT-EFS evaluation of latent fingerprint technologies: extended feature sets [evaluation# 1]. NISTIR, 7775.
31. Dror IE, Wertheim K, Fraser-Mackenzie P, Walajtys J. 2012 The impact of human–technology cooperation and distributed cognition in forensic science: biasing effects of AFIS contextual information on human experts. *J. Forensic Sci.* **57**, 343–352. (doi:10.1111/j.1556-4029.2011.02013.x)
32. Ulery BT, Hicklin RA, Buscaglia J, Roberts MA. 2012 Repeatability and reproducibility of decisions by latent fingerprint examiners. *PLoS ONE* **7**, e32800. (doi:10.1371/journal.pone.0032800)
33. Neumann C, Evett IW, Skerrett J. 2012 Quantifying the weight of evidence from a forensic fingerprint comparison: a new paradigm. *J. R. Stat. Soc. A* 371–415. (doi:10.1111/j.1467-985X.2011.01027.x)