**Published paper**
Allinson, N.M., Sivarajah, J., Gledhill, I., Carling, M. and Allinson, L.J. (2007) *Robust wireless transmission of compressed latent fingerprint images* IEEE Transactions on Information Forensics and Security, Volume 2 (3, Part 1), 331 – 340.

---

# Robust Wireless Transmission of Compressed Latent Fingerprint Images

Nigel M. Allinson, *Member, IEEE*, Jeevandra Sivarajah, Ian Gledhill, Michael Carling, and Lesley J. Allinson

***Abstract*—Maximizing the potential of latent fingerprints from crime scenes in the identification of suspects requires the rapid transfer of the latent from the scene to a remote fingerprint bureau. Transmission over restricted-bandwidth cellular wireless networks requires the latent images to be compressed but without compromising the likelihood of a match being achieved. We present details of experiments to establish the optimum form of compression that provides realistic transmission times and yet does not affect the utility and integrity of the U.K. Fingerprint Service in searching for latent identifications and in archiving unidentified latents on the U.K. national automatic fingerprint identification system (AFIS). Practical aspects of the implemented system, especially in respect to communication and security protocols, are outlined. Finally, we give some details of the operational advantages of this system as it begins to be employed across U.K. police forces.**

***Index Terms*—Fingerprint identification, forensic techniques, image coding, wireless networks.**

## I. INTRODUCTION

THE use of an individual's fingerprints as a means of identification was first considered in the mid-19th century by British administrators working in India. They wished to exploit a simple procedure to combat, what we would now call "identity theft," such concerns as pension entitlement and land ownership. Recovering the residual traces of fingerprints from crime scenes was first applied toward the end of that century by John Faulds [1]. The U.K. Metropolitan Police set up the first fingerprint bureau in 1901 and the first conviction, for burglary, on fingerprint evidence was obtained the following year. The steady growth of fingerprint records made manual searching untenable and there were several early attempts during the 1960s and 1970s to exploit mainframe computer systems. The Royal Canadian Mounted Police commenced operation of the first automatic fingerprint-identification system (AFIS) in 1977, with the U.K. Metropolitan Police following soon afterwards. A short history of the development of AFISs is given in [2]. The vast majority of police authorities across the world use AFIS technology to assist in identifying fingerprint latents.[1] The U.S. Federal Bureau of Investigation (FBI) AFIS holds fingerprint and other records for more than 47 million subjects. The smaller U.K. national AFIS[2] contains details of more than seven million individuals in the form of ten print (TP) records (TPs are the reference set of all digits recorded as slaps and rolls and retained as images and minutiae vectors) and, at any one time, approximately one million unidentified marks (MK) or latents.

TABLE I
TYPICAL REQUIRED RESPONSE SCENARIO

| | |
|---|---|
| 3 am | Burglary occurs |
| 7 am | Burglary reported to Police |
| 9 am | CSE attends scene and commences search |
| 10 am | Fingerprint lift arrives at Bureau |
| 12 am | Identification sent to Operational Division and suspect sought |

Normal practice would be for a crime to be reported and, if appropriate, a crime scene examiner (CSE) would visit the scene to collect any forensic evidence. Though a range of fingerprint recovery techniques exist, most are recovered through dusting with fine aluminum powder and the print lifted onto clear adhesive tape. This tape is then secured to a thin acetate sheet to protect the impression—called a lift. Extensive details on the wealth of fingerprint recovery techniques are provided in [3]. For nonserious and volume crimes, for example, thefts from vehicles and properties, CSEs would normally visit several scenes during their working day and the lifts would not be returned to the fingerprint bureau until the end of the day or even later.

It is well recognized that an excessive delay in transporting lifts back to a bureau would adversely affect the likelihood of apprehending a suspect. For one U.K. Police Force surveyed, the average time to transport a lift to its bureau was three days even though the average response time for a CSE to attend a crime scene was only 3 h. What was required was a same-day response, along the lines of the scenario outlined in Table I.

To meet these time restraints, it is necessary, certainly for a force with jurisdiction over large rural areas, to transmit lift images directly from the crime scene using commercial cellular wireless networks. These networks provide in the U.K. more than 86% and 99% coverage of the U.K. land mass and its population, respectively. The population coverage figure is probably

Manuscript received September 15, 2006; revised May 4, 2007. This work was supported by the UK Home Office. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Davide Maltoni.

N. M. Allinson and J. Sivarajah are with the Department of Electronic and Electrical Engineering, University of Sheffield, Sheffield S1 3JD, U.K. (e-mail: n.allinson@sheffield.ac.uk; j.sivarajah@sheffield.ac.uk).

I. Gledhill and M. Carling are with the Lincolnshire Police, Lincoln, LN5 7PH, U.K. (e-mail: ian.gledhill@lincs.pnn.police.uk; mick.carling@lincs.pnn.police.uk).

L. J. Allinson is with the Department of Psychology, University of Lincoln, Lincoln LN6 7TS, U.K. (e-mail: lallinson@lincoln.ac.uk).

Digital Object Identifier 10.1109/TIFS.2007.902684

---

[1] "Latent" is the term used in the U.S. and other countries to denote fingerprint impressions lifted from crime scenes as opposed to inked prints obtained directly from a subject. In the U.K., the term "mark" is employed.

[2] The UK national system was called "NAFIS" but following a major refurbishment in 2005, it was renamed "Ident 1." Though this occurred during the period of the work described here, the operating procedures and, more important, the search algorithms used were unaltered. We will use the name NAFIS throughout to avoid confusion.

more relevant to the crime scene location than land mass. The current U.K. Emergency Services cellular network Airwaves was designed for secure voice communication and possesses very limited bandwidth for data transmission (typically 3 kb/s). Lifts are scanned at a standard 500 dpi with 8-b grayscale. A typical latent image would yield a 1.5–3.0-MB file on average more than when a single digit is recorded. Practical data rates using second-generation general-packet radio service (GPRS) networks are in the range of 20–45 kb/s. This equates to transmit times of 4–20 min, which is obviously not practical especially as a single crime scene may yield multiple latents. In order to achieve realistic transmission times, lossy image compression is required with the essential proviso that such compression must not reduce the possibility of obtaining a positive identification by a bureau-based latent fingerprint examiner (LFE).

This paper describes experiments undertaken to determine the optimum image compression technique as well as the realization of a secure and robust system for transferring latent images using commercial networks. Our approach is unusual in that, unlike other studies on fingerprint compression, we had the opportunity to conduct our tests using latents recovered from crime scenes with the corresponding TPs present on NAFIS and for which a match had been obtained previously. This provides ground truth verification. Section II provides a brief introduction to the latent fingerprint identification procedures that are relevant to this work. Section III outlines image compression options, previous work on fingerprint image compression, and our initial studies in selecting appropriate compression standards. Section IV describes the remote transfer system with special reference to security issues. Section V describes experiments 1) to determine the effectiveness of the system over an extended trial covering a single police force and 2) to determine the validity in retaining unidentified latents on NAFIS in only compressed form. Section VI illustrates the value of the system through both summaries of overall effectiveness and a specific case history and, finally, Section VII offers a brief conclusion.

## II. LATENT FINGERPRINT IDENTIFICATION

### A. *Fingerprint Classification*

Fingerprints are classified first in terms of the general form of the ridge and valley appearance (Level 1 detail) and second, in terms of the occurrence, location, and direction of various minutiae (Level 2 detail). At Level 1, the fingerprint pattern reveals regions where the ridge lines assume distinctive shapes of which four named examples are shown in Fig. 1 and most current classifications are still based on Henry's original scheme [4]. The identification based solely on a limited number of Level 1 classes is clearly not feasible, so the examination of Level 2 detail is necessary. At Level 2, the distinguishing features are the various ways the individual ridges are discontinuous. These minutiae, of which a few common forms are represented diagrammatically in Fig. 2, have been classified in several ways. The ANSI standard [5] proposes a taxonomy based on four classes—terminations, bifurcations, compound (crossovers), and undetermined. Some experts have suggested up to 150 different minutiae variations [6], though most LFEs can probably identify, at most, about 20 types. Most current AFIS algorithms only identify and exploit terminations and bifurcations. Details of NAFIS or, indeed, AFIS systems, in general, are not of concern to this study. What is important is that any developed scheme has to be compatible with existing identification processes, including NAFIS and, above all, not compromise the ability to make identifications. Some aspects of current AFIS systems are provided in [7] and [8]; however, it should be noted that details of image data enhancement and filtering, feature detection, and search algorithms employed in AFIS systems are generally commercially confidential.

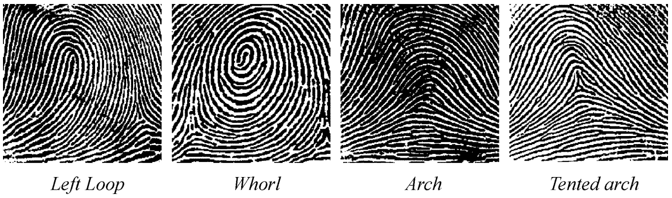


Fig. 1. Examples of Level 1 fingerprint descriptors. Adapted from [5].

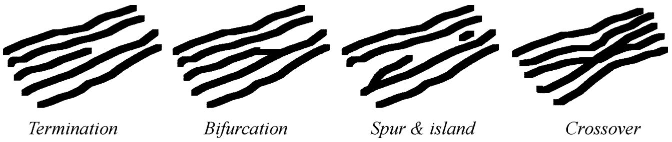


Fig. 2. Examples of Level 2 fingerprint descriptors (minutiae).

### B. *Outline of Identification Process*

The LFE will first make a judgment on the overall quality of the latent as to whether it is worth proceeding with a search. The latent lift is scanned and the resulting image entered into NAFIS as an unidentified MK. The image is rotated and cropped by the LFE, to ensure that the fingerprint region is only retained and is at approximately the correct orientation. NAFIS then processes the image and labels the various minutiae. The LFE inspects the results and will delete marked minutiae they are not satisfied are correct, and may add additional ones of their own. They will also indicate, if possible, the specific finger corresponding to the MK. A search is then launched at the local, regional, or national level. The system returns an ordered list (typically 15 items) of TPs ranked in terms of their auto-encode score. This score is a measure of the similarity between the MK and each recovered TP, and is a function of the number, distribution, type, and strength of the corresponding minutiae. Its detailed formulation is commercially confidential. The LFE inspects, pairwise, the submitted MK image and each returned TP image in turn; and it is they who make the decision on a match and not NAFIS. If no match is located in the first list, then the next set of ordered matches can be inspected. A positive identification is based on the proficiency and skill of the individual examiner. An earlier legal standard of proof based on a threshold number of corresponding points (e.g., minutiae) has been abandoned in many countries. The U.S. discarded this approach in 1973 and the U.K. in 2001 (though Scotland retained a 16-point comparison standard until 2006). This outlines the normal process of identifying a latent and is referred to as a mark/ten-print (MK/TP) search. Other search types are regularly undertaken, for example, from a known individual's TP on

NAFIS to the database of unidentified latents—a TP/MK search. What is important is that ground truth as to whether identification is made rests with the human expert and is not determined by the AFIS system whose primary function is to act as a search engine. The suitability of any image compression scheme needs to be considered in its effect on potential identifications by an expert LFE and its effect on searching by an AFIS.

As the criminal justice system differs from country to country, a short note of U.K. practice in relation to how fingerprint evidence is employed in criminal prosecutions and in the courts is appropriate. The identification of a suspect can be made on the basis of a fingerprint match, and this suspect's details would then be released to the relevant police operational division and the suspect could be subsequently arrested on this identification. The justification for arrest is that reasonable grounds exist that a suspect has committed an offense. The arrestee may later be charged when there are reasonable grounds that a successful prosecution can be obtained. Individuals may be arrested but no charge may be subsequently brought. All of these procedures are described in the codes of practice that form part of the U.K. Police and Criminal Evidence Act (PACE): 1984 [9]. Prior to charging, all evidence would be reassessed, including fingerprints, and reference would be made to the physical lifts. If the case progresses to court, the appropriate fingerprint officer would present his or her reasons for positive identification and the physical lifts would be entered as evidence.

## III. LATENT IMAGE COMPRESSION

### *A. Previous Image Compression Studies*

To achieve the necessary reduction in transmission time, the image coding will have to be lossy. Most studies on the compression of fingerprint images have been concerned with the requirement to reduce the overall memory requirements of very large databases of TPs rather than much poorer and variable quality latents. In our case, we are constrained by the overriding need to be congruent with existing systems. Compression standards for which software-based codecs exist within NAFIS are JPEG, JPEG2000 and WSQ. JPEG [10], being a block-based DCT approach, suffers from visible blocking artifacts and loss of fine details (e.g., ridge pores) even at relatively low compression rates for fingerprint images. Though the unsuitability of JPEG compression has been known for some time [11], it is still employed in some systems. Wide-area AFIS systems with fixed connections to remote terminals often employ such compression to return TP images of potential matches to bueaux. For example, NAFIS displays images of returned TPs as 12:1 JPEGs (reference images are archived in lossless JPEG format). Wavelet scalar quantization (WSQ) was developed by the FBI, Los Alamos National Laboratory, and the National Institute of Standards Technology (NIST) specifically to reduce the media storage requirements of the FBI's expanding AFIS facility by providing lossy compression over the range 10:1 to 20:1 [12]. Documentation of the WSQ standard is available at [13].

Both WSQ and JPEG2000 schemes are based around wavelet transforms, but with major differences in the form of the decomposition tree, quantization, and entropy coding employed. The WSQ uses the Daubechies (9,7) filter [14] and the same filter is the default in the irreversible JPEG2000 transform. The JPEG2000 employs a dyadic decomposition tree based on Mallat's original scheme [15], while WSQ employs a fixed structure with a larger number of sub-bands (Fig. 3). The greater decomposition structure of WSQ may enhance compression as it approximates orthnormalization [16]. The decomposition structure will influence the number of length of the zero coding runs, while the bit-plane scanning order of JPEG2000 permits finer control to achieve an arbitrarily specified compression rate. Both schemes use scalar quantization with JPEG2000 having the quantization step varying in response to the dynamic range of the respective sub-band. While for WSQ, all quantizer steps are uniform except for a lengthened middle interval. For the last coding step, WSQ employs Huffman entropy coding while JPEG2000 uses arithmetic coding. The WSQ coding table is calculated for each image and the coefficients are included in the file header.

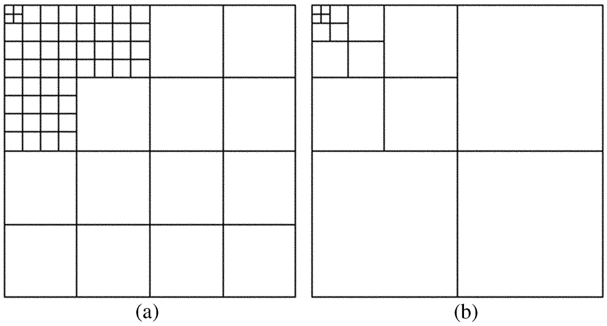
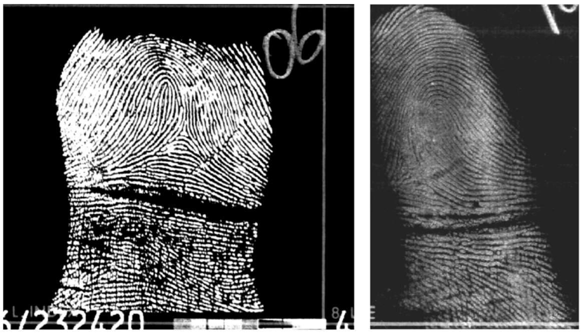


Fig. 3. Schematics of decomposition trees. (a) WSQ. (b) Mallat.

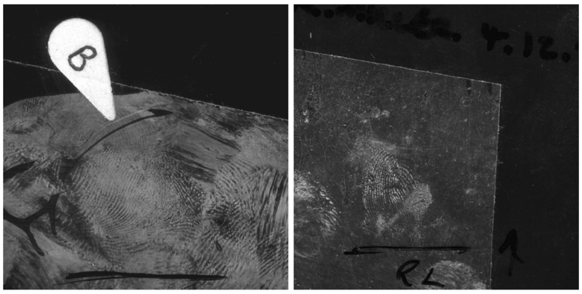
There have been a limited number of studies comparing the relative merits of WSQ and JPEG2000 for compressing fingerprint images. Most of this work has focused on coding high-quality inked prints or live print capture, and not poorer quality latents. Reference [17] showed a significant improvement for JPEG2000 over WSQ (at 0.75 bpp or 10.7:1 compression) in terms of peak signal-to-noise ratio (PSNR) and receiver operating curves (ROCs) for different sources—namely, capacitive sensor, optical sensor, and scanned inked prints. A study of JPEG2000 and WSQ interoperability [18] concluded that JPEG2000 produced a slightly lower quality reconstructed image compared to WSQ for the same file size. Compression ratios were in the range of 11.0:1 to 17.2:1, and the metrics employed were PSNR and image-quality metric (IQM) [19]. Current ISO/IEC standards on information technology—biometric data interchange formats [20] recommend WSQ for 500-dpi fingerprint images with compression limited to 15:1, but for images with greater than 500 dpi, it recommends JPEG 2000 at 15:1. As far as the authors are aware, no study had been undertaken on the effects of image compression on identification rates using an operational AFIS system.

### *B. Evaluation of Optimum Image Compression*

Experiments using representative latent test sets, in terms of subjective image quality (judged by experienced LFEs), were conducted to determine a preferred compression technique and corresponding compression ratio. The test sets were: 1)



(a) FBI/NIST test set



(b) HOSDB test set

Fig. 4. Example uncropped latents from test sets.

a 19-image set created by FBI/NIST and 2) a 12–image set created by the U.K. Home Office Scientific Development Branch (HOSDB). The HOSDB set was of generally poorer image quality and more representative of latents recovered from crime scenes. This set had the additional advantage that the corresponding TP records existed on NAFIS so a ground truth search was possible. Typical examples from each set are shown in Fig. 4. All original images were uncompressed RAW/TIFF formats at 500 dpi and 8-b gray scale. The JPEG2000 codec employed was an integration of the JJ2000 Java reference implementation [21] with the core coding system conforming to the ISO/IEC 15444– 1 specification [22]. The WSQ codec was an integration of the NIST release [23] of the FBI's WSQ encoder and decoder.

A summary of the PSNR of the compressed images is given in Table II. The PSNR for an 8-b image is defined as $\mathrm{PSNR} = 20\log_{10}(255/e_{\mathrm{mse}})$ where the mean square error ($e_{\mathrm{mse}}$) is given by

$$e_{\mathrm{mse}} = \frac{1}{MN}\sum_{m=1}\sum_{n=1}[u(m,n) - v(m,n)]^2$$

where $u(\bullet)$ and $v(\bullet)$ are the original and compressed images, respectively, each of size $M \times N$ pixels.

Higher PSNR means less distortion with no distortion equating to a $\mathrm{PSNR} = 48.13$ dB.

JPEG2000 performs consistently better than WSQ, which, in turn, performs better than JPEG. It is not always possible to produce highly compressed JPEGs due to the relatively large magnitude of its base image representation. The FBI/NIST images are of higher quality so their PSNR falls faster as compression is increased than for the poorer quality PSDB set. This is to be expected as the HOSDB images contain a smaller contribution of high spatial frequency components. Compressing a poor quality lift does not make it relatively more distorted than a higher quality lift. The PSNR does provide a reliable and simple method for comparing images but only if they possess similar content. The limitations of JPEG for fingerprint compression have been mentioned previously, and the comparative images of the same $64 \times 64$ pixel region in Fig. 5 indicate that JPEG blocking artifacts are clearly visible at 32:1 compression. The JPEG compression option is not considered further.

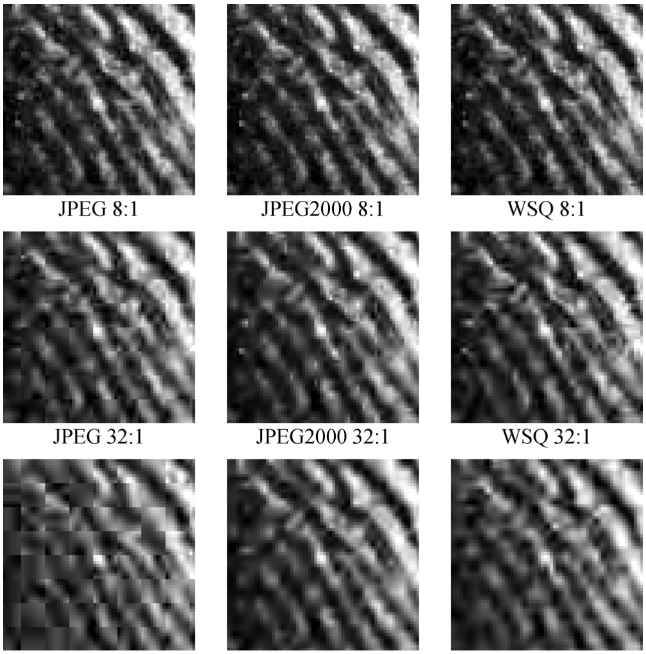
TABLE II
TEST SET PEAK SIGNAL-TO-NOISE RATIO (PSNR) FOR DIFFERENT COMPRESSION TYPES

FBI/NIST Set

| | Mean PSNR (± SD) dB | | | | |
|---|---|---|---|---|---|
| Comp. Ratio | 8:1 | 16:1 | 32:1 | 64:1 | 128:1 |
| bpp | 1.0 | 0.5 | 0.25 | 0.125 | 0.063 |
| JPEG2000 | 37.52<br>( 5.21) | 30.62<br>( 4.68) | 26.23<br>( 4.23) | 22.56<br>( 3.49) | 19.97<br>( 2.88) |
| WSQ | 35.19<br>( 4.78) | 28.94<br>( 4.47) | 24.68<br>( 3.78) | 21.40<br>( 3.14) | 18.93<br>( 2.62) |
| JPEG | 32.88<br>( 4.98) | 25.21<br>( 3.64) | 21.99<br>( 3.06) | 19.56<br>( 1.90) | |

HOSDB SET

| | Mean PSNR (± SD) dB | | | | |
|---|---|---|---|---|---|
| Comp. Ratio | 8:1 | 16:1 | 32:1 | 64:1 | 128:1 |
| bpp | 1.0 | 0.5 | 0.25 | 0.125 | 0.063 |
| JPEG2000 | 38.87<br>( 2.58) | 35.02<br>( 3.09) | 32.51<br>( 3.26) | 30.62<br>( 3.53) | 29.14<br>( 3.17) |
| WSQ | 36.99<br>( 2.22) | 34.05<br>( 2.42) | 31.36<br>( 2.34) | 29.96<br>( 2.77) | 28.20<br>( 3.08) |
| JPEG | 36.17<br>( 2.70) | 33.37<br>( 2.89) | 30.65<br>( 2.81) | 29.14<br>( 3.17) | 24.69<br>( 2.75) |



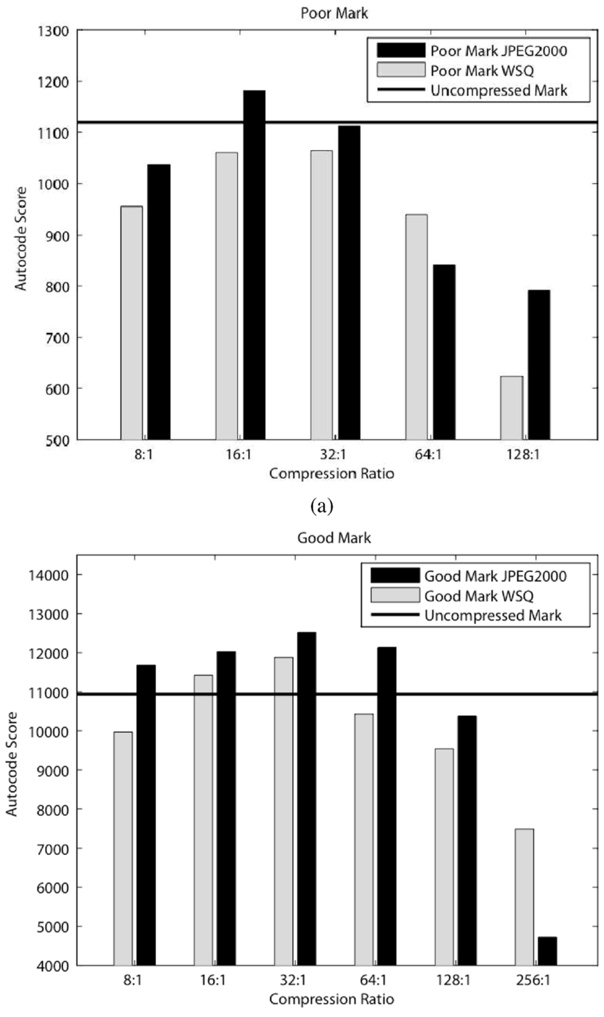
JPEG 8:1 JPEG2000 8:1 WSQ 8:1
JPEG 32:1 JPEG2000 32:1 WSQ 32:1
JPEG 64:1 JPEG2000 64:1 WSQ 64:1

Fig. 5. Comparative compressed images of $64 \times 64$ pixel region from HOSDB Image 41. Contrast has been stretched to increase visibility.

Discussions with LFEs suggested that they could operate normally to mark-up and manually compare latent images that had been subject to heavy compression—up to about 64:1 WSQ and

TABLE III
SUMMARY OF NAFIS SEARCH RESULTS FOR COMPARATIVE JPEG2000/WSQ COMPRESSION

| Comp. Ratio | Auto-encode range | | Ranking range | | Ident. Percentage | |
|---|---|---|---|---|---|---|
| | JPEG2000 | WSQ | JPEG2000 | WSQ | JPEG2000 | WSQ |
| 1:1 | 1145-11643 | | 1-3 | | 83 | |
| 8:1 | 978-121036 | 959-10496 | 1-4 | 1-5 | 83 | 79 |
| 16:1 | 1116-12708 | 994-12006 | 1-8 | 1-9 | 88 | 75 |
| 32:1 | 975-12728 | 838-121987 | 1-22 | 1-11 | 88 | 79 |
| 64:1 | 776-12361 | 816-10793 | 1-30 | 1-45 | 54 | 58 |
| 128:1 | 543-10348 | 710-9873 | 1-42 | 1-67 | 38 | 29 |



(a)

(b)

Fig. 6. Autoencode scores for typical poor- and good-quality latents as a function of JPEG2000 and WSQ compression ratios.

JPEG2000. Blind testing confirmed that they were unaware of any visual difference of compressed images to uncompressed ones up to about a 24:1 ratio. What was more important was the ability of NAFIS to perform satisfactorily, primarily in its search function, with compressed images. A series of trials was conducted with experienced LFEs with the HOSDB test set and other latent images. An LFE would align and crop the selected image in the normal manner and then submit to NAFIS for a full national search. There was no attempt by the examiner to modify the automatically generated minutiae marks. The returned autoencode score and rank position (if available) were recorded for a range of WSQ and JPEG2000 compression ratios. A summary of results is given in Table III. For compression ratios less than 32:1, JPEG2000 consistently produced higher ident rates than WSQ.

TABLE IV
PAIRED $t$-TEST SUMMARY STATISTICS FOR COMPARATIVE MK/TP NAFIS SEARCHES.

| | | NAFIS auto-encode score | | | |
|---|---|---|---|---|---|
| | N | Min. | Max. | Mean | SD |
| TIFF | 9 | 857.007 | 1203.00 | 1054.11 | 118.46 |
| JPEG2000 | 10 | 874.00 | 1398.00 | 1099.00 | 141.42 |
| Paired Sample Correlation, r = 0.729 | | | | p = 0.026 | |

Additional findings from these studies were as follows.

- For about 60% of latents, moderately compressed images provided higher autoencode scores then their corresponding uncompressed image. Fig. 6 shows typical plots for a poor and a good quality latent image. Increased AFIS coding scores had been observed previously for WSQ compression in a study of one-to-one fingerprint matching [24].
- If an uncompressed latent was identified (i.e., ranked), it remained ranked to at least 64:1 compression though the rank number may increase rapidly at higher compression ratios (i.e., beyond the ranking range that would normally be considered during routine searches).
- A few latents, about 16%, that were not identified from their uncompressed image were ranked (sometimes in first position) for moderate levels of compression.

These investigations confirm that JPEG2000 coding is superior to WSQ primarily in terms of ident rate for moderate levels of compression. For the ensuring system development and application, a compression ratio of 16:1 was employed as meeting the requirements of reducing transmission time per latent to a realistic 20–80 s, providing the highest ident rate if the ranking range was truncated at the normal limit of searching and providing no visual clues to the LFE as to the nature of the image format.

The ground truth for the acceptability of any compression scheme is that it does not affect the likelihood of a positive ident being obtained following standard operating procedures. Several studies, with different LFEs and test sets, were undertaken to confirm the suitability of 16:1 JPEG2000 compression in the normal operating environment. Individual LFEs, following standard working procedures, marked up latents in both uncompressed TIFF and 16:1 JPEG2000 formats and launched national searches on NAFIS. The results of a typical study are summarized in Table IV, where ten cases produced positive idents. A paired $t$ test applied to those lifts where there was an autoencoding score for image format pairs, indicating that the JPEG2000 format yields a higher score than the WSQ format $r = 0.729, p < 0.05$.

## IV. SYSTEM DESCRIPTION

The system is essentially an interlink that brings together the postmanual acquisition of lifts at a crime scene with their presubmission of their electronic representation for the use on the bureau-based AFIS. In general, it incorporates the common activities users would be familiar with in acquiring and transferring electronic images via e-mails. However, it is underlined by solutions designed to address the demands and constraints attributed with this process, including the efficient use of low bandwidth, maintaining image quality, and providing secure and reliable transfer across the public networks.

The software is comprised of five main parts; namely: 1) the graphical user interface (GUI); 2) image capturing; 3) image compression; 4) file security; and 5) e-mail transfer.

The user interface is kept simple to take ergonomic factors into account as often the CSE will need to operate in a constrained environment (e.g., inside vehicles). Software functionality follows an identified path flow where, from the click of a button, the user is taken through successive processes of scanning lifts, completing an incident form that includes the specific exhibit and crime scene details (forms are customizable to suit different force requirements), compressing the image, composing an e-mail, securing the e–mail attachments with cryptographic protection, and, finally, launching the e-mail.

Image capture employs a generic device driver that interfaces with any device, typically a flatbed scanner, which supports the TWAIN interface standard [25]. The software supports the encoding and decoding of images in various formats, including JPEG, TIFF, JPEG2000, and WSQ; all with codecs meeting their relevant reference standards. Options as to which codec is available and at what compression ratio can only be changed by an administrator. Under normal use, the CSE is restricted to 16:1 JEP2000 compression.

The system's security module is based on the well-known public-key infrastructure (PKI) scheme [26]. This system is essentially for the management of public-key cryptography which allows users to be authenticated to each other and to use the information in identity certificates (i.e., each other's public and private keys) to encrypt and decrypt transmitted information. Each user is associated with a keystore based on the personal information exchange syntax standard (PKCS#12) [27] which defines the file format of the infrastructure used to store private keys with their accompanying public-key certificates. Each user is bound to a private key and its corresponding public certificate in his or her own keystore and also, in some cases, to a shared private key and its corresponding public certificate if the user is part of a workgroup that is considered as a shared identity by other users interacting with the workgroup. These keystore entries are password protected; hence, the password also plays a role in the system's login access. Unsuccessful attempts during login to the system also defeats the loading and availability of all cryptography keys that are essential in identifying the user and facilitating secure interactions with other users. Apart from the user-associated keystore, each user possesses his or her own peer keystore which is the infrastructure to hold all public-key certificates of other users that the individual user could interact with through the system.

The implemented PKI does not involve third-party vetting of and vouching for user identities. The role of this third-party certificate authority is not seen as essential because the information exchanged through the system is not intended for distribution to any party in the public domain and is confined to a group of identified users. The management of identity certificates among this circle of users is intended to be carried out centrally where an administrator is responsible for collecting and distributing public certificates among the users involved. However, the software eases the exchange of public certificates with implemented import and export features using the XML format. The use of the XML format also provides a means for future developments where the need for interfacing the system with external systems, such as database web-based services, is to facilitate a more efficient way of managing and distributing public certificates. The exchange of confidential private keys is secured with password-based encryption.

In the current system, interactions with other users are carried out primarily through the use of e-mail. The e-mail client is based on Sun's JavaMail framework and supports SMTP and POP3 protocols. Attached fingerprint files are either sent as unencrypted with an attached signature file or, if necessary, they can be further secured with encryption. The former involves the generation of a digital signature using the SHA-1 algorithm [28] and the digital encryption of this signature using pretty good privacy (PGP) [29], employing the sender's private key. This does not prevent the file from being viewed by a third party, but using the sender's public key at the recipient's host confirms that file content has not been altered. To prevent third-party viewing of the file, the sender can further opt to encrypt the image files with PGP, employing the CAST-5 [30] cipher and this involves the public key of the recipient. At the recipient's end, the recipient will need to employ his or her private key to decrypt the file.

## V. IMPLEMENTATION EXPERIMENTS

### A. Force-Wide Trials

Radically changing a critical aspect of the way forensic fingerprint evidence is processed necessitates extreme caution before adoption on a countrywide basis. As there was no reduction in the ident rates achieved using compressed images from a series of small-scale experiments, it was agreed to conduct an extended large-scale live trial that followed normal operating practice. This was executed over a nine-month period within the Lincolnshire Police. This force is one of the smaller English forces with 26 CSEs who cover the second largest English county (approximately 7000 $\mathrm{km}^2$). It also has its own fingerprint bureau with 10 LFEs who provide 16 h cover per day and is situated at the Force's headquarters. CSEs were supplied with a laptop with the capture/transmission software installed, an integral GPRS wireless card, and a flatbed scanner (Fig. 7); they were also given initial training in the use of the system and provided with ongoing technical and other support. The suitability of the scanner, in terms of accuracy in reproducing latent images, was confirmed through a series of investigations by HOSDB. The lifts were taken in the normal manner. The period of study occurred when the system for electronic transfer was being gradually rolled out across the force, so individual CSEs had to transport the lifts to the bureau by road where they would be scanned by bureau staff, or to scan lifts at the crime scene and transmit them directly to the bureau as 16:1 JPEG2000 files. The collated results at the end of this trial period are given in

Fig. 7. Prototype latent scanning/wireless transmission system in use by a CSE.

TABLE V
COLLATED RESULTS FOR NINE-MONTH FORCE-LEVEL TRIAL

| | Traditional | Remote | Total |
|---|---|---|---|
| Cases submitted | 1,086 | 329 | 1,415 |
| | 76.7% | 23.3% | |
| Lifts submitted | 2,812 | 856 | 3,668 |
| No-value lifts | 735 | 190 | 925 |
| % Judged no-value | 26.1% | 22.2% | |
| Average lifts per scene | 2.6 | 2.6 | |
| Idents achieved | 161 | 59 | 220 |
| % Idents | 14.8% | 17.9% | |

Table V, where "traditional" refers to road transport to the bureau and "remote" to crime scene scanning and compression. The ratio of traditional to remote is approximately 3.3:1 and the average number of lifts per crime scene examined is the same for both transfer methods. Though there is a higher percentage of idents obtained using wireless transmission (17.9% versus 14.8%), a chi-square test of independence indicates that this difference is not significant $\chi^2\,(2, N = 220) = 1.86, p > 0.05$. The difference in no-value lifts for the two conditions is significant $\chi^2\,(2, N = 925) = 5.41, p = 0.025$.

The question that naturally arises is "Did this gradual change in transport mode create an inadvertent bias in the above results?" It is therefore necessary to confirm that the lifts sent by the two methods were from the same population (i.e., there is no difference in the average quality of lifts sent by the two routes). A randomized selection of 90 original lifts (60 traditionally transported and 30 wireless transmitted) was presented to six LFEs from the London Metropolitan Police fingerprint bureau, who were unaware of the transport mode. They were asked to judge the quality of the lifts on a 5-point Likert Scale. The descriptive statistics are provided in Table VI. A two-way factorial ANOVA yielded no main effect for the transport mode $F(1{,}528) = .032, p > .05$. There was a main effect for the expert quality ratings $F(5{,}528) = 3.944, p = .002$. A Tukey HSD post-hoc test revealed a significant pairwise variation between the quality ratings used by the experts. This means that the different experts used the rating scale differently. More important though, there was no interaction effect $(F(5{,}528) = 0.321, \mathrm{p} > 0.05)$; hence, the individual experts used their own rating scale consistently.

TABLE VI
DESCRIPTIVE STATISTICS FOR EXPERT QUALITY ASSESSMENT OF LIFT SAMPLES

| Condition | | Expert 1 | Expert 2 | Expert 3 | Expert 4 | Expert 5 | Expert 6 |
|---|---|---|---|---|---|---|---|
| 1 | Mean | 3.200 | 2.583 | 3.167 | 2.383 | 3.067 | 2.700 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| | SD. | 1.424 | 1.225 | 1.379 | 1.291 | 1.552 | 1.317 |
| 2 | Mean | 3.017 | 2.533 | 3.233 | 2.517 | 2.950 | 2.983 |
| | N | 60 | 60 | 60 | 60 | 60 | 60 |
| | SD. | 1.324 | 1.362 | 1.300 | 1.353 | 1.478 | 1.347 |
| Total | Mean | 3.078 | 2.550 | 3.211 | 2.472 | 2.989 | 2.889 |
| | N | 90 | 90 | 90 | 90 | 90 | 90 |
| | SD. | 1.353 | 1.311 | 1.320 | 1.327 | 1.495 | 1.336 |

Condition 1 = wireless transmission; Condition 2 = road transport.

The conclusion drawn from this comprehensive trial is that there is no reduction in idents through the use of 16:1 JPEG2000 images but that the remote transfer of these images greatly reduces the time delay to obtain an ident and so enhancing the value of the forensic evidence. An interesting side issue, highlighted by the significant difference in no-value lifts between uncompressed and compressed formats, is the possible advantage of wavelet compression of improving poor-quality lifts. This effect is also apparent in the frequently observed increase in the NAFIS autoencoding score for low values of compression. Wavelet decomposition is commonly employed to improve the quality of a wide range of signal types by reducing noise artefacts, and similar effects may occur in this case [31].

### B. *Compression Image Storage*

Having confirmed that effective and uncompromised searching could be achieved using compressed latent images, then some of the efficiency gains in productivity would be forfeited if uncompressed versions of unidentified lifts had to be subsequently loaded onto NAFIS by bureau staff into the current archive of unidentified latents. It is necessary, therefore, to confirm that there was no loss in search capability for TP/MK searches. This is potentially a different search scenario to the more usual MK/TP searches. The methodology was to present 11 independent LFEs with a randomized set of representative latent images (in TIFF and 16:1 JPEG2000 formats) with each examiner marking up 15 lifts of each format. Though there were corresponding image format pairs of each latent, no officer saw more than one example of each latent. Lifts were all cropped and prealigned before these officers began their markups. This was carried out by a single experienced LFE to ensure consistency in the latent presentation to NAFIS, who took no further part in the experiment. The set of 60 latent lift images was carefully selected to be fully representative of the range of expected latent quality found in practice. The composition of the test set was agreed with the HOSDB and independent fingerprint experts.

A smaller set (10) of chemical lifts was included as foils to eliminate any bias due to potentially detected differences in image appearance. Chemical lifts are photographs (either digital or 35-mm film) of fingerprint-ridge detail that have been

TABLE VII
DESCRIPTIVE AND PAIRED t-TEST SUMMARY STATISTICS FOR JPEG2000 MK/TP AND TP/MK NAFIS SEARCHES

| | | Mean | N | SD | Std. Error |
|---|---|---|---|---|---|
| Pair 1 | TIFF MK/TP | 9.636 | 11 | 1.748 | 0.527 |
| | JPG2K MK/TP | 10.000 | 11 | 1.095 | 0.330 |
| Pair 2 | TIFF TP/MK | 4.636 | 11 | 2.420 | 0.730 |
| | JPG2K TP/MK | 3.818 | 11 | 2.786 | 0.840 |

| | | Mean | SD | t | df | Sig. Level |
|---|---|---|---|---|---|---|
| Pair 1 | TIFF MK/TP - JPG2K MK/TP | -0.3636 | 2.11058 | -0.571 | 10 | 0.580 |
| Pair 2 | TIFF TP/MK - JPG2K TP/MK | 0.8182 | 4.91565 | 0.552 | 10 | 0.593 |

found on items seized at crime scenes and produced by chemically treating them with reagents that react with perspiration deposits. The chemical laboratory that develops these latents is normally attached to the fingerprint bureau and they can have a markedly different visual appearance to powder lifts. All lifts had previously been identified on NAFIS and related to real cases (though all legally closed). Full national searches were initiated and both MK/TP and TP/MK searches were undertaken. The autoencoding score and rankings were recorded for all successful matches. Normal working practices were followed as far as possible, and the participants were unaware of the precise purpose of the experiment other than it involved an assessment of latent image quality. LFEs were asked to search as far down the ranking list in order to complete visual comparisons of the returned matches with each presented latent as they would in a normal operational environment. The key measure is the ident rate for the various conditions—a change in an autoencoding score or rank number would not affect an examiner's decision on a match.

A paired t-test comparing TIFF MK/TP searches ($M = 9.636$, $SD = 1.748$) and JPEG2000 MK/TP searches ($M = 10.000$, $SD = 1.095$) showed no significant difference $t(10) = -0.571$, $p = 0.580$; and a paired t-test comparing TIFF TP/MK searches ($M = 4.636$, $SD = 2.412$) and JPEG2000 TP/MK searches ($M = 3.818$, $SD = 2.786$) showed no significant difference $t(10) = -0.593$, $p = 0.593$. Summary statistics are given in Table VII. As there is the possibility of falsely accepting the null hypothesis $Ho$ (i.e., Type II error) a post-hoc statistical power test is performed. For MK/TP searches, the power $P = 0.92$ and for TP/MK searches $P = 0.86$. Powers greater than 0.80 are taken to indicate a strong statistical test. The conclusion is that there is no disadvantage in using compressed images in both MK/TP and TP/MK searches and, hence, unidentified latents need only be retained in compressed format on NAFIS.

## VI. BENEFITS TO POLICE OPERATIONS

### A. General Improvements

For the police force where the extended trial was conducted, prior to the wireless transmission of lifts, the average time to ident was four days. This delay composed of a delay of three days for the lift to reach the bureau and a further delay for it be recorded and scanned before a NAFIS search could be initiated. Postutilization of the wireless transmission of compressed latent images, the average time to ident is just under 2 h. Though a lift can be transmitted in less than a minute, there is a series of in-bureau procedures to complete. The latent image has to be launched onto NAFIS and a search instigated. The LFE will then inspect the returned TPs for a match. If a match is found, then another LFE as well as the Head of Bureau or their designate must confirm it before a suspect's identity can be released. It is more difficult to assess the system's contribution to crime rates and arrests, as there is a range of external and other internal factors that have a bearing on collated crime statistics. For burglaries, there has been a long-term decline in numbers across the U.K., but for the year that this system was in operation for the trial force, its burglary rate fell by 8% for 2005–2006 against a national picture of no annual change [32].

### B. Case Example

The developed system has made a significant impact on reducing the average time to obtain ident from crime scene latents and this has contributed in increased clearup rates for several categories of offense. However, it is its contribution to specific cases that really demonstrates the system's capabilities. Many cases are still progressing through the U.K.'s legal system and so cannot be reported; however, the example given below has completed all such processes.

A 92-year-old woman was attacked and robbed in the street of the Lincolnshire town of Gainsborough. The incident generated considerable public concern and the local police were under heightened pressure to make progress. Acting on local intelligence, they had a suspect but insufficient grounds to make an arrest. The police raided a flat where the suspect and his partner were temporarily living but a search failed to find any property from the robbery. There were well-grounded reasons to believe that if the suspect was not detained then he would quickly flee from the area. Near the flat, there was a car that had been reported stolen from a neighboring county. The keys from this car were found on the suspect's partner but there was nothing to directly link the suspect to the vehicle. It became vitally important to associate the suspect with this vehicle. A CSE was dispatched to the scene and he searched the vehicle. A fingerprint was found on the car's wing mirror; this was lifted and the resulting lift (Fig. 8) was scanned and transmitted directly from the scene. The lift was searched at the force bureau and the suspect's ident was confirmed. It took only 30 min between the examiner arriving at the scene and a positive ident to be made. The suspect was arrested and remanded for vehicle theft. This gave the police sufficient time to collect and analyze CCTV tapes from the town that showed the suspect following the victim through the streets prior to the attack. The suspect was charged the following week with aggravated robbery and sentenced to four year's imprisonment seven months later.

## VII. CONCLUSION

This series of experimental studies, together with the analysis of an extended trial, have confirmed the suitability of 16:1 JPEG2000 compression for the effective and reliable transmission of fingerprint latents directly from crime scenes. The capability to establish ground truth on any possible effects image

Fig. 8. Latent recovered from stolen car (see case example).

compression may have on ident rates made this work highly principled in its approach. The outcome of this study and its presentation to the U.K. National Fingerprint Board (The body, incorporating a range of stakeholders, that oversees the operation of all fingerprint activities with the U.K.) was that the system should be adopted by all U.K. police forces and that unidentified latents can be archived on NAFIS in compressed JPEG2000 format except for a small number of serious crimes (where the uncompressed image must be loaded and retained on NAFIS as well). At the time of writing, ten police forces use the system with 16 more in the process of adopting it.

General future improvements in network bandwidth (e.g., EDGE or G2.75, and UMTS or G3) may alleviate the requirement for compression. However, there are no plans within the U.K. and many other countries that such networks will provide full countrywide coverage. There are also proposals that fingerprint image resolution be increased from 500 dpi to 1000 dpi, which may reinforce the need for compression. The WSQ compression standard was developed for inked TPs, and JPEG2000 was developed for the widest range of possible imagery; so it may be productive to examine the potential for custom image coding schemes tuned to the specific and unique nature of latent fingerprint images.

## ACKNOWLEDGMENT

The authors would also like to thank the long-term assistance of Robert Green (UK Home Office: Police Standards Unit) and Chief Constable Tony Lake (UK Association of Chief Police Officers) for their support of this work through its delivery to an increasing number of UK Police Forces. The authors also thank the U.K. Home Office Scientific Development Branch, notably V. Bowman and S. Bleay, who provided additional assistance with experiments and determined the suitability of scanners. The authors thank numerous fingerprint officers and crime scene examiners who generously gave their time and expertise.

## REFERENCES

[1] H. Faulds, *Dactylography. or the Study of Finger-Prints*. Halifax, NS, Canada: Milner, 1912.

[2] P. Komarinski, *Automated Fingerprint Identification Systems (AFIS)*. Burlington, MA: Elsevier, 2005.

[3] V. Bowman, Ed., Fingerprint Development Handbook St. Albans, U.K., Home Office Scientific Development Branch, 2005.

[4] E. Henry, “Classification and uses of fingerprints, original figures,” Routledge, London, U.K., 1900 [Online]. Available: www.ridgesandfurrows.homestead.com.

[5] Interchange of fingerprint, facial, & scar mark & tattoo (SMT) information Nat. Inst. Standards Technol., Special Publ. 500-245, 2000.

[6] A. Moenssens, *Fingerprint Techniques*. London, U.K.: Chilton, 1971.

[7] N. Ratha and R. Bolle, Eds., *Automatic Fingerprint Recognition Systems*. New York: Springer-Verlag, 2004.

[8] A. Jain and S. Pankanti, “Automated fingerprint and imaging systems,” in *Advances in Fingerprint Technology*, H. C. Lee and R. E. Gaensslen, Eds. Boca Raton, FL: CRC, 2001.

[9] Police and criminal evidence act 1984 codes of practice A-G2005 ed. London, U.K., Home Office, Stationery Office, 2005.

[10] Information technology – digital compression and coding of continuous-tone still images: requirements and guidelines, Int. Org. Standardization, ISO/IEC 10918-1:1994, 1994.

[11] T. Hopper and F. Preston, “Compression of grey-scale fingerprint images,” in *Proc. Data Compression Conf.*, Snowbird, UT, Mar. 1992, pp. 309–318.

[12] J. Bradley, C. Brislawn, and H. Topper, “The FBI wavelet/scalar quantization standard for fingerprint compression,” *Proc. SPIE*, vol. 1961, pp. 293–304, 1993.

[13] WSQ “Gray-scale fingerprint image compression specification,” FBI/Los Alamos Nat. Lab., Document no. IAFIS-IC-0110 (v2), 1993.

[14] M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, “Imaging coding using the wavelet transform,” *IEEE Trans. Image Process.*, vol. 1, no. 2, pp. 205–220, Apr. 1992.

[15] S. G. Mallat, “A theory for multiresolution signal decomposition: The wavelet representation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 674–693, Jul. 1989.

[16] O. Ryan, “Applications of the wavelet transform to image processing,” presented at the Seminar on Wavelets, Centre of Mathematics for Applications, Univ. Oslo, Oslo, Norway, Dec. 12, 2004.

[17] M. A. Figueroa-Villanueva, N. K. Ratha, and R. M. Bolle, “A comparative performance analysis of JPEG 2000 vs. WSQ for fingerprint image compression,” *Lecture Notes in Computer Science*, vol. 2688, pp. 385–392, 2003.

[18] M. A. Lepley, JPEG 2000 and WSQ Image Compression Interoperability MITRE, Tech. Rep. MTR 00B0000063, 2001.

[19] “Image quality measure, “overview and software” MITRE Corp. [Online]. Available: http://www.mitre.org/tech/mtf.

[20] “Information technology – biometric data interchange formats – Part 4: finger image data” Int. Org. Standardization, 2005, ISO/IEC 19794-4:2005.

[21] EPFL, ERICSSON, and Canon Research Center France , JJ2000, “A JAVA™ Implementation of JPEG 2000”, White Paper by EPFL, ERICSSON and Canon Research Center France (CRF) 2000 [Online]. Available: http://jj2000.epfl.ch/jj_whitepaper/index.html.

[22] *Information Technology – JPEG 2000 Image Coding System: Core Coding System*, ISO/IEC 15444-1:2004, Int. Org. Standardization, 2004.

[23] Nist fingerprint image software 2 (NFIS2), Craig Watson and Michael Garris Nat. Inst. Standards Technol., Oct. 2004, NIST Fingerprint Image Software 2 (NFIS2).

[24] C. I. Watson and C. L. Wilson, “Effect of image size and compression on one-to-one fingerprint matching” Nat. Inst. Standards Technol., Rep. NISTIR 7201, 2005.

[25] TWAIN specification 2001 [Online]. Available: http://www.twain.org., 1.9a

[26] R. Housley, W. Ford, W. Polk, and D. Solo, “Internet X.509 public key infrastructure certificate and crl profile,” RFC 2459, 1999.

[27] “PKCS 12 V1.0: personal information exchange syntax,” RSA Labs. Redwood City, CA, 1999.

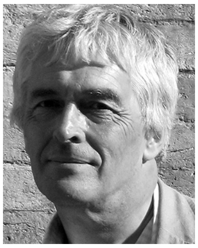
[28] D. Eastlake and P. Jones, “U.S. secure hash algorithm,” 1 (SHA1) RFC 3174, 2001.

[29] D. Atkins and W. Stallings, "PGP message exchange formats," RFC 1991, 1996.

[30] C. Adams, "The CAST-128 encryption algorithm," RFC 2144, 1997.

[31] R. R. Coifman and D. L. Donoho, "Translation-invariant denoising," in *Wavelets and Statistics*, A. Antoniadis and G. Oppenheim, Eds. Berlin, Germany: Springer-Verlag, 1995.

[32] A. Walker, C. Kershaw, and S. Nicholas, Crime in England and Wales 2005/6 U.K. Home Office, Home Office Statistical Bulletin 12/06, 2006.



**Nigel M. Allinson** (M'83) received the B.Eng. degree in electrical and electronic engineering from the University of Bradford, Bradford, U.K., and the M.Sc. degree in electrical and electronic engineering from the University of Cambridge, Cambridge, U.K., in 1977.

Currently, he is the Chair of Image Engineering at the University of Sheffield, Sheffield, U.K., and previously held the same title at the University of Manchester Institute of Science and Technology (UMIST), Manchester, U.K. His research interests are the development of novel imaging devices and systems (especially for scientific applications), image transmission and processing, and pattern recognition. He has co-founded three spinout companies based on research within his group.

**Jeevandra Sivarajah** received the B.Eng. degree in computer systems engineering and the Ph.D. degree from the University of Manchester Institute of Science and Technology (UMIST), Manchester, U.K., in 1999 and 2004, respectively.

Currently, he is a Research Associate at the University of Sheffield, Sheffield, U.K.

Dr. Sivarajah was awarded the IEE Communication Premium Prize for a paper "A New TCP-friendly, rate-based transport protocol for media streaming application" and is currently supported by the U.K. Home Office: Police Standards Unit.

**Ian Gledhill** is Head of the Bureau with the Lincolnshire Police, Lincoln, U.K. He has 24 years of experience in fingerprint examination.

**Michael Carling** received the B.Sc. degree in mechanical engineering from the University of Manchester Institute of Science and Technology (UMIST), Manchester, U.K.; the M.Sc. degree in polymer science and engineering from Lehigh University, Bethlehem., PA; and the Ph.D, degree in mechanical engineering from Imperial College, London, U.K.

Currently, he is Scientific Support Manager for Lincolnshire Police, Lincoln, U.K.

**Lesley J. Allinson** received the B.A. degree in psychology from Open University, U.K., in 1983 and the M.Sc. degree in computer science and the Ph.D. degree in navigational aspects of human–computer interaction (HCI) from the University of York, U.K., in 1986 and 1991, respectively.

Currently, she is a Senior Lecturer in Psychology at the University of Lincoln, Lincoln, U.K.