Forensic Science Regulator
Overseeing Quality

Forensic Science Regulator Guidance

Validation: Friction Ridge Detail (Fingerprint) Search Algorithm

FSR-G-230

Issue 2

1. Introduction

1.1.1 The fingerprint community currently uses an Automated Fingerprint Identification System (AFIS) in its bureaux to narrow down the range of possible biometric candidate(s), whose finger(s) or palm could be responsible for a mark left at a crime scene.

1.1.2 Marks recovered from crime scenes and individuals' tenprint records are held in data collections (databases). The AFIS system searches these databases to identify similarities between specified areas of interest on a scene mark and either:

a. tenprint detail to indicate a possible matching candidate; or
b. other scene marks to ascertain whether the same individual left marks at multiple scenes.

1.1.3 Following a search a range of possible corresponding records will generally be recognised as potential candidates producing a biometric candidate list, so that a full manual biometric comparison can be carried out by a qualified fingerprint examiner.

1.1.4 The underlying search algorithm is to be replaced and to that end a supplier product has been identified by Home Office Biometrics (HOB) who will be the provider to the fingerprint bureaux. As such there are at least two major aspects to consider with the replacement of the algorithm:

a. The search capability of the new algorithm and;
b. The establishment of the new algorithm in operations.

1.1.5 This guidance document addresses the validation of an algorithm to replace the one that is currently employed by fingerprint bureaux.

2. Purpose and Scope

2.1.1 The purpose of this document is to provide guidance for validation of the search/comparison algorithm and the method in which it is deployed. It expands and builds upon some of the elements of the existing Forensic Science Regulator's Codes of Practice and Conduct (the Codes) and the Validation Guidance FSR-G-201. Particular emphasis is placed on the

documentation to be provided to users from each stage of the validation process to construct and maintain the validation library.

2.1.2 The generic requirements set out in section 7, figures 1 and 2 in the Regulator's guidance Software validation for DNA mixture interpretation, FSR-G-223 apply to this guidance and shall be taken into account when validating software.

2.2 Inclusions

2.2.1 This document covers:

a. Consideration of user requirements;
b. Consideration of specification;
c. Suggested structure for verification of supplier performance claims;
d. Suggested structure for 'central' validation plan;
e. A consideration of error rates;
f. Suggested structure for local verification and;
g. Suggested structure for implementation into an operational situation.

2.2.2 Home Office Biometrics (HOB) may consider 2.2.1c above as biometric accuracy testing (BAT) and 2.2.1d as primarily user acceptance testing (UAT) in combination with other tests run by HOB.

2.3 Exclusions

2.3.1 This document illustrates the elements that a comprehensive validation plan should contain and the areas that it should cover. It does not prescribe the exact nature of any required testing; that is for HOB and the fingerprint bureaux to determine.

2.3.2 This document does not prescribe the content of any required training for bureau staff.

3. Implementation

3.1.1 This guidance is available for incorporation into a forensic unit's [1] quality management system from the date of publication. The Regulator required that the Codes [2] were included in the forensic units' schedule of accreditation by October 2017 and the accreditation of fingerprint comparison by October 2018.

4. Modification

4.1.1 The Regulator uses an identification system for all documents. In the normal sequence of documents this identifier is of the form 'FSR-#-###' where (a) the '#' indicates a letter to describe the type or document and (b) '###' indicates a numerical, or alphanumerical, code to identify the document. For example, the Codes are FSR-C-100. Combined with the issue number this ensures each document is uniquely identified.

4.1.2 In some cases, it may be necessary to publish a modified version of a document (e.g. a version in a different language). In such cases the modified version will have an additional letter at the end of the unique identifier. The identifier thus becoming FSR-#-####.

4.1.3 In all cases the normal document, bearing the identifier FSR-#-###, is to be taken as the definitive version of the document. In the event of any discrepancy between the normal version and a modified version the text of the normal version shall prevail.

4.1.4 This is the second issue of this document.

4.1.5 Significant changes to the text have been highlighted in grey and noted in paragraph 4.1.6.

4.1.6 The modifications made to create Issue 2 of this document were to ensure compliance with The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018. There is an updated

1 Software provider/developer if not the forensic unit.

2 Forensic Science Regulator, Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System.

copyright statement, some reformatting, and provision of text alternatives where information has been presented in a non-text format. Any references that have necessarily changed with the passage of time have been refreshed. The content of the document is otherwise unchanged save for in Section 4.

5. Terms and Definitions

5.1.1 The terms and definitions set out in the Forensic Science Regulator's Codes of Practice and Conduct (the Codes), Fingerprint Comparison, FSR-C-128, Fingerprint Examination – Terminology, Definitions and Acronyms, FSR-C-126 and the Glossary at section 14 apply to this document.

5.1.2 The word 'shall' has been used in this document where there is a corresponding requirement in BS EN ISO/IEC 17025 General Requirements for the Competence of Testing and Calibration Laboratories and in the Codes; the word 'should' has been used to indicate generally accepted practice where the reason for not complying or any deviation shall be recorded.

6. User Requirement And Specification

6.1 User Requirement

6.1.1 The requirement is for a replacement search/comparison algorithm for the Automated Fingerprint Identification System (current AFIS) – 'IDENT1' – in use in the various fingerprint bureaux.

6.1.2 The replacement algorithm shall be compatible with the established working practice so as to minimise any disruption to the operations of the bureaux.

6.1.3 The replacement shall 'perform' at least as well as or better than its predecessor.

6.2 Specification

6.2.1 The specification is set to fulfil the user requirement.

6.2.2 The new algorithm as a minimum shall meet the following requirements.

a. Allow for the same method(s) of input as currently employed.
b. Be able to search a database(s) and be able to return a correct record:
    i. for the same mark/print (duplicate);
    ii. between a questioned mark and a known print held on a database; and
    iii. between two different marks to establish common source or not.
c. Be better than its predecessor in the rate at which it returns correct records.
d. Demonstrate a lower error rate than that demonstrated by its predecessor.
e. Work at least at the same speed as its predecessor.
f. Be perceived (qualitative) to be at least as user friendly as its predecessor.
g. Be at least as reliable as its predecessor in terms of:
    i. the repeatability and robustness of its output; and
    ii. its resilience to attack and/or malfunction.
h. Provide an output in a form that is compatible for use in subsequent stages of the fingerprint examination process.

6.2.3 The validation acceptance criteria shall be determined from both the user requirement and specifications. Validation shall provide evidence that these have been met.

7. Risk Assessment Identification And Mitigation

7.1 Risk Identification

7.1.1 What are the risks that could be associated with this new algorithm and so produce a risk to the Criminal Justice System (CJS)?

7.1.2 What would the effect be if such risks were realised?

7.1.3 Since the new algorithm is to be introduced as a replacement for one already in use, then it is perceived that any new risk to the CJS will come from the

algorithm itself and whether it has been correctly integrated into the new matcher platform and existing IDENT1 workflow.

7.1.4 Once staff are trained and competent in the use of the new algorithm, all other process activities and risks around it are essentially unchanged.

Risk Description	Unmanaged Risk	Control Measures to Reduce Risk	Managed Risk
Unsuitable mark entered, i.e. not recognised by the algorithm	Moderate	Appropriate training and competency assessment of staff in determining mark suitability. Automated failure message.	Low
Poor assessment of mark	Moderate	Quality assessment of mark is independently corroborated by a second practitioner, e.g. at peer review.	Low
Incorrect algorithm functionality or initial installation results in an incorrect search result	Moderate	Ensure statistical model is sound in concept and operation by validation of the model (through BAT and UAT), plus peer review and publication.	Low
		Back-to-back testing of the software with the previous AFIS (during the 'parallel run' phase of deployment) to minimise the risk of potential errors not being detected.	
Algorithm output not recognised by subsequent process causing failure of the process	Moderate	The algorithm and its implementation will be put through a series of 'IT tests' prior to deployment. Once deployed there will be a period of 'early life support' to identify and remedy issues not picked up during the original IT testing.	Low
Errors in reporting conclusions arising from analysis of the output	Moderate	Technical check and peer review prior to closing case.	Low
		Ensure that staff are appropriately trained and demonstrably competent.	
		Implement regular dip sample, case audit and quality assurance trials to check for correct and consistent interpretation of findings.	
	Moderate	Check correct data are being used when drafting the validation plan.	Low

Use of incorrect data for validation		Once implemented, periodically review the validation including version of software.	
Algorithm returns a record not found by its predecessor	Moderate	Re-search negative outputs from previous marks. Determine whether the new candidate list includes any candidates missed by the previous algorithm rather than those candidates added to the database since the previous search.	Low
New algorithm fails to return a record found by its predecessor	Moderate	Spot checks/rerun previous marks, revisiting algorithm functionality, installation and searching parameters as necessary.	Low
Security breach: a deliberate act	Low	Ensure adequate physical and IT security is in place and review as necessary.	Very low

Table 1: Potential risks and possible mitigation measures for the introduction of a new fingerprint search algorithm

8. Validation

8.1.1 Validation is required not just to show that the new algorithm performs as expected in isolation, although that is part of it. Rather, the validation considers the whole process that can impact or be impacted by the algorithm. Therefore, it needs to be based on a number of test samples that represent the range of samples likely to be encountered during the algorithm's working life.

8.1.2 The validation addresses whether the method actually meets the requirements of the user specification.

8.2 Validation Plan

8.2.1 The validation guidance FSR-G-201 sets out the process that organisations shall follow for validation. Table 2 lists the various stages and identifies whose responsibility it is to carry out and produce the relevant documentation for each stage.

	Commercial Provider	Home Office Biometrics	Fingerprint Bureaux
Define User Requirement		[redacted]	Consulted
Specification	[redacted]	[redacted]	Consulted
Risk Assessment	[redacted]	[redacted]	Consulted
Set Acceptance Criteria	[redacted]	[redacted]	[redacted]
Validation of Statistical Model	[redacted]		
Algorithm Development and Testing	[redacted]		
Functionality Testing	[redacted]	Recipient of report	
System (Central) Validation/User Acceptance Testing Plan		[redacted]	Consulted
Validation Report	[redacted]	[redacted]	Recipient of report
Validation Library	[redacted]	[redacted]	Recipient of library
Statement of Completion	[redacted]	[redacted]	Recipient of statement
Implementation Plan		[redacted]	[redacted]
[redacted]	Carries out and produces documentation for that stage.		

Table 2: Responsibilities for the various stages of bringing the search algorithm from procurement to business as usual

8.3 Supplier Obligations

8.3.1 Fingerprint comparison algorithms vary in terms of how they perform the required comparisons and the features they employ. Algorithm accuracy, comparison speed and robustness to poor image quality are critical elements of system performance. HOB will have determined the parameters that were set for procurement tenders for the replacement algorithm for 'IDENT1'. Further considerations of those criteria are out of the scope of this document.

8.3.2 It is required that prior to delivering the algorithm, the supplier will have carried out Factory Acceptance Testing (FAT), which is a series of

developmental and functionality tests to show that it (the algorithm) functions as stated. In the case of the fingerprint search algorithm, this development and functionality testing would be required to have constituted at least a number of repeats of searches for a number of prints amongst a large dataset of prints that itself is known to contain the print(s) being sought. Such ground truth testing serves to show that the algorithm will (or indeed will not) carry out the search function for a typical tenprint to tenprint comparison.

8.3.3 As the end use of the algorithm is to process marks then some examples of ground truth marks representing tiered degrees of challenge/difficulty shall be provided to the supplier to test the algorithm on the final version established following print-to-print testing.

8.3.4 Testing should include the following elements.

a. Stress testing – to determine whether functionality is maintained when the system is being simultaneously used by a sufficiently large number of practitioners to replicate operational conditions.
b. Consideration of error rates – determined in terms of false positive and false negative rates.
c. Version control – where testing fails, the algorithm should be revised and the new version subjected to repeat functionality testing until successful.

8.3.5 At the completion of functionality testing, a test report shall be provided including a description of identified issues and their solutions or any necessary mitigation.

8.3.6 This report and data results evidencing support for the stated claims of performance shall be made available to HOB, and to end users, to be used as part of the central validation plan and validation library.

8.3.7 Central validation and local verification shall then be carried out using the final version of the algorithm.

8.4 Central Validation

8.4.1 Acceptable functionality of the algorithm shall not be assumed and testing such as biometric accuracy testing (BAT) shall be carried out by HOB to

repeat some of the supplier's testing procedure as verification that the algorithm functions as claimed.

8.4.2 The output of such testing should be designed to enable a high level search method standard operating procedure (SOP) to be developed. A report detailing the testing, its outcomes and the search method SOP shall be provided to the fingerprint bureaux.

8.4.3 It is imperative that validation shall only be carried out on the final production version of the algorithm. Any subsequent updates shall be evaluated and any likely impact to match accuracy will require further validation; such validation shall be planned into the update procedure and notification shall be given to all bureaux ahead of updates, to enable local verification to be planned and executed.

8.4.4 Central validation shall be designed to explore the full working range of the new algorithm, including, but not necessarily limited to:

a. marks and prints with a tiered level of challenge/difficulty;
b. marks in different media and on different substrates;
c. marks generated using the range of revealing enhancement techniques and imaging in use;
d. auto-encoded searches;
e. examiner-encoded searches;
f. a consideration of error rates;
g. stress testing (i.e. multiple simultaneous users); and
h. performance comparison with the current algorithm to determine the extent of any performance improvement.

8.4.5 The testing should include print-to-print, mark-to-print, print-to-mark and mark-to mark considerations.

8.4.6 Datasets employed should allow for comparisons that can be categorised as 'Easy', 'Medium' and 'Difficult' (or 'Low', 'Medium' and 'High' risk of not returning the correct record).

8.4.7 To test the algorithm in a real-world situation, the ‘questioned’ marks should replicate marks typical of those encountered at crime scenes and during casework.

8.4.8 The ‘real-world’ marks should include varying degrees of sufficiency, as well as quality and complexity for comparison (for example, movement, distortion, damage, interference/artefacts) to test the search and comparison capability and provide data to assess against the user requirement criteria set.

8.4.9 Marks that test as closely as possible the live processing environment will provide some robustness/case hardening data, testing the limits of the algorithm.

8.4.10 Sets destined for use as ‘background’ in a searched database should be representative of live data in terms of quality and quantity. Where mated pairs are required, the ground truth shall not have been established through either automated matching or comparison by competent practitioners.

8.4.11 To lessen the impact of local verification by providing comprehensive known source validation data, the tests used here should include the following.

a. Marks generated from routine substrates encountered using the range of revealing enhancement treatments and imaging used across police forces.
b. Be built up and maintained in co-operation with the fingerprint bureaux and the donor prints provided in all media formats (for example, paper scan, ink, transmission from scene and electronic live scan) to include previous and current methodologies.
c. Mated pairs (marks and prints), where the ground truth has been established through the collection process from known donors rather than by automated matching.

8.4.12 Such data as described at 8.3.9 are what would populate an anticipated virtual bureau testing facility.

8.4.13 For each validation phase a number of competent practitioners from a range of organisations should be used. This will multiply the number of

comparisons proportionately to provide an indication of the reliability/repeatability of the algorithm. They should:

a. be working blind (i.e. without prior knowledge of expected outcomes);
b. be trained for input and marking up; and
c. have a range of experience.

8.5 Back-to-Back (Parallel) Testing

8.5.1 To compare the performance of the new algorithm directly against its predecessor, the central validation plan shall also include some back-to-back testing where the tests shall be run with both algorithms, using the same ground truth test data and staff.

8.5.2 Back-to-back (parallel) testing should also be carried out prior to the release of updates to the software that would affect the performance of the algorithm. The central validation phase can be the platform for developing and validating a mark search method SOP.

8.6 Validation Exercise

8.6.1 As a minimum the validation plan and testing shall consider the parameters as set out in Figure 1.

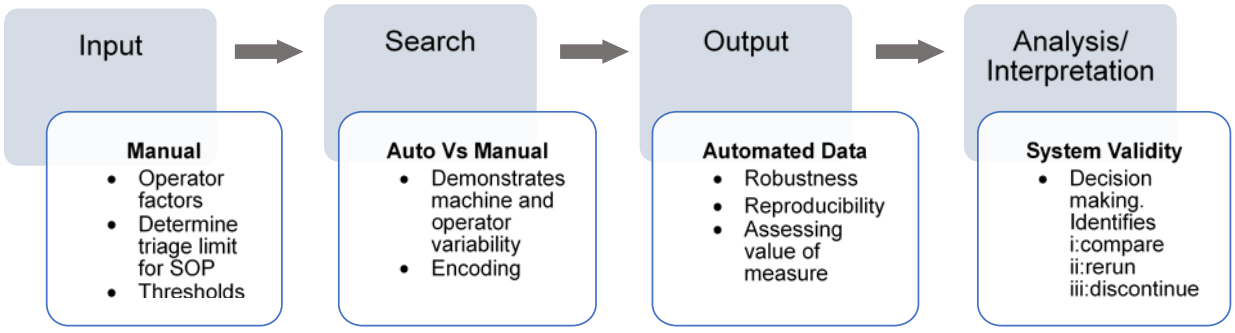

Figure 1: Expected Parameter Testing

8.6.2 Data and information from the supplier's previous functionality testing shall be taken into account for the validation testing.

8.6.3 Marks previously classified as 'nearest non-match' marks shall be included to help to define the limits of discrimination of the algorithm.

8.6.4 Once the validation plan has been agreed and finalised by a technical manager or similar, it shall be performed.

8.6.5 The output of the validation exercise shall clearly state whether or not the method with the new algorithm achieved the requirements of the specification. If it did not, then the method including the new algorithm will have failed its validation.

8.6.6 In the event of a failed validation, it is possible to reconsider the specification to determine whether the requirements can be met by further amendment of the method or by additional safeguards. If that is acceptable, then a new specification and validation plan reflecting those amendments shall be produced.

8.6.7 In the event of a successful validation exercise (i.e. the method achieved the requirements of the specification) then a validation report shall be produced. See the Codes and validation guidance FSR-G-201 for more detail.

8.6.8 The outputs from the validation should be published and shall be available to end users. These outputs will provide data to inform triage criteria and identify good practice. From this, the training manual and existing SOPs should be updated or new ones developed prior to implementation and business as usual (BAU).

8.7 Validation Report

8.7.1 The validation report shall include:

a. outcomes of the validation tests and assessment against the acceptance criteria;
b. a clear definition of the conditions and limitations within which the method can be utilised; and
c. an evaluation, by the individual identified at 8.8.1, of the assessment of error rates.

8.8 Validation Library

8.8.1 To support the validation, a validation library shall also be produced.

8.8.2 This is a collection of documents relevant to the validation of the algorithm and each party should contribute to it as set out in Table 2. The library shall include, but need not be limited to, the following.

a. Documented details of the version of the algorithm validated and the process within which it is applied.
b. The risk assessment for the relevant version of the algorithm and the process within which it is applied.
c. Any associated supporting material, such as academic papers or technical reports that were used to support or provide evidence on the applicability of the method.
d. The validation plan for the approved search/comparison algorithm and the process, including user acceptance criteria.
e. Summaries of the data and an assessment against the acceptance criteria. The information provided must properly reflect the results obtained from the validation tests and be sufficient to support any conclusions drawn in the report and,
f. The statement of validation completion and record of approval as agreed by the individual identified at 8.8.1.

8.8.3 Where the validation relies on the material of others (such as publications or the test data results provided by the supplier), a copy shall be kept as part of the library to ensure that the information is readily accessible. This is especially important if the source of the material is not permanent, for example, published on the internet; an ‘instance’ of the material should be captured and the time and date of capture recorded.

8.8.4 The validation library shall be maintained by HOB to cover the period for which the algorithm is in use and to aid in addressing any legal challenges to the output from the algorithm that might arise.

8.9 Validation Completion

8.9.1 The validation exercise shall be reviewed and agreed by an identified individual who is independent of the validation plan. It is not within the scope of this document to identify who that individual should be, but it shall not be:

a. a representative from within the HOB team;
b. any person who has designed or carried out any of the validation testing; nor
c. any person who has a vested interest in the outcome of the validation exercise.

9. Local Verification

9.1 Responsibility and Action

9.1.1 Verification demonstrates technical competence in providing valid and accurate data and results, which is the fundamental aim of accreditation to BS EN ISO/IEC17025.

9.1.2 Verification shall involve fingerprint bureau staff carrying out a similar range of ground truth tests as were carried out for the central validation, but on a smaller scale to demonstrate that the algorithm functions as expected in their operational environment.

9.1.3 Verification is conducted once the staff of the bureau adopting the new algorithm and associated method have reviewed the central validation documentation. That review shall include an assessment of the central validation's sufficiency and applicability to their own proposed use in terms of whether:

a. the central validation user requirement coincides with theirs; and
b. the central validation specification and pass criteria is appropriate for them.

9.1.4 The assessment at 9.1.3 shall be documented and included as part of the validation library.

9.1.5 Verification shall include any process carried out by the particular fingerprint bureau and shall be carried out following local standard operating procedures (SOPs) with local staff. It should encompass the range of expected quality, sufficiency and complexity of mark encountered and involve different competent practitioners at all levels of skill and experience within the bureau across the working day.

9.1.6 Each fingerprint bureau shall repeat certain comparisons, previously carried out as part of central validation and most relevant to their own bureau, to demonstrate that the algorithm performs at least as well on those bureau-based comparisons as it did for the central validation.

9.1.7 If the algorithm appears to perform less well in the bureau than in the central validation exercise, then the cause of that shall be investigated and addressed appropriately. Appropriate measures could include, but are not necessarily limited to:

a. adjustment of local procedures to bring bureau performance to the same level as seen at central validation;
b. identification of a training need for staff; and
c. identification of necessary equipment upgrade.

9.1.8 If the algorithm appears to perform better in the bureau than in the central validation, then the cause of that shall be investigated.

9.1.9 Any identified performance improvement over the validation exercise shall be communicated to HOB as the system provider to ensure that any required change to the process is captured and promulgated.

9.1.10 If a change to process is implemented, then consideration shall be given to any subsequent need to revisit and repeat all or part of the validation.

9.1.11 If a software update does not affect the original validation then a full revalidation is not required, but an appropriate verification is. This could include back-to-back comparison with the previous, non-updated version. The validation library shall be updated accordingly and communicated to the bureaux.

9.1.12 The bureaux shall ensure that all appropriate staff receive training on the use of the replacement algorithm sufficient for them to be considered competent in its use.

9.1.13 As part of the verification process, staff shall demonstrate that they can obtain the expected results, and this shall be documented in their competency records.

10. Implementation Management

10.1 Responsibility and Action

10.1.1 If the validation has been successful, then there shall be a documented plan to implement the method developed by HOB and the fingerprint bureaux.

10.1.2 The introduction of any new technique into BAU. following validation and verification shall be carefully considered and planned for, to ensure that the implementation is controlled and that the application of the method continues to be fit for purpose once introduced.

10.1.3 The implementation plan shall involve an appropriately appointed and authorised member of the organisation approving the implementation of the method and determining what it will be used for. This shall be based on the specification that was used for validation and verification and shall include consideration of the following.

a. Training and competency assessment. Staff training in the application of the method of which the new algorithm forms a part, plus the means of assessing their competency in its use and interpretation of the outputs, needs to be in place prior to implementation.
b. The approach being adopted to rolling out the use of the algorithm and any associated hardware and software needs to be decided upon and included in the implementation plan.
c. Quality assurance, audit and accreditation requirements, which may include:

    i. the use of the search algorithm being captured within the laboratory regular quality assurance reviews (blind checking and dip sampling of the different outcomes), quality control, competency tests and audit programmes;
    ii. the HOB test strategy document relating to the use of the new algorithm; and
    iii. a monthly ‘Ping’ test on the new algorithm.

d. Configuration management to ensure that the method uses only the version of the algorithm that was validated, otherwise there can be no confidence that the method will operate as expected.

e. The use of the algorithm in the fingerprint examination workflow shall be included as an extension to scope for accreditation to the standard BS EN ISO/IEC 17025.

10.1.4 A short (approximately two pages) 'Question and Answer' style document should be generated by HOB, outlining the strengths and weaknesses of the algorithm software (see the Codes clause 20.2.57 A statement of validation completion). This should form part of the validation library and be made available to the courts in the event that the admissibility of the technique is questioned.

10.1.5 It is a Crown Prosecution Service (CPS) requirement that a document of this nature be generated for scientific techniques under consideration by the courts.

10.1.6 As part of implementation and initial monitoring of UAT for the new algorithm, a short period of live parallel running before switching completely to the new algorithm should be carried out by HOB.

10.1.7 The outcome of the parallel running shall be documented and provided to the fingerprint bureaux to be included in their verification documentation and the validation library.

10.1.8 Part 15 of Criminal Procedure Rules dictates that differences in the output of the two algorithms identified during live parallel running must be disclosed, so therefore shall be included in the report produced for the CJS.

10.1.9 As part of implementation, it is essential that the supplier and the provider of the algorithm (HOB) and any hardware, as well as operational stakeholders, are equally aware of their obligations regarding the investigation of quality failures in any aspect of the system during operational use. The requirements for the escalation of quality issues are outlined in the Codes, but in any event, all quality failures must be investigated as part of the continuous improvement process embedded in BS EN ISO/IEC 17025.

11. Review

11.1.1 This document is subject to review at regular intervals.

11.1.2 If you have any comments please send them to the address as set out on at: www.gov.uk/government/organisations/forensic-science-regulator, or email: FSREnquiries@homeoffice.gov.uk

12. References

BS EN ISO/IEC 17025 General Requirements for the Competence of Testing and Calibration Laboratories.

Criminal Procedure Rules and Practice Directions. Available at: www.justice.gov.uk/courts/procedure-rules/criminal/rulesmenu-2015 [Accessed 13/07/2020].

Forensic Science Regulator Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System. Birmingham: Forensic Science Regulator. Available at: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct [Accessed 13/07/2020].

Forensic Science Regulator Fingerprint Comparison, FSR-C-128. Birmingham: Forensic Science Regulator. Available at: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct#appendices [Accessed 13/07/2020].

Forensic Science Regulator Fingerprint Examination – Terminology, Definitions and Acronyms, FSR-C-126. Birmingham: Forensic Science Regulator. Available at: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct#appendices. [Accessed 13/07/2020].

Forensic Science Regulator Software validation for DNA mixture interpretation, FSR-G-223. Birmingham: Forensic Science Regulator. Available at: www.gov.uk/government/collections/dna-guidance [Accessed 13/07/2020].

Forensic Science Regulator Validation FSR-G-201. Birmingham: Forensic Science Regulator. Available at: www.gov.uk/government/publications/forensic-science-providers-validation [Accessed 13/07/2020].

13. Abbreviations

Abbreviation	Meaning
AFIS	Automated Fingerprint Identification System
BAT	biometric accuracy testing
BAU	business as usual
CJS	Criminal Justice System
CPS	Crown Prosecution Service
HOB	Home Office Biometrics
SOP	standard operating procedure
UAT	user acceptance testing
UKAS	United Kingdom Accreditation Service

14. Glossary

Algorithm

Sequence of computer software instructions that tell a biometric system how to solve a particular problem according to a pre-determined model. [SOURCE: ISO/IEC 19794-2:2011 Information technology – Biometric data interchange formats – Part 2: Finger minutiae data]

Auto-Encoding

Encoding carried out automatically by the system in place.

Biometric Candidate

The biometric data record stored in a database, determined to be sufficiently similar to the biometric data being searched against on that database to warrant further analysis.

Biometric Candidate List

A set of zero, one or more biometric candidate(s) that may be intermediate or final. Intermediate lists may be produced by systems that use multi-pass biometric identification. Biometric candidate lists may or may not be ordered (ranked). [SOURCE: ISO/IEC 2382-37:2017 Information Technology – Vocabulary – Part 37: Biometrics]

Biometric Comparison

The automated process of measuring the similarity or difference between the biometric features of a biometric sample against stored biometric samples. For example, print to mark, mark to print or print to print.

Biometric Comparison Decision

Determination of whether two biometric samples have the same biometric source, based on a comparison score(s), a decision policy including a threshold, and possibly other inputs. A ‘match’ is a positive comparison decision. A ‘non-match’ is a negative comparison decision. A decision of ‘undetermined’ may sometimes be given. [Adapted from ISO/IEC 2382-37:2017 Information Technology – Vocabulary – Part 37: Biometrics]

Biometric Comparison Score [1]

Numerical value (or set of values) resulting from an algorithmic comparison (a high value does not necessarily mean more similar). [Adapted from ISO/IEC 2382-37:2017 Information technology – Vocabulary – Part 37: Biometrics]

Biometric Comparison Score [2] Dissimilarity/ Distance

A comparison score that decreases with similarity.

Biometric Comparison Score [3] Similarity

A comparison score that increases with similarity.

Biometric Data

A biometric sample or aggregation of biometric samples used at any stage of the process, for example, prints or friction ridge detail from marks.

Biometric Sample

Analogue or digital representation of biometric characteristics prior to biometric feature extraction**.** A biometric sample may be attributable to either a specific subject (known source) i.e. a reference sample, or representation(s) such as images of fingermarks taken from a crime scene (unknown source). A record containing the image of a finger is an example of a biometric sample**.** [Adapted from ISO/IEC 2382-37:2017 Information Technology – Vocabulary – Part 37: Biometrics]

Comparison

The assessment of similarities and differences between two areas of friction ridge detail, it can be manual such as the second step of the Assessment, Comparison, Evaluation (ACE) test process (see FSR-C-128 Fingerprint Comparison) or an automated computer algorithm.

Duplicate

No variation between the subject print or mark and its counterpart on the database. For example, it could be a second reproduction of a given image rather than a photocopy of the image as the two reproductions will be produced in an identical fashion whilst some variation would be introduced to the image by the photocopying process.

Encoding

The process of identifying areas of interest within a mark or print. Such areas could be level 1, level 2 or level 3 detail.

Examiner-Encoding

Encoding carried out by a competent fingerprint practitioner.

False Negative

A positive test sample has not been associated to the correct contributor, for example, a fingermark from a known contributor that is known to be present

amongst a dataset has not been associated with that known subject by the method(s) used. Also known as ‘false non-match’ or ‘missed match’.

False Positive

A negative test sample has been positively associated to a non-contributor, for example, a known fingermark has been identified to the wrong subject’s prints by the method(s) used. Also known as a ‘false match’. Such records can bear a close resemblance to the true responder and so be indicated on a ranking to be detail checked and eliminated. In this context they may not necessarily be considered as ‘non-match’ over the described small area of automated search.

Ground Truth

A dataset made from data where the source is known, not adduced, such as marks and prints produced by a variety of known donors, used for validation, proficiency and competency testing purposes.

Mark

The term used to refer to an area of friction ridge detail from an unknown donor/person. Usually recovered, enhanced or imaged from a crime-related item, or directly retrieved from a crime scene. See also Fingerprint Examination – Terminology, Definitions and Acronyms, FSR-C-126.

Mated Pair

Mated pairs are repeats of a print taken with a stated interval between them, and/or on different media, to introduce a level of variation within the test sample set. They would not be identical to one another but would still be from the same source. A mated pair could also be formed from a mark and a print, so long as their correspondence could be assured.

Parallel Running

Running the two (current and new) algorithms in parallel and comparing the results in live cases for a defined period.

Ping

A periodic performance monitoring review of small-scale automated matching sets run in the background of the operational system to verify that biometric matching performance is being maintained at an acceptable / required level by the live system.

Print

An impression of the friction ridges recorded under controlled conditions from a known or identified person. These include elimination print, fingerprint, inked print, palm print, plantar print, tenprint and reference sample.

Provider

The (internal) service supplier of the software (Home Office Biometrics).

Ranking

The order in which a set of potential respondents, identified by the algorithm's searching process, is returned. Each will bear a similarity to the true respondent according to the search algorithm. Usually the 'best' matching is returned with the highest score. It is for the competent practitioner to determine which, if any, is the correctly matching respondent.

Search

The process of comparing existing biometric data electronically held against a biometric sample of interest to return either a biometric candidate list or a biometric comparison decision.

Subject

The person from whom the biometric sample was obtained.

Sufficiency

The combination of extent, clarity and the level of detail within a mark that are necessary to facilitate a meaningful comparison.

Supplier

The external provider (manufacturer) of the software.

Tenprint

A generic reference to a controlled recording of a person's (subject's) fingers (available digits) and palms using a medium on a contrasting background. See print.

Threshold (Verb) / Filter (Verb)

Eliminate biometric samples that have failed to attain a level of any type of score such as quality score, comparison score. [Adapted from ISO/IEC 2382-37:2017 Information Technology – Vocabulary – Part 37: Biometrics]

User Acceptance Testing

A series of exercises/tests designed to determine whether or not a method or process fulfils the stated user requirement.

Validation

The process of providing objective evidence that a method, process or device is fit for the specific purpose intended.

Validation Library

A collection of documents relevant to the validation. Included are such things as technical documentation of search models and test results.

Verification

The confirmation through the assessment of existing evidence or through experiment that a method, process or device is fit (or remains fit) for the specific intended purpose. This includes an overriding requirement that there is evidence that the forensic unit's own competent staff can perform the method at a given location.

Virtual Bureau

An isolated area within the system that mirrors the content and functionality of the algorithm but does not impact upon the live data. This separate environment on the Automated Fingerprint Identification System acts as a testing and/or training facility.

Published by:
The Forensic Science Regulator
5 St Philip's Place
Colmore Row
Birmingham
B3 2PW
www.gov.uk/government/organisations/forensic-science-regulator