Sensor Dependency in Efficient Fingerprint Image Protection using Selective JPEG2000 Encryption

Martin Draschl, Jutta Hämmerle-Uhl, and Andreas Uhl
Department of Comuter Sciences, University of Salzburg, Austria
Email: uhl@cosy.sbg.ac.at

***Abstract*—Biometric system security requires cryptographic protection of sample data under certain circumstances. We assess low complexity selective encryption schemes applied to JPEG2000 compressed fingerprint data by conducting fingerprint recognition on the selectively encrypted data. This paper specifically investigates the effect of considering different sensors for data acquisition and finds significant dependency of optimal encryption settings on the sensor employed.**

I. Introduction

The International Organization for Standardization (ISO) specifies biometric data to be recorded and stored in (raw) image form (ISO/IEC FDIS 19794), not only in extracted templates (e.g. minutiae-lists or iris-codes). On the one hand, such deployments benefit from future improvements (e.g. in feature extraction stage) which can be easily incorporated without re-enrollment of registered users. On the other hand, since biometric templates may depend on patent-registered algorithms, databases of raw images enable more interoperability and vendor neutrality [1].

The certainly most relevant standard for compressing image data relevant in biometric systems is JPEG2000, suggested for lossy compression of fingerprint images in the ISO/IEC 19794 standard suite on Biometric Data Interchange Formats and the ANSI/NIST-ITL 1-2011 standard on "Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information" (former ANSI/NIST-ITL 1-2007).

In (distributed) biometric recognition, biometric sample data is sent from the acquisition device to the authentication component and can eventually be read by an eavesdropper on the channel. Also, biometric enrollment sample databases as mentioned before can be compromised and the data misused in fraudulent manner. Therefore, these data, often stored as JPEG2000 data as described before, require cryptographic protection for storage and transmission.

In this paper, taking into account the restrictions of biometric cryptosystems, cancelable biometrics, and homomorphic encryption techniques [2], we investigate lightweight encryption schemes for JPEG2000 compressed fingerprint sample data based on selective bitstream protection. It is important to notice that, being based on classical AES encryption, matching in the encrypted domain is not supported. However, our proposed technique offers extremely low computational effort and there is absolutely no impact on recognition accuracy once the data are decrypted. Still, in case a full AES encryption of the data is feasible in terms of computational resources, this option is always perferable due to unquestioned security. Thus, the proposed approach is especially useful for protection of transmission between sensor and feature extraction / matching modules when involving low-powered devices and for the encryption of vast user sample datasets (like present in the Unique Identification Authority of India's (UID) Aadhaar project) where matching in the encrypted domain is not an absolute prerequisite for sensible deployment.

Section 2 introduces principles of encrypting JPEG2000 data and specifically describes the approach as used in this paper. The target fingerprint recognition schemes as used in the experiments are sketched in Section 3. Section 4 describes a large corpus of experiments, where we specifically assess the security of the proposed encryption schemes by applying fingerprint recognition to the (attacked) encrypted data. Section 5 presents the conclusions of this paper.

II. Efficient Encryption of Fingerprint Data

A. JPEG2000 Encryption in the Biometric Context

A large variety of custom image and video encryption schemes have been developed over the last years [3], many of them being motivated by the potential reduction of computational effort as compared to full encryption (see e.g. a depreciated scheme for fingerprint image encryption [4]). Reducing computational encryption effort is of interest in the context of biometric systems in case either weak hardware (e.g. mobile sensing devices) or large quantities of data (e.g. nation-wide sample databases) are involved.

However, when encrypting a JPEG2000 file (or any other media file) in a non format-compliant manner it is not possible to assess the security of the chosen encryption strategy since the encrypted file can not be interpreted by decoding soft- or hardware (this specifically applies to selective or partial encryption schemes which protect a specific part of a codestream only). But for assessing security (e.g. applying corresponding image quality metrics, or, as done in the present paper, attempting to use the protected data in the target application context), encrypted visual data usually need to be decoded and converted back into pictorial information.

Thus, an actual biometric system will opt to employ a non format-compliant encryption variant in its deployment installation (e.g. to decrease computational cost or to disable common decoders to interpret the data). However, we will consider the corresponding format-compliant counterpart to facilitate security assessment of the chosen scheme (while the results are equally valid for the corresponding non-compliant variants).

For JPEG2000, [5] provides a comprehensive survey of encryption schemes. In our target application context, only

bitstream oriented techniques are appropriate, i.e. encryption is applied to the JPEG2000 compressed data, as fingerprint data might be compressed right after acquisition but encrypted much later. In a JPEG2000 codestream either packet headers or packet body data (or both) may be encrypted. For reasons explained in [2], we consider encryption of packet body data in this work, while additional packet header encryption may be used to further strengthen the schemes discussed [6].

B. Selective JPEG2000 Encryption Approaches

In the following, we introduce a systematic approach to assess selective encryption techniques wrt. the question how to apply encryption to different parts of the JPEG2000 codestream.

We aim to achieve format compliance to enable security assessment as discussed above, while actual encryption schemes deployed in practice would not care about format compliance (while still following the same approaches where and to which extent encryption should be applied). Each packet within the JPEG2000 code stream eventually contains start of packet header (SOP) and end of packet header (EOP) markers. For this purpose, the used encoding software, i.e. JJ2000, is executed with the $-Psop$ and $-Peph$ options which enable these optional markers. These markers are used for orientation within the file and for excluding all header information from the encryption process. Additional care must be taken when replacing the packet data with the generated encrypted bytes. If the result of the encryption operation results in a value of a SOP or EOP header marker (or any other non-admissible packet value), a second encryption iteration is conducted to maintain format-compliance [7].

In the following, we consider a specific type of selective encryption methodology, i.e. "Windowed Encryption", which is used to accurately spot the encryption location in the JPEG2000 bitstream with the biggest impact (in our context on matching rates when automated fingerprint identification systems (AFIS) are applied to encrypted data). "Windowed Encryption" is operated by moving a fixed window (of the size of some percent of the filesize in our experiments) across the packet data. While the percentage of encrypted data does not change during the experiments, only the position of the window is changed in fixed steps within packet data. In this manner, recognition experiments on the protected data reveal the parts of the JPEG2000 codestream that contain the most "valuable" fingerprint information exploited by the different AFIS for matching purposes, i.e. that is most sensitive if protected by encryption.

In recent work [2] we have compared different ways how to apply encryption to different parts of a fingerprint-image JPEG2000 codestream, specifically focusing on the question if encryption should preferably be applied to one single chunk of data right at the start of the codestream ("Absolute Encryption") or if it is better to encrypt smaller contiguous chunks distributed over the packets of the codestream ("Sequential Encryption" and "Distributed Encryption"). While the corresponding results indicate highest security for the approach distributing the encryption as uniformly as possible across the codestream (thus favoring "Distributed Encryption"), experiments have been limited to the minutiae-based NIST NBIS AFIS system and have ignored the question which are the most sensitive, i.e. confidentiality-relevant, parts of the codestream.

In applying "Windowed Encryption" in subsequent work [8], we have been looking into the question if the location of the most sensitive parts of the JPEG2000 codestream depends on (i) the AFIS employed to attempt recognition on the protected data and on (ii) the progression order of the JPEG2000 codestream. The latter question has been discussed in general JPEG2000 selective encryption schemes and it has been found that the choice of either protecting layer progressive or resolution progressive JPEG2000 codestreams indeed has a significant impact wrt. the extent of confidentiality achieved [9].

In this work, we will adopt the methodology of [8] to investigate if the location of the most sensitive parts of the JPEG2000 codestream additionally also depends on the sensor used to acquire the data. If this is indeed found to be true, each specific application scenario has to be optimised separately wrt. the most efficient selective encryption configuration as significant AFIS type dependency has already been demonstrated [8].

1) Security Assessment: When assessing the security of format compliantly encrypted visual data, the data can simply be decoded with the encrypted parts (called "direct decoding"). Due to format compliance, this is possible with any given decoding scheme, however, the encrypted parts introduce noise-type distortion into the data which kind of overlay the visual information still present in the data (see Fig. 1). An informed attacker can certainly do better than this naive approach. Therefore, a highly efficient attack is obtained when removing the encrypted parts before decoding and replacing them by suited data minimising error metrics. This can be done most efficiently using codec specific error concealment tools, which treat encrypted data like any type of bitstream error ("error concealment attack"). Thus, any serious security analysis needs to consider encrypted imagery being attacked using this error concealment approach at least. The JJ2000 version used in the experiments includes the patches and enhancements to JPEG2000 error concealment provided by [10], [8].

As visible in Fig. 1 (leftmost two images) especially after error concealment attacks ridge and valley information can still be present, which could be improved further with fingerprint specific quality enhancement techniques (thus, images like those cannot be assumed to be sufficiently secured). Only the error concealment example with better protection in Fig. 1 (rightmost image) does no longer exhibit any fingerprint related structures which could be exploited by an attacker.

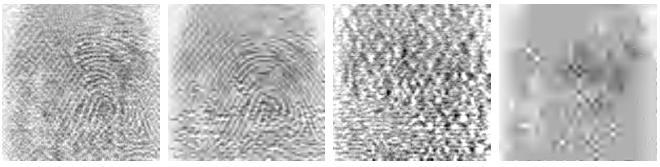

Figure 1. Examples - Distributed Encryption (0.5% encrypted with direct reconstruction and error concealment; the same for 3.0% encrypted)

The general assessment of the security of low quality encrypted visual data (as obtained by direct decoding or error

concealment attacks) is difficult. Although classical image and video quality metrics (IVQM) like SSIM or even PSNR have been repeatedly applied to such data, it has been shown recently that this does not correlate well to human perception [11]. Also, IVQM specifically developed to assess the security (i.e. confidentiality / protection level) of encrypted visual data have been recently shown not to meet the design expectations [12]. Moreover, the general quality appearance to human observers is not at all relevant in our setting. Only the assessment of forensic fingerprint experts would meake sense in terms of human judgement.

However, in our case, security assessment does not need to rely on human specialists – since our application context is highly specific and well defined, we apply AFIS to the protected data to verify if the protection is sufficiently strong to prevent the use of the encrypted fingerprint data in an automated recognition context.

III. Fingerprint Recognition

Different types of AFIS react differently to image degradations. Therefore, we will consider fundamentally different types of fingerprint feature extraction and matching schemes, based on the discriminative characteristics fingerprints do contain [13]:

Correlation-Based Matcher: These approaches use the fingerprint images in their entirety, the global ridge and valley structure of a fingerprint is decisive. Images are correlated at different rotational and translational alignments, image transform techniques may be utilised for that purpose. As a representative of this class, we use a custom implementation of the phase only correlation (POC) matcher [14] the details of which are described in recent work [15].

Ridge Feature-Based Matcher: Matching algorithms in this category deal with the overall ridge and valley structure in the fingerprint, yet in a localised manner. Characteristics like local ridge orientation or local ridge frequency are used to generate a set of appropriate features representing the individual fingerprint. As a representative of the ridge feature-based matcher type we use a custom implementation of the fingercode approach (FC) [16] the details of which are described in recent work [15].

Minutiae-Based Matcher: The set of minutiae within each fingerprint is determined and stored as list, each minutia being represented (at least) by its location and direction. The matching process then basically tries to establish an optimal alignment between the minutiae sets of two fingerprints to be matched, resulting in a maximum number of pairings between minutiae from one set with compatible ones from the other set. As the first representative of the minutiae-based matcher type we use *mindtct* and *bozorth3* from the "NIST Biometric Image Software" (NBIS, denoted "BOZ" in the plots) package (available at http://fingerprint.nist.gov/NBIS/) for minutiae detection and matching, respectively. Additionally, to complement NBIS with a commercial system, we habe employed the Griaule Biometrics Fingerprint SDK 2009 (GF – http://www.griaulebiometrics.com/). It has been honored to be " *[..] the most precise in the open category*" at the Fingerprint Verification Competition (FVC) in 2006. One of the important differences to NBIS is the consideration of 3 minutiae interconnected by polygons where in matching, internal angles, sides and each minutia angle are computed.

IV. Experiments

A. Experimental Settings

All experiments are based on images taken from databases of the 2004 Fingerprint Verification Competition (FVC). In particular, our results are based on set A of the three natural datasets of the FVC 2004 (DB1: Optical sensor, 500dpi, 640×480 pixels resolution, DB2: Optical sensor, 500dpi, 328 pixels resolution, and DB3: thermal sweeping sensor, 512 dpi, 300×480 pixels resolution). Set A contains 100 different fingers (8 imprints each).

Images are compressed into lossless JPEG2000 format using JJ2000 in layer as well as resolution progressive ordering, respectively. Subsequently they are encrypted using the different variants of "Windowed Encryption" with different positions where to start the encryption. Subsequently data are either directly decoded or decoded with enabled error concealment with the JJ2000 variant mentioned [10].

The procedure used for matching the decoded / encrypted fingerprint images is chosen to be exactly the same as FVC demands for performance evaluation [2], [8]. Overall, we consider equal error rate (EER) and receiver operating curves (ROC) to compare the protection capabilites of the different encryption schemes. Obviously, higher EER corresponds to better data protection as well as worse ROC behaviour is preferred for better data protection.

B. Experimental Results

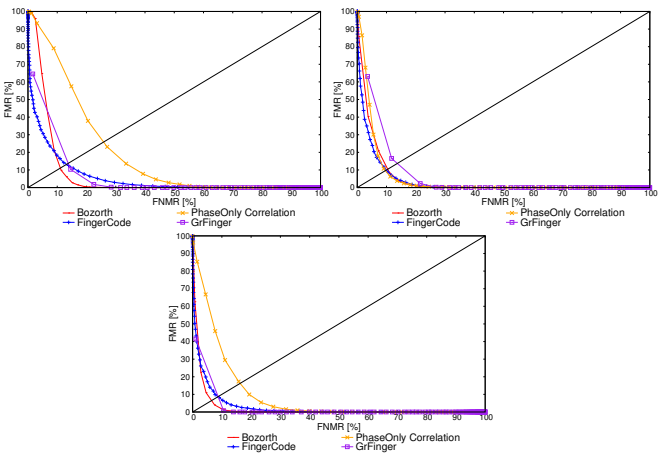

Figure 2. ROC on plaintext datasets DB1 - DB3 of FVC2004 data.

Fig. 2 displays the recognition performance in terms of ROC measured on unencrypted data with the four AFIS considered. We notice a very different behaviour for the three datasets. On DB1 and DB3, for FMR < 10%, NBIS exhibits the lowest FNMR followed by GF, FC and POC. For larger FMR, POC stays the worst technique, but FC and GF take the lead while NBIS looses performance. On DB2, POC is the best performing technique for FMR < 10%, while GF is the worst performing one across the entire range of ROC parameters. FC is best performing for FMR > 10%. So overall,

we observe a comparable ranking of the four AFIS on datasets DB1 and DB3, although these data are fairly different (visually and in terms of sensor technology), while the results for DB2 are very different even though the capturing device is also an optical sensor (and thus could be expected to behave similarly to DB1).

Fig. 3 shows results in case Windowed Encryption is applied to 2% of the JPEG2000 packet data of a bitstream in *layer progressive* ordering. The range of encryption is varied from the start of the bitstream (0.0%) in 0.2% steps and we display the EER values for direct reconstruction and error concealment reconstruction (the latter denoted as "seg" in the plots' legend). The three plots show the results for the three datasets considered.

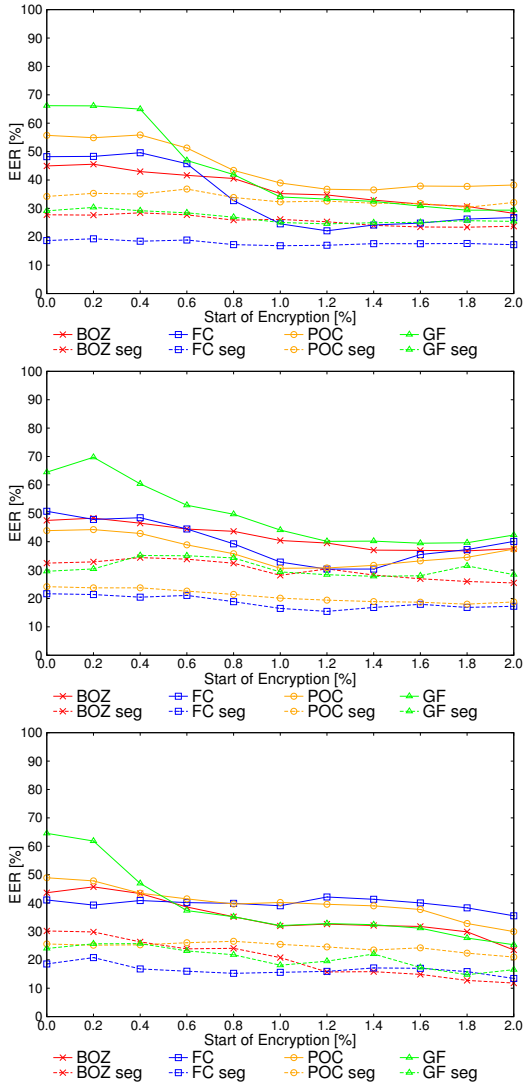

Figure 3. EER for DB1 - DB3 when windowed encryption is applied to JPEG2000 data in layer progressive ordering at different starting positions.

The highest EER (i.e. best protection) is seen when GF recognition is conducted on directly reconstructed data which is encrypted right from the bitstream start (0.0 - 0.4% on the x-axis) no matter which dataset is considered. However, the lowest EER (i.e. worst protection) when considering direct reconstruction is highly data set dependent: For DB1, it is obtained for FC at 1.2% of the data (EER $\approx$ 25%), for DB2 it is obtained for FC/POC at 1.2% of the data (EER $\approx$ 32%), and for DB3 it is obtained for NBIS at 2% of the data (EER $\approx$ 23%). Thus, we have a high dependence on datasets and actual AFIS used. However, as discussed before, error concealment reconstruction is more important for security assessment.

The highest EER (i.e. best protection) on data reconstructed with error concealment is also dataset dependent as follows: For DB1, it is observed for POC recognition starting at 0.6% of the data (EER $\approx$ 38%), for DB2 it is observed for GF also at 0.6% of the data (EER $\approx$ 36%), and for DB3 it is observed for NBIS at bitstream start (EER $\approx$ 30%). On the other hand, the lowest EER (worst protection), is seen for both DB1 and DB2 for FC recognition at 1.0% and 1.2% of the data respectively (EER $\approx$ 19% and 16%). For DB3, the lowest EER is attained for NBIS at 2.0% of the data with EER $\approx$ 12% only. Overall, when considering EER only, we observe very significant dependence on the datasets considered when looking for the most and least secure protection strategies (i.e. most and least sensitive areas of the bitstream).

To provide more insight on the entire ROC range, we exemplary visualise ROC plots of NBIS recognition comparing the three datasets and again varying the position encyption is applied to the bitstream. Here (Fig. 4), data is again considered in *layer progressive* ordering and only error concealment reconstruction is considered.

We are able to constitute different ROC behaviour for the three datasets. While the worst results in terms of protection (lowest error values) are identical for all three datasets (i.e. starting at 1.8% and 2.0% of the data), the best results (highest error rates) are dataset dependent: Starting the encryption at 0.4% and 0.6% of the data for DB1 and DB2 and at 0.0% and 0.2% for DB3.

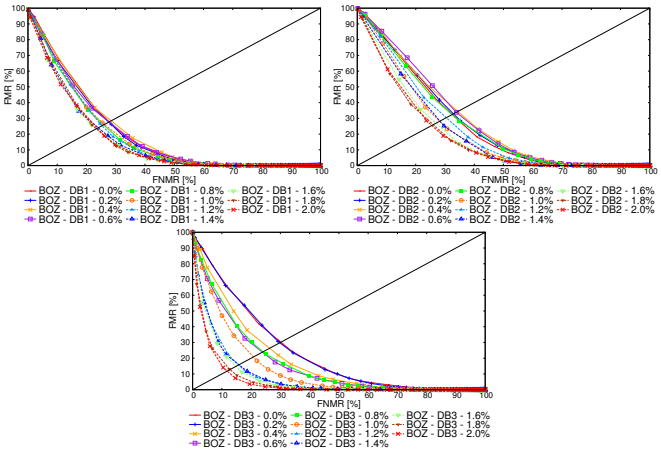

Figure 4. ROC for DB1 - DB3 for data in layer progressive ordering using NBIS under error concealment.

What is even more striking, is the different range of error results seen for the three datasets (i.e. the spread of the different curves representing the different encryption starting positions). While for DB1, the variability is rather low (e.g. EER in $[22, 29]$), it is much higher for DB3 (in $[11, 30]$). EER variability for DB2 is in $[25, 34]$.

Having observed the different results when comparing optimal encryption configuration for image data in JPEG2000 layer and resolution progressive ordering [8], we discuss *resolution progressive* JPEG2000 data in the following. Fig. 5 shows results in case Windowed Encryption is applied to 2% of the JPEG2000 packet data of a bitstream.

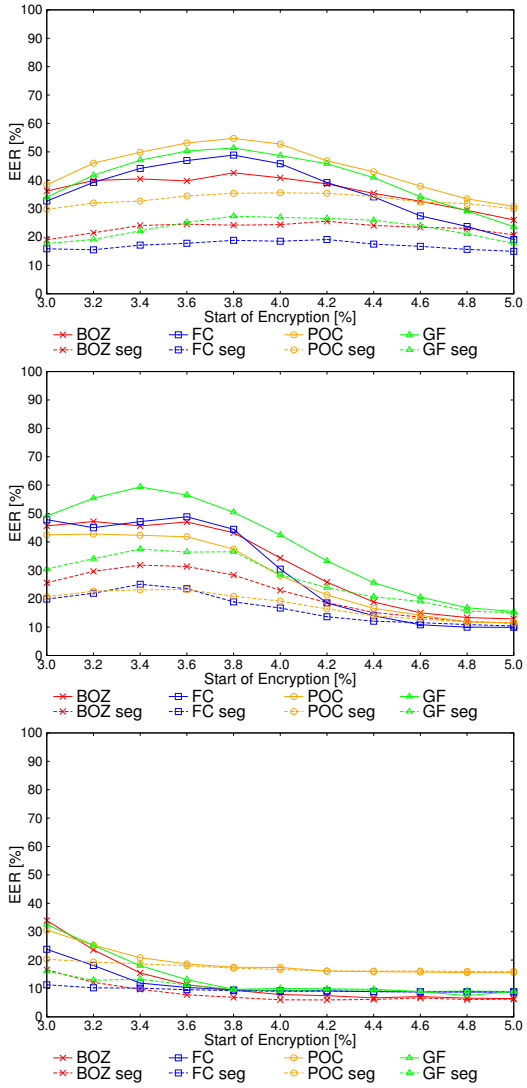

Figure 5. EER for DB1 - DB3 when windowed encryption is applied to JPEG2000 data in resolution progressive ordering at different starting positions.

By analogy to the case of layer progressive ordering before, the range of encryption is varied in 0.2% steps and we display the EER values for direct reconstruction and error concealment reconstruction (the latter denoted as "seg" in the plots' legend). The three plots show the results for the three datasets considered where the location of the encryption start has been selected in accordance to earlier results on most sensitive bitstream parts in resolution progressive bitstream organisation [8], i.e. at 3% of the bitstream length.

When comparing the overall shape of the results, we immediately recognise an effect caused by the dependency of the results on the sensor used. For the DB1 results, we notice a bump-like shape almost in the centre of the plot, while the bump is shifted to the left for DB2 and not present at all (even more shifted to the left) for DB3. Since the start position of the encryption has been determined based on results of [8] (which in turn is based on set B of all the FVC datasets) this effect already underpins the significant influence of the sensor used to capture the data.

Discussing directly reconstructed data first, the highest EER (best protection) is attained at encryption start 3.8% with POC (DB1, EER $\approx$ 57%) and at 3.4% with GF (DB2, EER $\approx$ 60) while the corresponding DB3 values is located at starting position clearly $<$ 3.0% of the data (but not in the depicted range). Lowest EERs for directly reconstructed data (worst protection) are seen at start 5.0% with EER $\approx$ 19% using FC (DB1, but with even lower values outside of the plot range), at start 5.0% with EER $\approx$ 10% (DB2) using FC, and at start 5.0% with EER $\approx$ 8% using NBIS (DB3). Thus, when comparing the values to layer progressive JPEG2000 bitstream organisation we are able to confirm earlier results [8] that the type of bitstream progrssiveness has significant impact on the parameters for deploying optimal selective encryption. And again, we observe high dependence on the sensor considered.

The results for data after error conceralment attack exhibit similar data / sensor dependencies. The highest EERs are delivered by POC recognition (DB1, start at 4.0%, EER $\approx$ 35) or GF recognition (DB2, start at 3.4%, EER $\approx$ 37), while the highest EER for DB3 also for this setting is outside of the plot range. Lowest EERs after error concealment are found for FC (DB1 and DB2 starting at 5.0% of the data with EERs of 15% and 10%, respectively) and NBIS (DB2, also at 5.0% of the data with EER $\approx$ 8%). Thus, results differ in dependency of the underlying dataset wrt. optimal encryption location and the most and least successful recognition scheme.

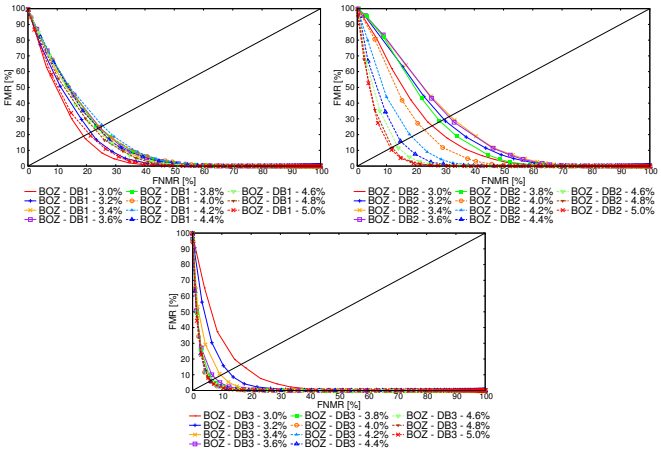

Figure 6. ROC for DB1 - DB3 for data in resolution progressive ordering using NBIS under error concealment.

To once more provide more insight on the entire ROC range, we exemplary visualise ROC plots of NBIS and FC recognition comparing the three datasets and again varying the position encyption is applied to the bitstream organised in *resolution progressive* organisation. Fig. 6 shows the NBIS results. In addition to the different spreads of the curves already noted for data in layer progrssive ordering we notice even

more varying behaviour: For DB1, starting encryption at 0.0% (the bitstream start) leads to "best" ROC behaviour (worst protection), while for DB3, this leads to the best protection setting (for DB2, starting encryption at the beginning leads to mediocre results). Additionally, the range of EERs is again *very* different: [18,26] for DB1, [12,32] for DB2, and [5,17] for DB3.

Also the results for FC as shown in Fig. 7 exhibit results with significant sensor dependency: Considerably different ranges of EERs (and of course correspondingly highly varying overall ROC behaviour) – [15,18] for DB1, [10,25] for DB2, and [8,11] for DB3 – as well as different encryption starting positions leading to best or worst ROC behaviour, e.g. the configuration starting to encrypt at 4.2% of the data leads to "worst" ROC behaviour for DB1 (most secure), while for DB2 and DB3 it is one of the least secure options.

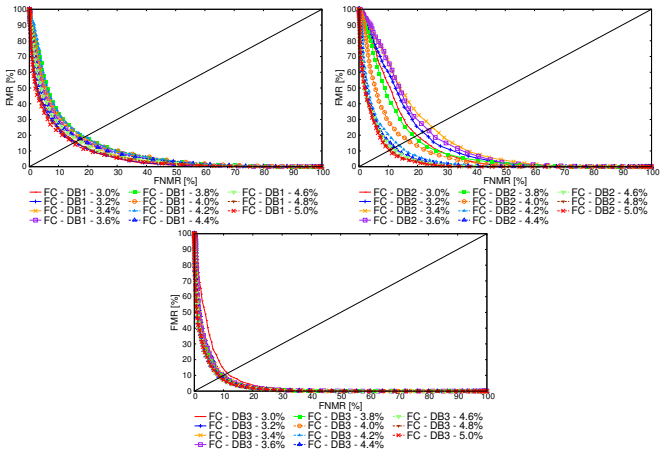

Figure 7. ROC for DB1 - DB3 for data in resolution progressive ordering using FC under error concealment.

V. Conclusion

We have investigated the sensitivity of certain parts of fingerprint data compressed into JPEG2000 format wrt. selective protection / encryption. Evaluations are done by comparing AFIS recognition performance on encrypted data after conducting attacks. We have found that sensitivity / robustness against partially encrypted data is highly dependent on the sensor used to acquire the data under investigation. Also, results have confirmed high dependence on the actual recognition scheme used and do not correspond to the recognition performance ranking of the different AFIS seen on clear data. Moreover, there is a significant difference if the JPEG2000 codestream is organised in layer progressive or resolution progressive ordering. Overall it can be stated that it is not possible to formulate general guidelines which parts of the JPEG2000 bitstream are most sensitive against protection (i.e. carry the information most important to AFIS recognition success). Thus, given a fingerprint recognition system, a protection scheme aiming to employ selective encryption of the FP images' JPEG2000 bitstream needs to be carefully tuned for the specific combination of FP sensor used to acquire the data and AFIS employed in recognition for optimal protection performance.

Acknowledgment

This work has been partially supported by the Austrian Science Fund, project no. 27776, and by the ICT COST Action IC1206 "De-identification for privacy protection in multimedia content".

References

[1] C. Rathgeb, A. Uhl, and P. Wild, *Iris Recognition: From Segmentation to Template Security*, ser. Advances in Information Security. Springer Verlag, 2013, vol. 59.

[2] M. Draschl, J. Hämmerle-Uhl, and A. Uhl, "Efficient fingerprint image protection principles using selective JPEG2000 encryption," in *Proceedings of the 1st Workshop on Sensing, Processing and Learning for Intelligent Machines (SPLINE 2016)*, Aalborg, Denmark, 2016, pp. 1–6.

[3] A. Uhl and A. Pommer, *Image and Video Encryption. From Digital Rights Management to Secured Personal Communication*, ser. Advances in Information Security. Springer-Verlag, 2005, vol. 15.

[4] D. Engel, E. Pschernig, and A. Uhl, "An analysis of lightweight encryption schemes for fingerprint images," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 173–182, Jun. 2008.

[5] D. Engel, T. Stütz, and A. Uhl, "A survey on JPEG2000 encryption," *Multimedia Systems*, vol. 15, no. 4, pp. 243–270, 2009.

[6] ——, "Format-compliant JPEG2000 encryption with combined packet header and packet body protection," in *Proceedings of ACM Multimedia and Security Workshop, MM-SEC '07*. New York, NY, USA: ACM Press, Sep. 2007, pp. 87–95.

[7] T. Stütz and A. Uhl, "On format-compliant iterative encryption of JPEG2000," in *Proceedings of the Eighth IEEE International Symposium on Multimedia (ISM'06)*. San Diego, CA, USA: IEEE Computer Society, Dec. 2006, pp. 985–990.

[8] M. Draschl, J. Hämmerle-Uhl, and A. Uhl, "Assessment of Efficient Fingerprint Image Protection Principles using different Types of AFIS," in *Proceedings of the 18th International Conference on Information and Communications Security (ICICS'16)*, ser. Springer LNCS, Singapore, 2016.

[9] R. Norcen and A. Uhl, "Selective encryption of the JPEG2000 bitstream," in *Communications and Multimedia Security. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '03*, ser. Lecture Notes on Computer Science, A. Lioy and D. Mazzocchi, Eds., vol. 2828. Turin, Italy: Springer-Verlag, Oct. 2003, pp. 194 – 204.

[10] T. Stütz and A. Uhl, "On JPEG2000 error concealment attacks," in *Advantages in Image and Video Technology: Proceedings of the 3rd Pacific-Rim Symposium on Image and Video Technology, PSIVT '09*, ser. Lecture Notes in Computer Science. Tokyo, Japan: Springer, Jan. 2009, pp. 851–861.

[11] H. Hofbauer and A. Uhl, "Visual quality indices and low quality images," in *IEEE 2nd European Workshop on Visual Information Processing*, Paris, France, Jul. 2010, pp. 171–176.

[12] ——, "Identifying deficits of visual security metrics for images," *Signal Processing: Image Communication*, vol. 46, pp. 60 – 75, 2016.

[13] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition (2nd Edition)*. Springer-Verlag, 2009.

[14] I. Koichi, N. Hiroshi, K. Koji, A. Takafumi, and H. Tatsuo, "A fingerprint matching algorithm using phase-only correlation," *IEICE Transactions on Fundamentals*, vol. E87-A, no. 3, pp. 682–691, Mar. 2004.

[15] J. Hämmerle-Uhl, M. Pober, and A. Uhl, "Towards standardised fingerprint matching robustness assessment: The stirmark toolkit – cross-feature type cmparisons," in *Proceedings of the 14th IFIP International Conference on Communications and Multimedia Security (CMS'13)*, ser. Springer Lecture Notes on Computer Science, vol. 8099, Magdeburg, Germany, Sep. 2013, pp. 3–17.

[16] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based Fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.