Assessment of Efficient Fingerprint Image Protection Principles using different Types of AFIS

Martin Draschl, Jutta Hämmerle-Uhl, and Andreas Uhl

Visual Computing and Security Lab (VISEL)
Department of Computer Sciences, University of Salzburg, Austria
uhl@cosy.sbg.ac.at

Abstract. Biometric system security requires cryptographic protection of sample data under certain circumstances. We assess the impact of low complexity selective encryption schemes applied to JPEG2000 compressed fingerprint data when protected data is subjected to different types of automated fingerprint recognition schemes (AFIS). Results indicate that the obtained security is highly dependent on the type of AFIS applied, but also on the progression order of the underlying JPEG2000 codestream. Still we are able to identify general trends independent of the applied AFIS and determined by the chosen progression order, thus enabling the design of generic protection principles.

1 Introduction

The International Organisation for Standardisation (ISO) specifies biometric data to be recorded and stored in (raw) image form (ISO/IEC 19794 specifies JPEG2000 [1] for lossy fingerprint image compression), 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. These facts motivate detailed investigations and optimisations of image compression in biometrics (see e.g. for face detection and iris recognition [2, 3]) in order to provide an efficient storage and rapid transmission of biometric records.

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 (these are designed to support template security as well as matching and partially suffer from questionable security and high computational demand), we investigate options for a lightweight encryption scheme for JPEG2000 compressed fingerprint data. In particular we consider the interplay between applying different types of automated fingerprint identification systems (AFIS) to the protected data and the achieved level of security / data protection

when the JPEG2000 data is given in different progression orders. 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 preferable due to unquestioned security. Thus the investigated 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 applied in this paper. Fingerprint recognition schemes as used in the paper are sketched in Section 3. Section 4 describes experiments, where we systematically assess the security of the proposed encryption scheme by applying different types of fingerprint recognition schemes to the (attacked) encrypted data. Section 5 presents the conclusions of this paper.

2 Efficient Encryption of Fingerprint Data

2.1 JPEG2000 Encryption in the Biometric Context

A large variety of custom image and video encryption schemes have been developed over the last years [4, 5], 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 [6]). 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, [7] 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. We consider encryption of packet body data in this work, while additional packet header encryption may be used to further strengthen the schemes discussed [8].

2.2 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 [9].

In the following, we introduce 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 AFIS-based recognition is applied to encrypted data). In recent work [10] 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" we will look 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 (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 confidentiality achieved [11].

"Windowed Encryption" as shown in Fig. 1 is operated by moving a fixed window (of the size of one percent of the filesize in our experiments) across the packet data, the percentage of encrypted data does not change during the experiments. Instead, only the position of the one percent window is changed in one percent steps within packet data.

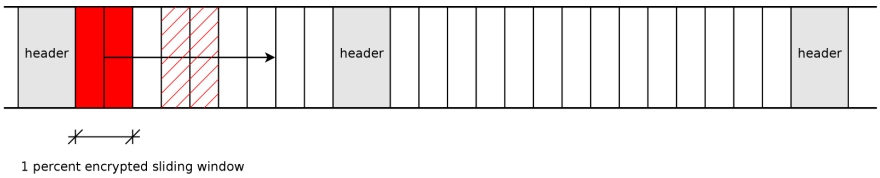

Fig. 1. Windowed Encryption mode

In this manner, recognition experiments on the protected data reveal the parts of the JPEG2000 codestream that contains the most "valuable" fingerprint information exploited by the different AFIS for matching purposes, i.e. that is most sensitive if protected by encryption.

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. 3). 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 (termed "replacement attack [12]) which has been successfully conducted in the JPEG2000 context [11]. 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"). The JJ2000 version used in the experiments includes the patches and enhancements to JPEG2000 error concealment provided by [13]. It fixes issues within the error concealment code found in the original code and improves results noticeably. The basic version of JJ2000 uses a simple resetting strategy as error concealment method while the version used enables JJ2000 to reset the coefficients on bitplane basis.

As visible in Fig. 3 even after error concealment attacks ridge and valley information can still be present, which could be improved further with fingerprint specific quality enhancement techniques (images like those displayed cannot be assumed to be sufficiently secured). Thus, the final design goal for a secure fingerprint encryption scheme is to get rid of this residual ridge information.

The general assessment of the security of low quality encrypted visual data 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 [14]. 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 [15]. Moreover, the general quality appearance to human observers is not at all relevant in our setting. Only the assessment of forensic fingerprint experts would make 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 fingerprint

recognition algorithms (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.

3 Fingerprint Recognition

Different types of fingerprint recognition schemes 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 [16]:

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 [17] the details of which are described in recent work [18].

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) [19] the details of which are described in recent work [18].

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 representative of the minutiae-based matcher type we use *mindtct* and *bozorth3* from the "NIST Biometric Image Software" (NBIS) package (available at `http://fingerprint.nist.gov/NBIS/`) for minutiae detection and matching, respectively.

4 Experiments

4.1 Experimental Settings

All experiments are based on images taken from databases of the Fingerprint Verification Competition (FVC). In particular, our results are based on set B of all 4 datasets of the years 2000, 2002 and 2004. Set B contains a subset of 10 fingers (8 imprints each) of each of the four datasets in each year, thus leading to 120 fingers overall. This strategy is chosen to have a high diversity of fingerprint sensors represented in the data.

Images are compressed into lossless JPEG2000 format using JJ2000 in layer progressive and resolution progressive ordering. Subsequently they are encrypted using the different positions in "Windowed Encryption" by shifting the encryption window across

the data as described and subsequently either directly decoded or decoded with enabled error concealment with the JJ2000 variant mentioned [13].

The procedure used for matching the decoded / encrypted fingerprint images is chosen to be the same as FVC demands for performance evaluation. In a first run, every sample of a finger is matched against all other samples of the same finger from that dataset. Symmetric matches are not taken into account. Based on this run the False Non Match Rate (FNMR) is calculated. A second run is performed matching the first impression of each finger against all other first images of all fingers from that dataset. Again symmetric matches are not evaluated. The results of these matches are used for the calculation of the False Matching Rate (FMR). Overall, we will consider equal error rate (EER) and receiver operating curves (ROC) to compare the protection capabilities of the different encryption schemes. Obviously, higher EER correspond to better data protection as well as worse ROC behaviour is preferred for better data protection. Windowed Encryption experiments involve all three AFIS types described.

4.2 Experimental Results

In the following, we will apply Windowed Encryption and will assess the sensitivity towards location of the protected data when using different types of AFIS. Fig. 2 shows the ROC behaviour of the three recognition schemes when applied to plain (unprotected, i.e. unencrypted) data. NBIS exhibits the best behaviour except for very low FNMR where FC is better, POC exhibits the worst behaviour, except for high FNMR, where it is superior to FC.

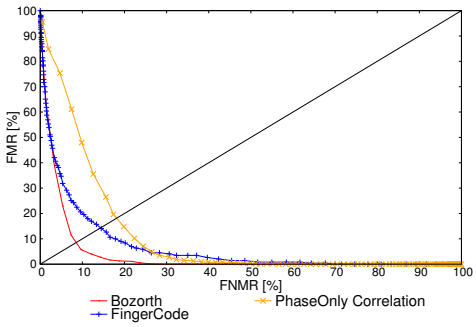

Fig. 2. ROC - Reference matches set B

In Fig. 3 image examples for Windowed Encryption are given where encryption starts right at the first packet data and only 0.5% of the bitstream are encrypted. The visual impression confirms that error concealment indeed is able to reveal data which seems to be protected under direct decoding. This fact has been already observed [10] and its implication for fingerprint image security under partial encryption has been extensively discussed.

The first results are obtained when encrypting layer progressive JPEG2000 codestreams. Fig. 4 shows the effects of Windowed Encryption using NBIS for recognition.

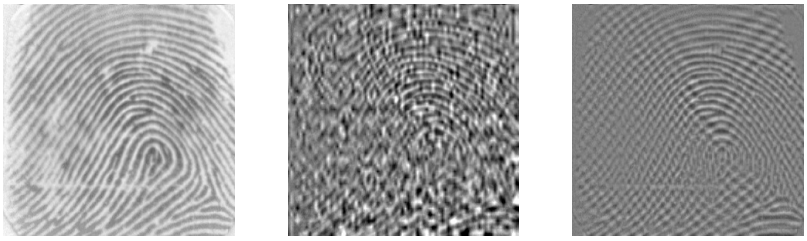

Fig. 3. Encryption Examples - original, 0.5% encrypted with direct reconstruction and error concealment, respectively.

Results are very clear in that the further the encryption window is moved away from the bitstream start, the less secure the scheme gets. This is true for direct decoding as well as for error concealment. When encrypting data at positions starting at 10% of the data or later, recognition "degrades" to the unprotected case (see Fig. 2) for direct decoding, the same is true at 8% or later for error concealment. It is obvious that in general, conducting an error concealment attack only slightly reduces security.

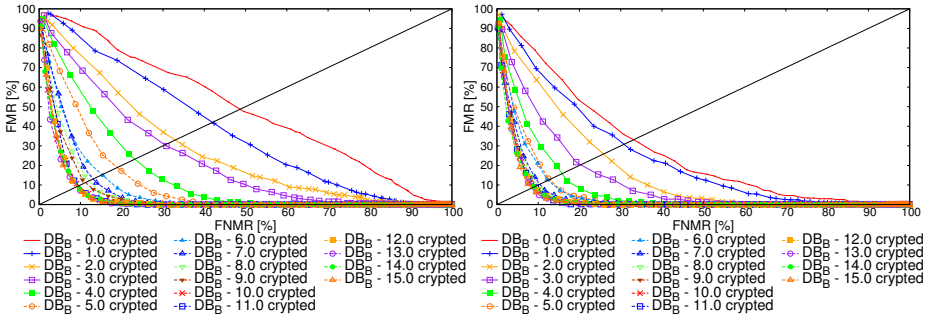

Fig. 4. ROC - Windowed Encryption (NBIS) - direct reconstruction vs. error concealment attack.

Fig. 5 exhibits a fairly different behaviour for FC. For direct encoding, recognition is "down" to the unprotected behaviour already when starting encryption at 6% or later. Additionally, is turns out to be more secure to encrypt starting at 2% data as compared to starting at 1%. Apart from that, the "natural order" (i.e. less secure when encrypting parts farther away from the codestream start) is preserved. The more significant differences however are seen when error concealment is used. FC is obviously very well capable to handle encrypted data and apart from encrypting right from the bitstrems start, almost no protection at all can be achieved. This result indicates that different types of recognition schemes are able to handle encrypted data to a very different extent (here, robustness of FC is clearly superior to NBIS for the encryption effects introduced).

Fig. 6 visualises the POC results. For direct decoding, degradation to unprotected behaviour is also seen for encryption starts at 6% of the data or later. Apart from a slight mingling of 1% and 2% start position, applying encryption closer to the start of the data leads to more secure results. For error concealment, degradation to unprotected behaviour is found at the same position and the relative ordering is entirely following

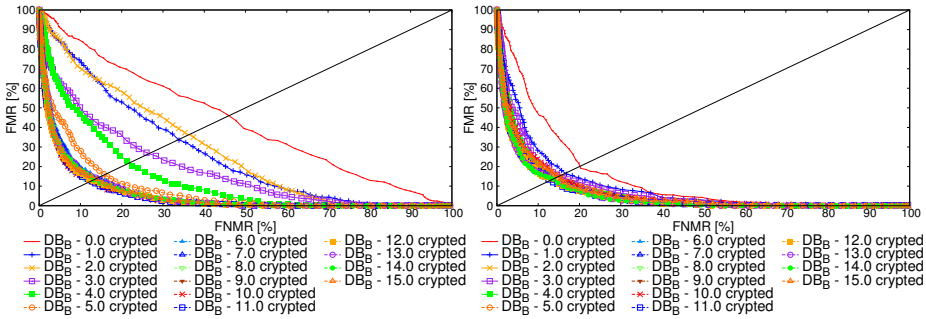

Fig. 5. ROC - Windowed Encryption (FC) - direct reconstruction vs. error concealment attack.

the bitstream ordering, however, all variants are significantly less secure as compared to direct decoding.

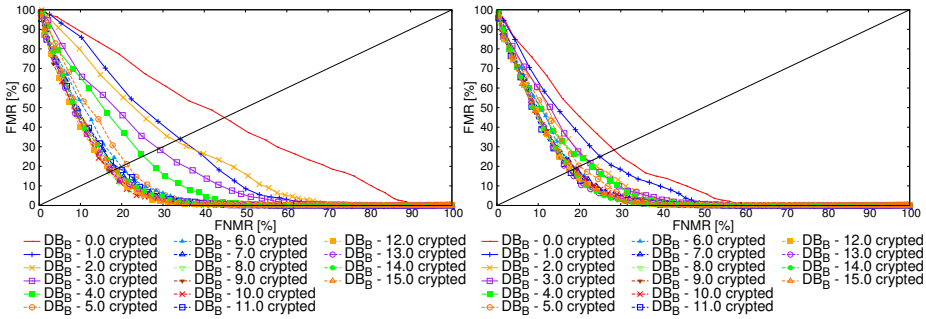

Fig. 6. ROC - Windowed Encryption (POC) - direct reconstruction vs. error concealment attack.

Table 1 only looks at the EERs (i.e. a single point at the ROC curve), but already comparing layer progressive and resolution progressive ordering in two subsequent lines. The numerical values for layer progressive codestream ordering of course confirm the graphical results as displayed in Figs. 4 – 6. However, for the resolution progressive ordering, we notice significant differences as follows. Obviously, contrasting to the layer progression mode, the data most important for AFIS is not located at the start of the codestream, but, depending on the actual AFIS and decoding variant (direct vs. error concealment) considered, either at 3% or 4% of the data. It is also interesting to note that there is not a single peak in the EER values but there is a second local maximum in the area of 11% – 13% of the data, less distinct for the error concealment decoding case. The locations of these peaks point to the position of the first data packets in layer progression ordering. Despite all the differences spotted, it gets obvious that the positions of the most sensitive areas in the JPEG2000 codestream are not depending on the actual AFIS employed.

Another clear difference is the best protection (i.e. highest EER) achieved by the different AFIS: For error concealment decoding, layer progressive ordering achieves EERs of 33% (NBIS), 20% (FC), and 28% (POC), while resolution progressive decoding results in maxima at 24% (NBIS), 18% (FC), and 24% (POC), respectively. Thus,

Table 1. EER [%] - Layer progressive (first line for each start value) vs. resolution progressive (second line for each start value) codestream ordering.

start [%]	NBIS	NBIS err.conc.	FC	FC err.conc.	POC	POC err.conc.
0.0	48.70	33.10	45.97	20.11	44.88	28.37
	19.87	9.52	13.66	12.41	26.93	21.39
1.0	42.00	30.80	33.77	16.58	34.08	24.96
	16.70	9.29	13.15	13.04	21.81	18.76
2.0	32.97	25.83	36.28	15.40	33.06	22.53
	25.34	13.83	19.11	12.42	24.83	20.81
3.0	30.46	20.33	26.64	15.16	28.95	22.32
	39.31	21.86	32.10	15.32	32.89	21.54
4.0	23.17	15.79	21.82	13.57	25.27	22.03
	37.51	23.94	32.47	17.76	35.48	23.87
5.0	18.94	12.76	15.89	13.72	21.19	20.04
	24.57	16.29	17.87	13.67	23.23	19.99
6.0	15.24	12.37	14.20	13.25	19.92	19.01
	12.23	11.39	14.35	13.25	17.97	19.21
7.0	13.08	10.41	13.81	13.68	18.63	18.99
	10.40	9.74	13.33	13.30	17.57	17.79
8.0	12.13	9.93	12.38	13.14	16.91	17.94
	15.06	11.68	17.84	14.78	22.29	18.40
9.0	11.26	9.49	12.64	13.28	17.26	18.28
	19.08	12.23	18.58	12.69	21.29	18.09
10.0	9.60	8.93	12.64	14.93	17.26	18.89
	15.63	11.43	16.91	14.56	21.41	18.52
11.0	9.59	9.26	12.65	12.89	19.25	17.59
	21.52	14.08	23.30	15.34	27.98	19.92
12.0	9.40	9.02	12.83	13.63	17.69	17.80
	24.56	14.21	22.50	13.85	26.23	20.26
13.0	9.21	8.68	14.08	13.45	17.50	17.49
	20.65	14.22	19.47	14.74	24.37	19.50
14.0	9.37	9.02	13.24	13.62	18.51	18.29
	15.41	12.33	14.83	13.24	20.15	18.89
15.0	9.22	8.40	13.76	14.86	18.41	18.63
	12.48	10.09	13.41	15.24	18.97	17.98

it gets clear that for an equal extent of protection, more data needs to be encrypted in resolution progressive ordering. The same tendency is observed for direct decoding, where layer progressive ordering achieves 49% (NBIS), 46% (FC), and 45% (POC), while resolution progressive decoding results in maxima at 39% (NBIS), 32% (FC), and 35% (POC), respectively.

Fig. 7 shows the effects of Windowed Encryption applied to resolution progressive codestream ordering using NBIS for recognition. The overall impression is similar compared to the layer progressive mode (Fig. 4) with two significant differences: First, results do degrade quicker to the unprotected case when moving away from the best

settings, and second, the best results are achieved when starting to encrypt at 3% or 4% of the data (both for direct as well as error concealment decoding). The next best settings are positioning the encryption window at 2%, 5%, and 12% of the data.

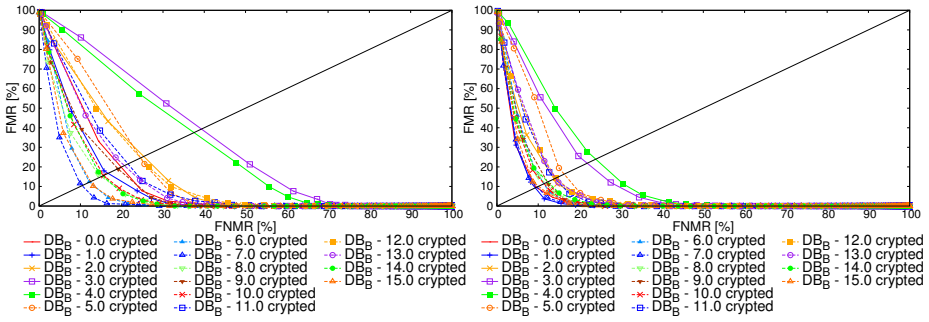

Fig. 7. ROC - Windowed Encryption (NBIS) - direct reconstruction vs. error concealment attack for resolution progressive mode.

The high robustness of FC wrt. partial codestream encryption is confirmed also for resolution progressive ordering as shown in Fig. 8. Compared to the layer progressive case (as shown in Fig. 5), even higher robustness is exhibited and for error concealment decoding, not even a single setting provides a sensible level of protection. Again, when starting to encrypt at 3% or 4% of the data the best results are achieved.

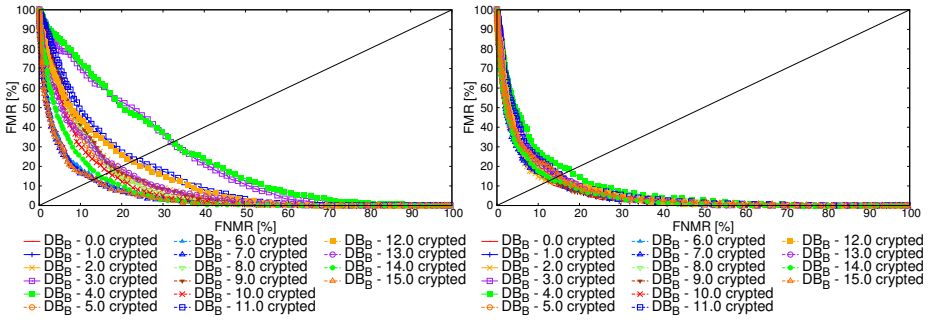

Fig. 8. ROC - Windowed Encryption (FC) - direct reconstruction vs. error concealment attack for resolution progressive mode.

Finally, Fig. 9 shows the results of POC when applied to protected codestream data in resolution progressive ordering. The same trends may be observed: Best protection is achieved for starting to encrypt at 3% or 4% of the data, protection level is worse compared to layer progressive codestream ordering (compare Fig. 6), and under error concealment decoding, the protection level is negligible.

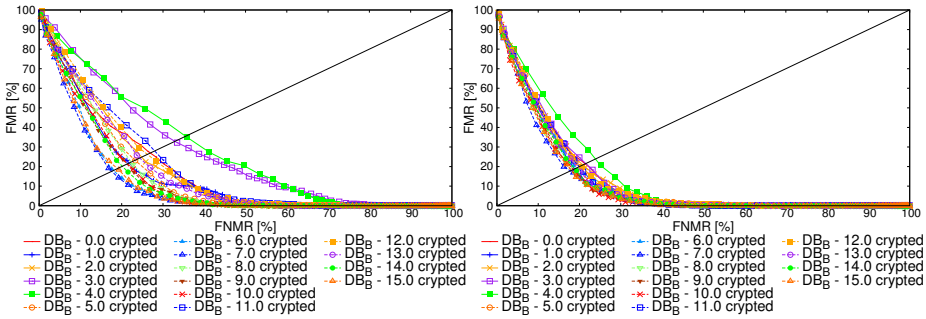

Fig. 9. ROC - Windowed Encryption (POC) - direct reconstruction vs. error concealment attack for resolution progressive mode.

5 Conclusion

We have compared various approaches to apply selective / partial encryption to fingerprint data compressed into JPEG2000 format. Evaluations are done by comparing recognition performance on encrypted data. We have found that sensitivity / robustness against partially encrypted data is highly dependent on the actual recognition scheme used and does 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, however, the observed differences are identical for all three types of AFIS. These first results will help to finally design AFIS recognition system aware encryption schemes with low encryption complexity and decent protection capability.

Acknowledgments

This work has been partially supported by the Austrian Science Fund, project no. 27776.

References

[1] Taubman, D., Marcellin, M.: JPEG2000 — Image Compression Fundamentals, Standards and Practice. Kluwer Academic Publishers (2002)

[2] Elmer, P., Lupp, A., Sprenger, S., Thaler, R., Uhl, A.: Exploring compression impact on face detection using Haar-like features. In: Proceedings of the 19th Scandinavian Conference on Image Analysis (SCIA'15). Volume 9127 of Springer LNCS. (2015) 53–64

[3] Ives, R.W., Bishop, D., Du, Y., Belcher, C.: Iris recognition: The consequences of image compression. EURASIP Journal of Advances in Signal Processing **2010** (2010) Article ID 680845, doi:10.1155/2010/680845

[4] Uhl, A., Pommer, A.: Image and Video Encryption. From Digital Rights Management to Secured Personal Communication. Volume 15 of Advances in Information Security. Springer-Verlag (2005)

[5] Lian, S.: Multimedia Content Encryption: Techniques and Applications. CRC Press (2008)

[6] Engel, D., Pschernig, E., Uhl, A.: An analysis of lightweight encryption schemes for fingerprint images. IEEE Transactions on Information Forensics and Security **3**(2) (June 2008) 173–182
[7] Engel, D., Stütz, T., Uhl, A.: A survey on JPEG2000 encryption. Multimedia Systems **15**(4) (2009) 243–270
[8] Engel, D., Stütz, T., Uhl, A.: 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 (September 2007) 87–95
[9] Stütz, T., Uhl, A.: 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 (December 2006) 985–990
[10] Draschl, M., Hämmerle-Uhl, J., Uhl, A.: 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) 1–6
[11] Norcen, R., Uhl, A.: Selective encryption of the JPEG2000 bitstream. In Lioy, A., Mazzocchi, D., eds.: Communications and Multimedia Security. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '03. Volume 2828 of Lecture Notes on Computer Science., Turin, Italy, Springer-Verlag (October 2003) 194 – 204
[12] Podesser, M., Schmidt, H.P., Uhl, A.: Selective bitplane encryption for secure transmission of image data in mobile environments. In: CD-ROM Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002), Tromso-Trondheim, Norway, IEEE Norway Section (October 2002) file cr1037.pdf.
[13] Stütz, T., Uhl, A.: 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. Lecture Notes in Computer Science, Tokyo, Japan, Springer (January 2009) 851–861
[14] Hofbauer, H., Uhl, A.: Visual quality indices and low quality images. In: IEEE 2nd European Workshop on Visual Information Processing, Paris, France (July 2010) 171–176
[15] Hofbauer, H., Uhl, A.: Identifying deficits of visual security metrics for images. Signal Processing: Image Communication **46** (2016) 60 – 75
[16] Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of Fingerprint Recognition (2nd Edition). Springer-Verlag (2009)
[17] Koichi, I., Hiroshi, N., Koji, K., Takafumi, A., Tatsuo, H.: A fingerprint matching algorithm using phase-only correlation. IEICE Transactions on Fundamentals **E87-A**(3) (March 2004) 682–691
[18] Hämmerle-Uhl, J., Pober, M., Uhl, A.: 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). Volume 8099 of Springer Lecture Notes on Computer Science., Magdeburg, Germany (September 2013) 3–17
[19] Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S.: Filterbank-based Fingerprint matching. IEEE Transactions on Image Processing **9**(5) (2000) 846–859