Efficient Fingervein Sample Image Encryption

Sanjay Shekhawat[2] • Heinz Hofbauer[1] • Bernhard Prommegger[1] • Andreas Uhl[1]

[1]Multimedia Signal Processing and Security Lab, University of Salzburg, Austria, {hofbauer, bprommeg, uhl}@cs.sbg.ac.at
[2]College of Technology and Engineering, Udaipur, Rajasthan, India, sanjay1997007@gmail.com

Abstract

Efficient sample encryption techniques are investigated for fingervein data. We propose an approach where it suffices to encrypt 0.5% of the sample JPEG2000 bitstream and thereby completely disable biometric recognition. Evaluations with 5 different recognition schemes on two different datasets reveal that results are stable accross all techniques considered as long as the start of the bitstream is encrypted.

Contents

1 Introduction

Vascular biometrics [1], in particular those modalities focussing on the vascular structure of the human hand [2], have emerged as an attractive alternative to more traditional biometric traits. One of the reasons is that corresponding biometric sample data can hardly be acquired without consent or knowledge of a human subject, and of course no "latent" variants do exist. Also, due to the bloodflow exhibited in near-infrared (NIR) video, liveness detection techniques can be used to prevent presentation attacks (PA) (aka. sensor spoofing [3]), which has been demonstrated mostly for the application case of finger veins [4, 5].

Nevertheless, it has been shown that artefacts can be constructed based on available sample data, which can be used to fool finger vein sensors [6] as well as palm vein sensors [7]. And although a wide variety of corresponding presentation attack detection (PAD) methods do exist [8, 9], these might either not be put into action or can be error-prone, in particular against unseen attack artefact types [10]. Therefore, in order to safeguard against such types of attacks, it is of highest importance to secure sample data against any misuse of this type.

The International Organisation for Standardisation (ISO) specifies biometric data to be also recorded and stored in (raw) image form (ISO/IEC FDIS 19794), i.e. sample images, 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. Furthermore, the application of low-powered mobile sensors for image acquisition, e.g. mobile phones, and the transmission of acquired data over high-latency, low-bandwidth wireless network connections raises the need for reducing the amount of transmitted data. These facts motivate detailed investigations and optimisations of image compression in biometrics in order to provide an efficient storage and rapid transmission of biometric records.

The certainly most relevant standard for compressing image data relevant in biometric systems is JPEG2000, suggested for (lossy) compression of vascular sample data in the ISO/IEC 19794-10 standard on Biometric Data Interchange Formats and in 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). There is limited work on the effects of using lossy JPEG2000 compression in vascular biometric template comparisons (e.g. [11]), while we will use JPEG2000 in lossless mode here.

As explained above, sample data are highly privacy sensitive, in particular when considering nation-wide data sets like present in the Unique Identification Authority of India's (UID) Aadhaar project. Also, 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. Therefore, cryptographic protection for sample data in such application contexts is urgently required.

Note that this application context is fundamentally different from that which triggered the development of template protection schemes. These are of course applied to template data (and aim to protect their respective security and privacy in case of data breach) and thus need to facilitate matching in the encrypted domain. This requirement is difficult to achieve and often causes a decrease in recognition accuracy or an increase in computational cost when comparing template protection schemes to recognition with unprotected data. The protection of sample data as considered in this work does not involve matching in either domain and thus allows the usage of classical cryptographic techniques like e.g. AES.

In this paper we investigate lightweight encryption schemes for JPEG2000 compressed fingervein sample data, suited also for mobile and/or low-power environments, based on selective bitstream protection. In particular, we consider the interplay between applying different types of feature extraction and template comparison schemes to the protected data and the achieved level of security / data protection when the JPEG2000 data is encrypted in different ways.

The proposed techniques offer extremely low computational effort and there is absolutely no impact on recognition accuracy once the data are decrypted for template extraction / matching. 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. Section II introduces principles of encrypting JPEG2000 data and specifically describes the approach used for fingervein data as proposed in this paper. The target fingervein recognition schemes as used in the experiments are sketched in Section III. Section IV describes a large corpus of experiments, where we specifically assess the security of the proposed encryption schemes by applying fingervein recognition to the (attacked) encrypted data. Section V presents the conclusions of this paper and an outlook to future work.

2 Efficient Encryption of Fingervein Sample Data

2.1 Selective JPEG2000 Encryption Approaches

A large variety of custom image encryption schemes have been developed over the last years for JPEG2000 [12], many of them being motivated by the potential reduction of computational effort as compared to full encryption. 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.

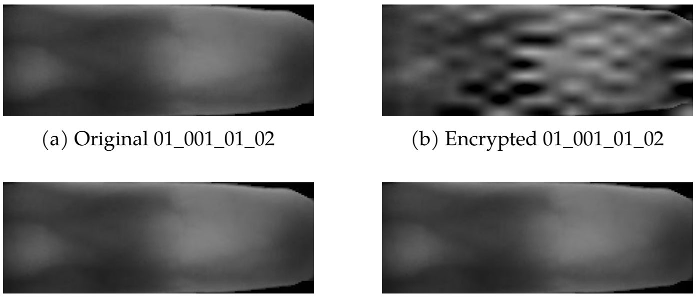
Thus, an actual biometric system will opt to employ a non format-compliant encryption variant in its deployment installation (e.g. to decrease computational cost or to disable common decoders to interpret the data). However, we will consider the corresponding format-compliant counterpart to facilitate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

In our target application context, only bitstream oriented techniques are appropriate, i.e. encryption is applied to the JPEG2000 compressed data, as fingervein data might be compressed right after acquisition but encrypted much later. 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. To enable security assessment (which involves decoding of encrypted data), only format compliant encryption schemes are admissible. Each packet within the JPEG2000 code stream eventually contains start of packet header (SOP) and end of packet header (EOP) markers. To achieve this, 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 not to emulate any header data or control bytes. Thus, we apply a format compliant JPEG2000 encryption scheme introduced in the context of JPSEC [13] to avoid such pitfalls.

In a series of papers (i.e. [14–17]), different ways how to apply encryption to different parts of a biometric sample-image JPEG2000 codestream have been defined and analysed, out of which we apply "Windowed Encryption" for the encryption of fingervein data. This approach is used to accurately spot the encryption location in the JPEG2000 bitstream with the biggest impact (in our context on recognition accuracy when fingervein recognition systems are applied to encrypted data, see related work on fingerprint [14, 15] and iris sample data encryption [16, 17], respectively. "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 (0.5% in our case), only the position of the window is changed in fixed steps within packet data.

Fig. 1 displays two original samples (left column) together with their encrypted variants (using identical "Windowed Encryption" parameters). Interestingly, at this (and other) offset value(s), the effect of encryption is very different and leaves a few samples almost unprotected (like that shown in Fig. 1(d)). It turns out that due to the extremely low amount of encrypted data, slight differences in image content cause the encryption or non-encryption of packet data to be highly important for visual quality. This effect cannot be observed in case we encrypt data right at the start of the bitstream (termed "absolute" encryption [17]).

In this manner, when using "Windowed Encryption", recognition experiments on the protected data reveal the parts of the JPEG2000 codestream that contain the most "valuable" fingervein information exploited by the different recognition schemes for matching purposes, i.e. that is most sensible to be protected by encryption. In particular it is of interest if these sensitive codestream parts differ for different feature extraction / matching schemes. For fingerprint and iris image encryption, a significant dependency on the type of used techniques has already been demonstrated [14, 16].



(a) Original 01_001_01_02

(b) Encrypted 01_001_01_02

(c) Original 02_001_01_03

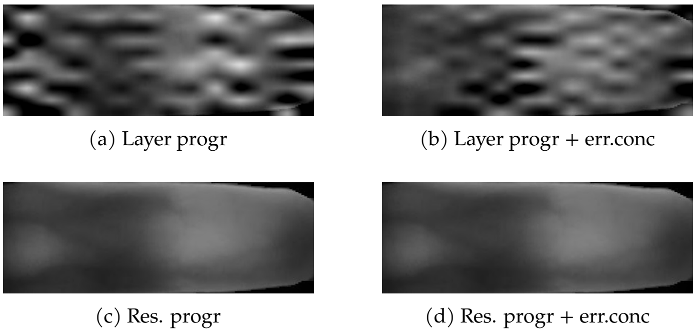
(d) Encrypted 02_001_01_03

Figure 1: Originals and encrypted samples (layer progressive order) at offset 6%.

2.2 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. 2 left column after direct reconstruction). 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 JPEG2000 bitstream being organised in layer progressive ("Layer progr") or resolution progressive ("Res. progr") manner. The JJ2000 version used in the experiments includes the patches and enhancements to JPEG2000 error concealment provided by [18], and results obtained by error concealment are denoted by "err.conc" in the result plots (see Fig. 2 right column). However, the pictorial example reveals an interesting effect: Contrasting to fingerprint [15] and iris [17] sample data, respectively, the error concealment methodology does not seem to improve the encrypted image quality significantly as compared to direct reconstruction.

In our application context, security assessment is done by applying fingervein recognition schemes to the protected data (either after direct reconstruction or after having applied error-concealment decoding) to verify if the protection is sufficiently strong to prevent the use of the encrypted fingervein data in an automated recognition context.


(a) Layer progr

(b) Layer progr + err.conc

(c) Res. progr

(d) Res. progr + err.conc

Figure 2: Encrypted samples at offset 6%.

3 Fingervein Recognition Techniques

There is a wide variety of fingervein recognition techniques known nowadays [2]. The implementation of our tool-chain is mostly based on the PLUS OpenVein Toolkit [19], an open source Matlab-based finger- and handvein recognition framework available online[1].

We have used the following components (original references of PLUS OpenVein techniques provided in [19]):

1. For *finger region detection*, *finger alignment* and *ROI extraction* an implementation that is based on [20] is used.
2. For *pre-processing* of finger vein images, to improve the visibility of the vein pattern, the OpenVein variants of *High Frequency Emphasis Filtering* (HFE), *Circular Gabor Filter* (CGF), and simple *CLAHE* (local histogram equalisation) are used.
3. For the feature extraction stage we have used again OpenVein variants of *Maximum Curvature Method* (MC), *Principal Curvature* (PC), *Wide Line Detector* (WLD), *Scale Invariant feature transform* (SIFT), and *Finger Vein Recognition with Anatomical Structure Analysis* (ASAVE).
4. *Comparison* of the binary feature images of MC, PC, and WLD is done by measuring correlation between the input images and in x- and y-direction shifted and rotated versions of the reference image. The more sophisticated techniques SIFT and ASAVE apply custom template comparison techniques as also implemented in OpenVein.

4 Experiments

4.1 Experimental Settings

All the experiments are performed on two publicly available fingervein sample image databases, i.e. Fingervein Universiti Sains Malaysia (FV-USM) Database [21] and The University of Twente Finger Vascular Pattern (UTFVP) Database [22]. The first database consists of data from 123 volunteers, four fingers each, i.e. left index, left middle, right index and right middle. In total there are 492 classes of fingers and each finger is being captured six times so there are 2952 images in one session (overall 5904 images in two sessions), image resolution is 640 x 480 pixels. The second dataset consists of data from 60 volunteers, six fingers i.e. ring, middle and index finger from both hands acquired in two sessions, image resolution is 672 x 380 pixels. So in total, we have 1440 Images to perform our experiments.

Table 1: EER [%]-unprotected.

Dataset	*MC*	*PC*	*WLD*	*SIFT*	*ASAVE*
FV-USM	0.99%	1.43%	1.61%	2.84%	5.14%
UTFVP	1.48%	1.57%	1.20%	1.90%	3.10%

The sample images are compressed into lossless JPEG2000 in either layer or resolution progression mode and protected by encrypting CCPs, i.e. codeblock contribution to packet of code blocks, while maintaining signal markers and thus format compliance. Due to the embedded-ness of the JPEG2000 bitstream, the data is ordered such that the base information comes at the beginning, followed by refinement blocks which bring more and more detail into the image. The encryption applied is based on AES encryption of a sliding window of 0.5% of the bitstream size. The offset gives the detail level of the encrypted material, the farther down the bitstream, the less visual influence the data should have. The offset values used are from the beginning 0% to 15% in 1% steps.

To calculate recognition performance parameters (EER, FMR100, ZeroFMR and FMR1000) we used the test protocol for matching encrypted probe sample to plaintext gallery data, adopted from fingerprint verification contests (FVC), as implemented in PLUS OpenVein.

4.2 Results

Table 1 shows the EER for the five recognition schemes considered when applied to plain (unprotected, i.e. unencrypted) data, while Fig. 3 displays the entire ROC-range for FV-USM data. With respect to EER, ASAVE is worst and SIFT second worst. While MC is best for FV-USM, WLD is best for UTFVP data. With respect to ROC behaviour on FV-USM data, MC performs best overall, except for very low FNMR where SIFT and WLD are superior. ASAVE exhibits the worst behaviour, except for high FNMR, where it is superior to all other recognition schemes.

First results are obtained on FV-USM data when applying MC feature extraction and comparison on encrypted sample data, comparing JPEG2000 data organised in layer progressive and resolution progressive order and comparing direct reconstruction to applying error concealment reconstruction. Fig. 4 displays EER against encryption offset and shows partially surprising results. The most important result: Even when encrypting only 0.5% of the JPEG2000 bitstream, almost perfect security (i.e. ERR $\approx$ 50%) is achieved no matter which bitstream organisation or reconstruction variant is chosen in the offset range [0,4]. This is a strong result compared to required encryption of $\approx$ 25% of normalised iris texture [16] or $\approx$ 3% of fingerprint images [15], respectively. Second: There is no relevant difference if we apply direct reconstruction or error-concealment aided reconstruction to the encrypted samples.

[1] http://www.wavelab.at/sources/OpenVein-Toolkit/

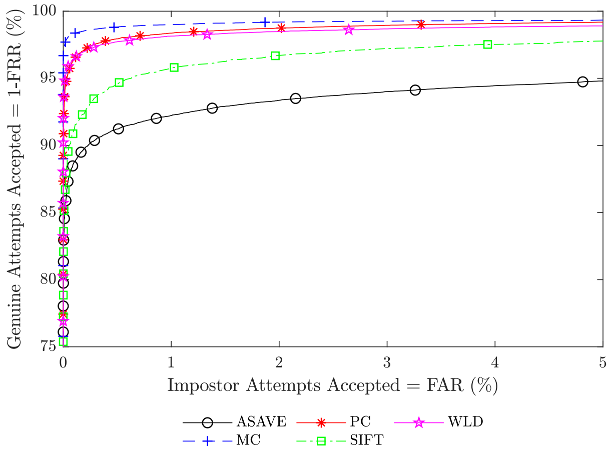


Figure 3: ROC on unencrypted data.

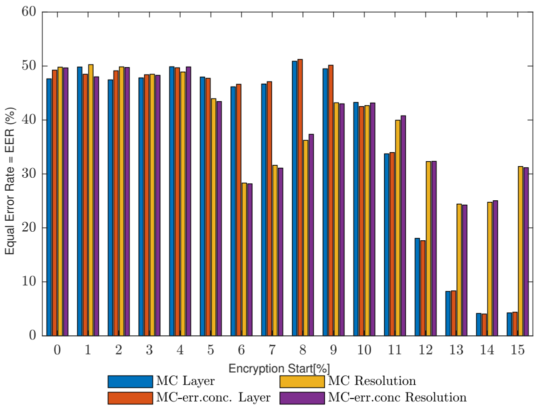
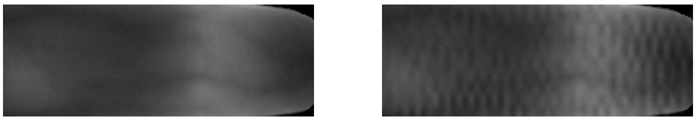


Figure 4: FV-USM: MC - Encryption Start % vs. Equal Error rate (EER)

This result confirms the observations made on the visual example in Fig. 2, where also almost no security relevant difference is visible comparing those two options. As already stated, this is in stark contrast to fingerprint and iris sample data protected in similar manner. However, we notice significant differences when comparing the JPEG2000 data organisation.

For layer progressive organisation, the security is high for offsets in the range [0,9] leading to EER of ≈ 50%, then subsequently EER decreases contineously down to values almost corresponding to the unprotected case. However, for resolution progressive organisation, we observe a wave-like pattern going down to 30% EER for offset 6, going up again to 45% EER at offset 9, then exhibiting another local EER minimum at offset 13 but with again rising EER for offset > 13. This observation is perfectly in line with earlier observations made on fingerprint [14, 15] as well as iris sample data, [16] respectively. Fig. 2 shows typical example images for encrypted samples at offset 6, comparing the two JPEG2000 bitstream organisation modes. The visual impression (sample exhibits clear vascular structures in the resolution progressive case) illustrates the higher security in the layer progressive organisation at this offset value.



(a) Layer progr + err.conc

(b) Res. progr + err.conc

Figure 5: Encrypted samples at offset 15%.

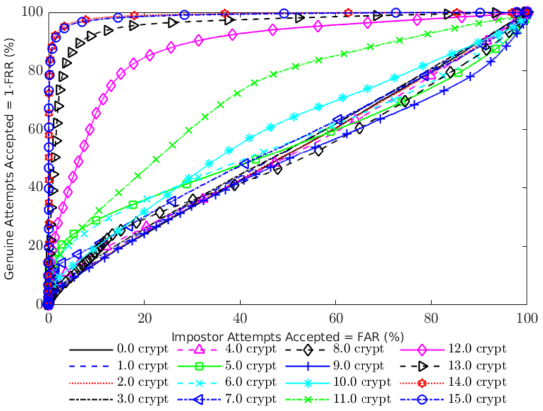


Figure 6: FV-USM: ROC-curves for MC features using different encryption offsets: Layer progressive JPEG2000 organisation and error concealment reconstruction.

In Fig. 5, we consider offset 15, where the relation between layer and progressive JPEG2000 organisation should be vice versa according to recognition results in Fig. 4 (i.e. layer progressiveness is less secure) - again, the visual impression illustrates and confirms the numerical recognition scores.

As MC features deliver the best overall ROC behaviour according to Fig. 3, we also show the entire ROC curves for different encryption offsets in Figs. 6 and 7 for this best-performing feature extraction methodology, in order not to limit the investigation to a single point on the ROC-curve (i.e. the EER).

The ROC curves confirm the behaviour observed so far when comparing layer and resolution progressive JPEG2000 bitstream organisation: Layer progressive mode behaves rather predictibly with steadily decreasing security for offsets larger than 9, while in resolution progressive representation the ROC-curves are not as symmetric and are far less clearly ranked. Therefore, we recommend to refrain form using JPEG2000 with resolution progressive for the sample encryption application.

When considering the other feature extraction schemes on FV-USM data, the overall tendency is highly similar (PC, SIFT, and ASAVE – not shown). Fig. 8 visualises the recognition results of WLD as the second example. Apart from smaller differences (e.g. at offset 5, we notice a small local minimum in the layer progressive ordering result and good protection is found in the offset range [0,4] only) the overall observations are identical. In order to have a closer look into observed differences between JPEG2000 bitstream ordering schemes, Fig. 9 compares the binary WLD features at offset 6, where the difference in EER between the two JPEG2000 bitstream organisation modes is rather large.

The connectivity of the vascular structures is clearly better for the resolution progressive (right) case, explaining the

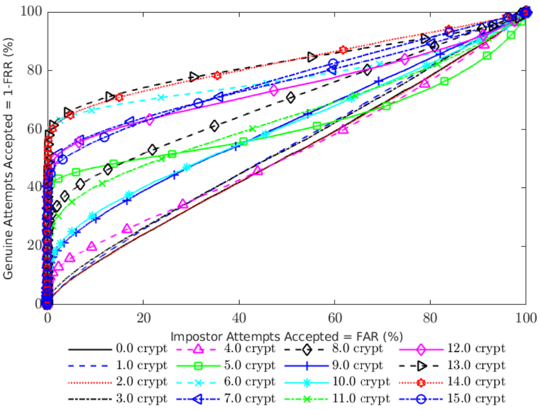


Figure 7: FV-USM: ROC-curves for MC features using different encryption offsets: Resolution progressive JPEG2000 organisation and error concealment reconstruction.

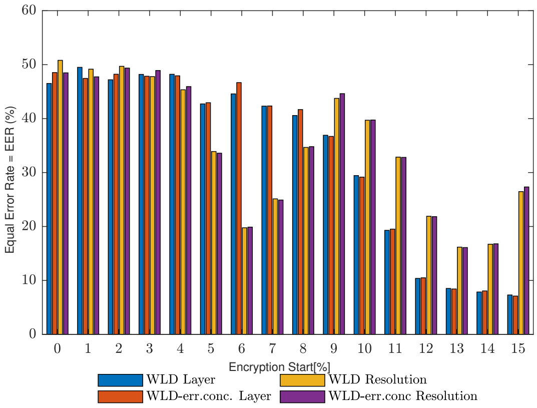
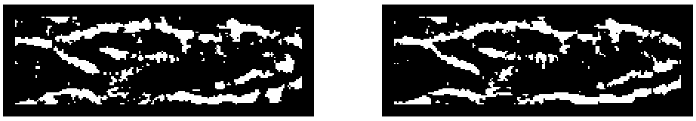


Figure 8: FV-USM: WLD - Encryption Start % vs. Equal Error rate (EER).

much better protection of the layer progressive mode. Examples can be seen in the right bottom corner and the top left corner where a bifurcation is present in Fig. 9(b), while it is disconnected in Fig. 9(a).

Fig. 10 displays an exemplary result for the UTFVP data. We observe many properties shared among the results of the two datasets (i.e. almost no difference between direct reconstruction and error concealment enabled reconstruction, clear differences between layer progressive and resolution progressive JPEG2000 bitstream organisation and corresponding security advantages for the former when the offset value is low, and a waveform pattern of EER values for increasing offset in case of resolution progressiveness). However, there are two distinct differences: First, good protection is achieved only for offset 0% and 1% in the case of UTFVP, and we also observe a waveform in the layer progressive results, e.g. a local EER minimum at offset 2%.



(a) Layer progr + err.conc

(b) Res. progr + err.conc

Figure 9: Extracted WLD binary features at offset 6%.

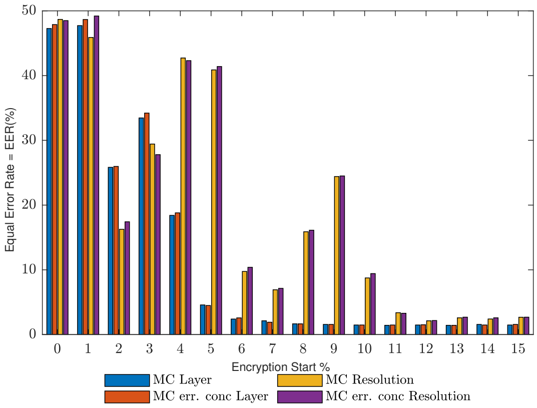


Figure 10: UTFVP: WLD - Encryption Start % vs. Equal Error rate (EER).

When considering the results of the other feature extraction schemes on UTFVP (i.e. MC, PC, SIFT, ASAVE - not shown), we observe entirely similar behaviour. Thus when applied on the same dataset, result characteristics are extremely invariant for different feature extraction schemes.

5 Conclusion

We have evaluated various approaches to apply selective/partial encryption to fingervein sample data (losslessly compressed into JPEG2000). The recognition performance on encrypted data using different types of recognition schemes indicates that we may achieve high security when encrypting only 0.5% of the JPEG2000 bitstream data. In accordance to earlier results on fingerprint and iris sample data it turns out that resolution progressive ordering of the JPEG2000 bitstream should be avoided due to unpredictible behaviour. Contrasting to these earlier evaluations, we have found that the application of error concealment techniques in decoding encrypted sample data does not lead to any improvements over directly using encrypted data. Results clearly indicate, that the best option is to apply encryption right at the start of a JPEG2000 bitstream in layer progressive ordering, as progression strength may decrease quickly for increasing the encryption offset relative to the bitstream start. Different datasets exhibit distinct properties with that respect, which is caused by differences in file size, share of background data, and image contrast, respectively.

6 Acknowledgments

This project was partly funded the FFG KIRAS project AUTFingerATM under grant No. 864785 and the FWF project "Advanced Methods and Applications for Fingervein Recognition" under grant No. P 32201-NBL.

References

[1] A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, *Handbook of Vascular Biometrics*, ser. Advances in Computer Vision and Pattern Recognition. 2019, ISBN: 978-3-030-27731-4. DOI: 10.1007/978-3-030-27731-4 (cit. on p. 2).

[2] A. Uhl, "State of the art in vascular biometrics," in *Handbook of Vascular Biometrics*, 2019, ch. 1, ISBN: 978-3-030-27731-4. DOI: 10.1007/978-3-030-27731-4 (cit. on pp. 2, 4).

[3] S. Marcel, M. Nixon, and S. L. (Eds.), *Handbook of Biometric Anti-Spoofing*. 2014 (cit. on p. 2).

[4] R. Raghavendra, M. Avinash, S. Marcel, and C. Busch, "Finger vein liveness detection using motion magnification," in *Proceedings of the Seventh IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS'15)*, 2015 (cit. on p. 2).

[5] J. Bok, K. H. Suh, and E. C. Lee, "Detecting fake finger-vein data using remote photoplethysmography," *Electronics*, vol. 8, no. 9, 2019 (cit. on p. 2).

[6] P. Tome, M. Vanoni, and S. Marcel, "On the vulnerability of finger vein recognition to spoofing attacks," in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'14)*, 2014 (cit. on p. 2).

[7] P. Tome and S. Marcel, "On the vulnerability of palm vein recognition to spoofing attacks," in *The 8th IAPR International Conference on Biometrics (ICB)*, 2015 (cit. on p. 2).

[8] R. Raghavendra and C. Busch, "Presentation attack detection algorithms for finger vein biometrics: A comprehensive study," in *11th International Conference on Signal-Image Technology Internet-Based Systems (SITIS'15)*, 2015 (cit. on p. 2).

[9] D. T. Nguyen, Y. H. Park, K. Y. Shin, S. Y. Kwon, H. C. Lee, and K. R. Park, "Fake finger-vein image detection based on fourier and wavelet transforms," *Digital Signal Processing*, vol. 23, no. 5, 2013 (cit. on p. 2).

[10] D. Söllinger, P. Trung, and A. Uhl, "Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing," *IET Biometrics*, vol. 7, no. 4, 2018 (cit. on p. 2).

[11] V. Ablinger, C. Zenz, J. Hämmerle-Uhl, and A. Uhl, "Compression standards in fingervein recognition," in *Proceedings of the 9th IAPR/IEEE International Conference on Biometrics (ICB'16)*, 2016 (cit. on p. 2).

[12] D. Engel, T. Stütz, and A. Uhl, "A survey on JPEG2000 encryption," *Multimedia Systems*, vol. 15, no. 4, 2009. DOI: http://dx.doi.org/10.1007/s00530-008-0150-0 (cit. on p. 2).

[13] F. Dufaux, S. Wee, J. Apostolopoulos, and T. Ebrahimi, "JPSEC for secure imaging in JPEG2000," in *Applications of Digital Image Processing XXVII*, vol. 5558, 2004 (cit. on p. 3).

[14] 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, vol. 9977, 2016 (cit. on pp. 3, 5).

[15] ——, "Sensor dependency in efficient fingerprint image protection using selective jpeg2000 encryption," in *Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF'17)*, 2017 (cit. on pp. 3–5).

[16] M. Rieger, J. Hämmerle-Uhl, and A. Uhl, "Efficient iris sample data protection using selective jpeg2000 encryption of normalised texture," in *Proceedings of the 6th International Workshop on Biometrics and Forensics (IWBF'18)*, 2018 (cit. on pp. 3–5).

[17] ——, "Selective JPEG2000 Encryption of Iris Data: Protecting Sample Data vs. Normalised Texture," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'19)*, 2019. DOI: 10.1109/ICASSP.2019.8683196 (cit. on p. 3).

[18] 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, 2009 (cit. on p. 3).

[19] C. Kauba and A. Uhl, "An available open-source vein recognition framework," in *Handbook of Vascular Biometrics*, 2019, ch. 4, ISBN: 978-3-030-27731-4. DOI: 10.1007/978-3-030-27731-4_4 (cit. on p. 4).

[20] Y. Lu, S. Xie, S. Yoon, J. Yang, and D. Park, "Robust finger vein roi localization based on flexible segmentation.," *Sensors*, vol. 13, no. 11, 2013 (cit. on p. 4).

[21] M. S. M. Asaari and B. A. R. S. A. Suandi, "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," *Expert Systems with Applications*, vol. 41, no. 7, 2014 (cit. on p. 4).

[22] B. Ton and R. Veldhuis, "A high quality finger vascular pattern dataset collected using a custom designed capturing device," in *International Conference on Biometrics, ICB 2013*, 2013 (cit. on p. 4).