Efficient Iris Sample Data Protection using Selective JPEG2000 Encryption of Normalised Texture

Martin Rieger, Jutta Hämmerle-Uhl, and Andreas Uhl
Department of Computer 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 iris data by conducting iris recognition on the selectively encrypted data. This paper specifically investigates the effect of applying the approach to normalised texture data instead of original sample data in order to further reduce the amount of data to be processed (i.e. compressed and encrypted). Result generalisability is facilitated by the employment of four different iris feature extraction schemes and the systematic consideration of three encryption variants. Depending on the applied iris recognition scheme, protection equivalent to full encryption can be achieved when encrypting 1/60 – 1/12 of the data amount of a full iris sample encoded in a JPEG2000 file.**

I. Introduction

The International Organisation for Standardisation (ISO) specifies biometric data to be also 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]. 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 iris sample images in the ISO/IEC 19794 standard suite 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 a vast literature on the effects of lossy JPEG2000 compression in iris recognition, see e.g. [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], while we will use JPEG2000 in lossless mode here.

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 (especially when considering nation-wide data sets like present in the Unique Identification Authority of India's (UID) Aadhaar project). Therefore, these data, often stored as JPEG2000 data as described before, require cryptographic protection for (long-term) storage and transmission.

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.

In this paper we investigate lightweight encryption schemes for JPEG2000 compressed iris sample data based on selective bitstream protection applied to normalised iris texture instead of actual original sample data. In particular, we consider the interplay between applying different types of feature extraction and matching 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 approaches tailored for iris data as proposed in this paper. The target iris 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 iris recognition to the (attacked) encrypted data. Section V presents the conclusions of this paper and an outlook to future work.

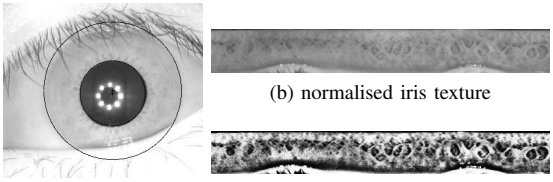
II. Efficient Encryption of Iris Sample Data

A. Iris Sample Data Types Subject to Compression and Encryption

The iris recognition processing chain typically consist of several stages (some of these depicted in Fig. 1), the first of which is iris localisation also termed "iris segmentation"

where the pupillar and limbic boundaries of iris texture are determined.

To perform the experiments we use USITv2[1] (University of Salzburg Iris Toolkit v2.0.x [1], [12]), a publicly available iris recognition software package which comprises different algorithms for iris pre-processing, feature extraction, and comparison. *Segmentation* is performed using a method based on contrast-adjusted Hough transform (`caht`) proposed by [1] (see Fig. 1.a for example boundaries).



(a) iris sample with boundaries

(b) normalised iris texture

(c) CLAHE enhanced texture

Figure 1: Types of iris (sample) data.

In the second step the localised iris is normalised. The reasons for this are differences in image acquisition, like the varying size of irises caused by changes of the camera-to-eye distance. The main idea is to transform the area between the two boundary-curves into a rectangle texture with fixed size for compensating such deformations. This is done by a coordinate-transform from Cartesian-coordinates to polar-coordinates also denoted as "rubber sheet-transform" (Fig. 1.b). The final pre-processing step enhances contrast and compensates for illumination variations by applying e.g. CLAHE (Fig. 1.c) to the normalised texture.

The experiments are done on the CASIA V3 Interval dataset. The original samples have a resolution of 320 $\times$ 280 pixels with 8bpp grayscale (NIR data), while the normalised iris texture derived using USITv2 has a resolution of 512 $\times$ 64 pixels with identical bitdepth, thus the pixel count is reduced by a factor of 2.73 when considering normalised iris texture. Note that these two types of iris data correspond to standardised iris images (IREX records) as defined by the NIST Iris Exchange (IREX I `http://iris.nist.gov/irex/`) program. In particular, original sample data corresponds to IREX record kind 1 or 3, while the normalised texture corresponds to record kind 16 (which has been later abandoned by NIST).

The observation of reduced data rate for normalised iris textures motivates the approach investigated in this paper. Instead of compressing and encrypting the original sample data for protected transmission or storage, we compute the normalised texture from the sample data, apply CLAHE eventually, and compress and encrypt it subsequently. This has three obvious advantages. First, the amount of data to be compressed and encrypted is reduced. Second, the protected data can be immediately subjected to feature extraction after decryption and decoding as the segmentation and normalisation process has already been conducted (recognition can be sped up significantly). Third, in case of lossy compression, there is no impact of compression artifacts onto segmentation results (which can be significant [13]). On the other hand, the disadvantage be to taken into account is that by storing these data, later improvements in the segmentation and normalisation procedures cannot be exploited. And, of course, this strategy puts additional computational load to the infrastructure entity which is already responsible for compression and encryption.

Table I compares the filesize of the different data types after lossless JPEG2000 compression, i.e. comparing the amount of data subjected to encryption in case of full protection.

Table I: Filesize in byte after JPEG2000 lossless compression (CASIA V3 Interval).

Data	$\varnothing$	σ	range
original sample	42501.80	3874.06	[27402,51998]
normalised texture	15471.84	1119.22	[10408,19803]
CLAHE limit=1	18522.91	1074.32	[12973,22373]
CLAHE limit=3	21933.45	1072.76	[16302,26679]

We observe that the relation between original sample and normalised texture is preserved from the case of looking at image resolution only, also the file size variability is significantly lower for normalised textures (which is beneficial for worst case planning). When applying contrast enhancement (CLAHE) with increasing strength, average filesize increases (but is still lower almost by a factor of two when compared to the original sample). Thus, the best option would be to compress and encrypt the normalised texture, while applying CLAHE to the decrypted and decoded normalised texture right before feature extraction.

B. Selective JPEG2000 Encryption Approaches

For JPEG2000, [14] 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 iris 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 [15] to avoid such pitfalls.

In a series of papers (i.e. [16], [17], [18]) we have defined and analysed different ways how to apply encryption to different parts of a fingerprint-image JPEG2000 codestream. From these techniques, we adopt "Absolute Encryption" (encryption is applied to one single chunk of data right at the start of the codestream [16]) as well as "Windowed Encryption" for encryption of iris data. The latter approach is used to accurately spot the encryption location in the JPEG2000 bitstream with the biggest impact (in our context on matching rates when

[1] http://www.wavelab.at/sources/USIT/

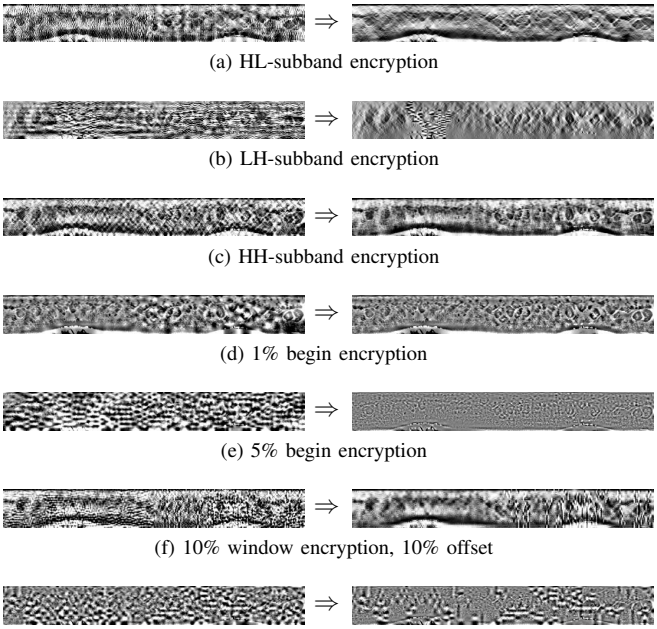
iris recognition systems are applied to encrypted data [17], [18]). "Windowed Encryption" is operated by moving a fixed window (of the size of some percent of the filesize in our experiments) across the packet data. While the percentage of encrypted data does not change during the experiments, only the 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" iris information exploited by the different recognition schemes for matching purposes, i.e. that is most sensitive if protected by encryption. In particular it is of interest if these sensitive codestream parts differ for different feature extraction / matching schemes. For fingerprint image encryption, a significant AFIS type dependency has already been demonstrated [17].

In addition to these two established encryption schemes, we consider "Subband Encryption" in this work. This means that we encrypt all packet data corresponding to distinct wavelet decomposition subbands with the aim of eventually exposing certain characteristics of different feature extraction and matching techniques when applying them to the protected data (as the different subbands correspond to the application of wavelet highpass and lowpass filters in different combinations and orders, the importance of certain directions or scales for a feature extraction scheme might be exhibited). Note that this scheme is not meant to be applied in practice, but is aimed to better understand the interplay of encrypting specific data parts and the applied iris recognition scheme wrt. observed recognition results.

C. 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). 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 [19], and results obtained by error concealment are denoted by "rep" (for replacement) in the result plots.

As visible in Fig. 2 (right column), especially after error concealment attacks, certain parts of the iris texture can still be present (see Fig. 1.c for the original), which could be improved further with iris texture 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. 2.e ("5% begin encryption") does not seem to exhibit any more iris texture related structures which could be exploited by an attacker.



(a) HL-subband encryption

(b) LH-subband encryption

(c) HH-subband encryption

(d) 1% begin encryption

(e) 5% begin encryption

(f) 10% window encryption, 10% offset

(g) 5% window encryption, 5% offset

Figure 2: Comparison of encrypted textures (direct decoding) with error-concealment decoding.

In our application context, security assessment is done by applying iris 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 iris data in an automated recognition context.

III. Iris Recognition

Different types of iris recognition schemes might react differently to image degradations caused by encrypted bitstream parts. Therefore, we will consider fundamentally different types of iris feature extraction and matching schemes, different wrt. the dominant orientation and the extraction domain considered, respectively.

We employ custom implementations of four feature extraction and matching techniques (for a detailed description of our implementation of preprocessing, feature extraction, and matching see [1], [12]). All implementations are available in USITv2[2] (University of Salzburg Iris Toolkit v2.0.x).

The first scheme has been published by Ma et al. [20] ("**Ma**") using a 1D dyadic wavelet transform maxima representation for small averaged stripes of the iris texture while the second technique is a re-implementation of the popular 1D log-Gabor MATLAB-code of Libor Masek [21] ("**Masek**"). The third scheme has been developed by Ko et al. [22] ("**Ko**") and extracts spatial domain features, while the forth approach has been designed by Monro et al. [23] ("**Monro**") and relies on DCT-derived features computed from rotated texture patches.

The first two schemes share the generation of a 1-D signal onto which the 1-D transforms are applied. The normalised iris texture is divided into ten vertical texture stripes of same

[2] http://www.wavelab.at/sources/USIT/

height (typically 5 rows wide) eventually ignoring several rows close to the limbic boundary. Subsequently, the average gray-scale value of each 1×5 stripe is estimated and normalised in an adequate range in order to obtain a 1-D signal.

1) **Ma**: A quadratic spline wavelet transform is performed on the ten signals, and two fixed subbands are selected resulting in a total number of 20 subbands. Subsequently, minima and maxima of the filter responses are detected and descending and ascending sequences are encoded with 0 and 1, respectively.
2) **Masek**: A a convolution with a 1-D complex Log-Gabor filter is performed. Subsequently, the phase angle of the resulting complex values for each signal is discretised into 2 bits.
3) **Ko**: The algorithm discards parts of the iris texture, from the right side [45^o to 315^o] and the left side [135^o to 225^o], since the top and bottom of the iris are often hidden by eyelashes or eyelids. Subsequently, the resulting texture is divided into basic cell regions (these cell regions are typically of size 8×3 pixels), for which an average gray scale value is calculated. Then basic cell regions are grouped horizontally and vertically (five basic cell regions in each group). Finally, cumulative sums over each group are calculated to generate an iris-code. If cumulative sums are on an upward slope or on a downward slope these are encoded with 1s and 2s, respectively, otherwise 0s are assigned to the code. In order to obtain a binary feature vector (to enable Hamming Distance computation for comparison) we rearrange the resulting iris-code such that the first half contains all upward slopes and the second half contains all downward slopes.
4) **Monro**: Divides the normalised iris texture into overlapping angular patches of a particular size and a particular orientation, with an overlapping part of half the size of a patch. Experimental optimisation led to a patchsize of 8×12 with an orientation of $45°$. Subsequently, a weighted averaging under a Hanning window is formed in horizontal direction with a subsequent windowing in vertical direction within each patch leading to a patch size of 8×1 pixels. Subsequently, a DCT transform is applied to each patch. The zero-crossings of the differences between particular coefficients of adjacent patches form the feature vector, where it turned out that the first three out of these 8-bit-codelets perform best.

IV. Experiments

A. Experimental Settings

All experiments are based on images taken from the CASIA V3 Interval iris image dataset consisting of 2647 NIR images from 395 different classes. Images are compressed into lossless JPEG2000 format using JJ2000 in resolution progressive ordering, using a single quality layer. The JPEG2000 bitstreams are encrypted by either "Absolute Encryption" varying the amount of encrypted data, by the different variants of "Windowed Encryption" with different positions where to start the encryption, and by "Subband Encryption". Subsequently, data are either directly decoded or decoded with enabled error concealment with the JJ2000 variant mentioned [19].

Error analysis is conducted in two different variants, always matching original gallery images to encrypted probe images. First, we only look at the genuine score distributions comparing the distribution of original to that of selectively encrypted data, respectively (we use all genuine as well as impostor scores that can be computed from the dataset, respectively). Properly protected data should look like a impostor distribution and the better the protection is, the closer the genuine score distribution moves to an imposter score distribution. Second, we conduct an ROC analysis and present EER and obviously, higher EER corresponds to better data protection.

B. Experimental Results

For discussing genuine score distributions with encrypted probe images, we only consider the case of conducted error concealment assuming an informed attacker.

Fig. 3 compares the results of the four recognition schemes in case of Subband encryption being applied to the first level HH, LH, and HL subbands, respectively. We notice that for Ko recognition, encryption of the LH subband has the strongest impact, while for the other three recognition schemes this is the case for HL encryption.

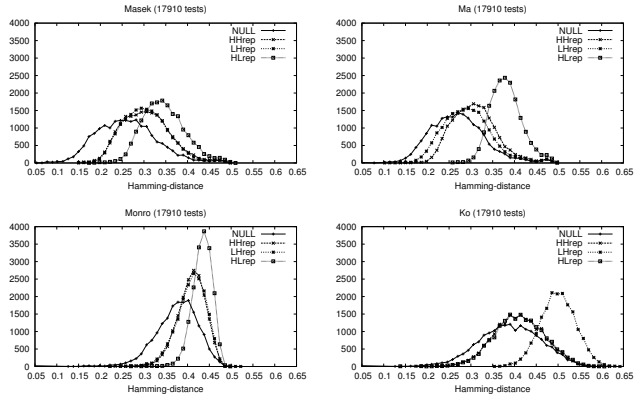


Figure 3: Subband encryption: Genuine score distributions with error-concealment.

HH and LH encryption leads to identical results except for Ma recognition, where HH encryption has slightly stronger impact. The observed results fit well to the expectations as the HL subband is generated by applying the high-pass filter in horizontal direction (i.e. horizontal detail is covered in this subband). As at least Masek and Ma predominantly apply filtering and coding in horizontal direction, HL encryption is expected to have the strongest impact.

In Fig. 4 we display the effect of increasing the amount of encrypted JPEG2000 packet data when encrypting right from the start of the bitstream. Results turn out to be quite similar for three out of four recognition schemes, respectively. For Masek, Ma, and Monro, encrypting 1% has a weak effect only, while encrypting 2% and 3% lead to exactly identical behaviour. The strongest impact is observed with 4% and 5% of packet data being encrypted, with almost non-existing overlap with

the original genuine score distribution (i.e. good protection is achieved, except for Monro where we notice a slight overlap).

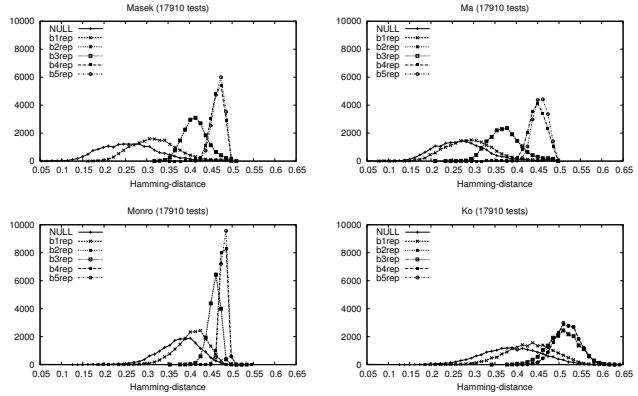


Figure 4: Absolute encryption: Genuine score distributions with error-concealment.

For Ko recognition, we have almost identical distributions for encrypting 2% - 5% of packet data, respectively, all of them exhibiting significant overlap with the original genuine score distribution. Thus, for Ko, a larger share of the JPEG2000 codestream needs to be encrypted to provide the desired protection. Note also that contrasting to the other three schemes, the Ko genuine score distributions under encryption are centered around Hamming distance 0.55 while the for the other recognition schemes these are centered around 0.45. This will lead to high error rates when applying Ko recognition to encrypted data due to confusing genuine with impostor matches while the other schemes will still be able to at least partially discriminate (encrypted) genuine scores from imposter scores.

Fig. 5 illustrates the effect of moving a window encrypting 5% of packet data across the JPEG2000 bitstream in 5% steps, starting right at the begin of the bitstream up to starting the encryption at 25% of all packet data.

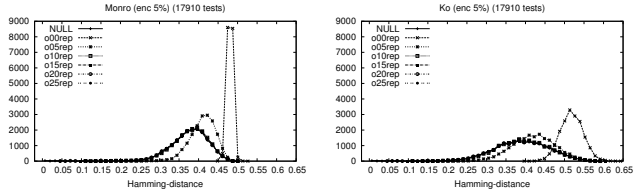


Figure 5: Windowed encryption (5%): Genuine score distributions with error-concealment.

Only starting right at the begin of the bitstream provides sensible protection. While the overlap with the original genuine distribution is small for Masek, Ma (both not shown), and Monro recognition, respectively, the overlap is considerable for Ko recognition underpinning the requirement for encrypting more data in this case already stated before.

Finally, Fig. 6 displays results for a 1% encryption window moving in 1% steps across the bitstream. Contrasting to the 5% case, we observe different behaviour (i.e. different sensitivity against certain parts of the bitstream being protected) for the four recognition schemes. Interestingly, best protection is never seen when starting directly at the bitstream begin. In two out of four schemes, it is best to start at 1% of the bitstream (Masek & Ko) while for the rest it is best to start at 2%.

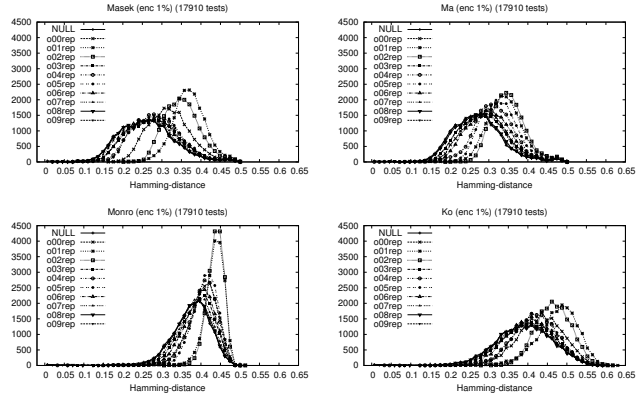


Figure 6: Windowed encryption (1%): Genuine score distributions with error-concealment.

For Ma and Monro, encrypting right from the start does hardly change the original genuine score distribution, while for Masek and Ko it is at least the third-best option. Note that overall, the encryption of 1% of the packet data does not lead to sufficiently displaced genuine score distributions to provide decent protection. In real applications, we need to encrypt more data (i.e. at least 5% for Masek, Ma and Monro and more for Ko). As the latter results indicate that starting encryption at the begin of the bitstream is either the third best option for a 1% window or is at least not worse than starting at later positions, we may start encrypting right from the bistream start for larger encryption window sizes.

In the following, we provide EER for the different encryption variants as one indicator for ROC behaviour. As Subband encryption is meant for illustrative purposes mainly, we restrict results to Absolute and Windowed encryption, respectively. In these results, we compare a direct reconstruction to applying error-concealment in decoding the encrypted data.

Fig. 7 shows that there is indeed a significant difference in the security assessment between considering direct reconstruction and error-concealment (an informed attacker in the latter case). Recall that the right-sided plot(s) (i.e. with error concealment) correspond(s) to the genuine score distributions discussed before and these are discussed first. The differences in recognition performance on original data (Ma and Masek are clearly superior to Monro and Ko, respectively, compare the values at 0% encryption on the x-axis) is clearly reflected also in the EER results on selectively protected data. Results indicate that decent protection under Ma recognition is achieved after having encrypted 25% of the packet data only. Also with Masek recognition, encrypting 10% of the packet data does not yet lead to the desired protection level (EER is still down to 25%). On the other hand, under Monro and Ko recognition EER is up to 42% - 44% after having encrypted 4% of the packet data only. Note that especially the poor EER results of Ko do correspond well to the expectation after having analysed the encrypted genuine score distributions (compare Fig. 4).

When comparing these results to those achieved after direct

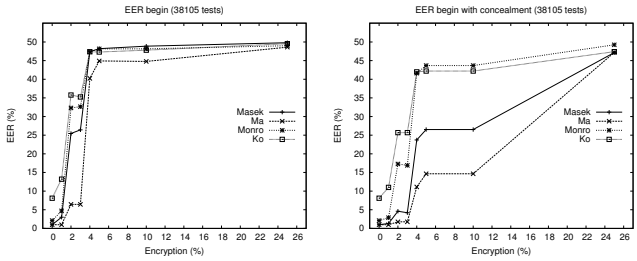


Figure 7: Absolute encryption: EER using direct reconstruction and with error-concealment.

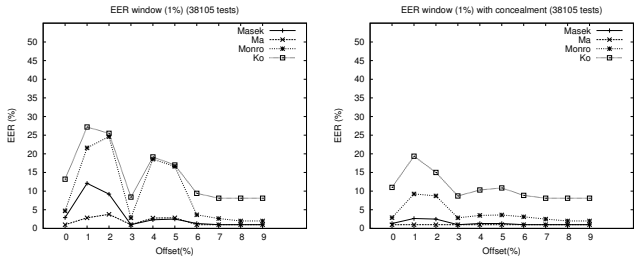


Figure 9: Windowed encryption (1%): EER using direct reconstruction and with error-concealment.

reconstruction, we see a very different picture. Results suggest that for all recognition types an encryption of 5% of the packet data is sufficient to result in more than 45% EER (more than 40% for Ma), thus indicating sufficiently secured data. These results drastically underline the importance of considering informed attackers to prevent an over-optimistic security assessment.

Figs. 8 and 9 consider the case of windowed encryption with encrypting 5% and 1% of the packet data respectively. Again we notice significant differences between direct reconstruction and applying error-concealment, at least for the lower offset values (i.e. closer to the start of the bitstream). While for the 5% encryption window (Fig. 8) it is clear that starting at the begin of the bitstream is the best option no matter which assessment is considered, the EER is over-estimated for direct reconstruction for offset values 0%, 5% , and 10%, especially for Ma and Masek recognition at 0% offset.

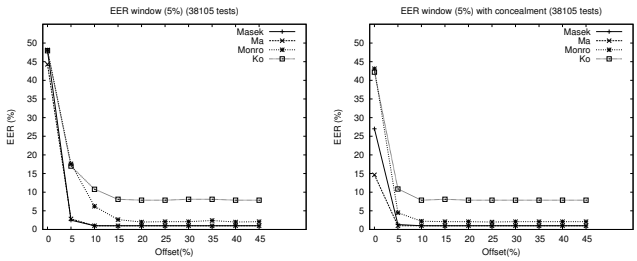


Figure 8: Windowed encryption (5%): EER using direct reconstruction and with error-concealment.

For the 1% encryption window (Fig. 9) we again observe an over-estimation of EER in the direct reconstruction results for the lower offset values, in particular for Masek and Monro. On the other hand, the varying sensitivity of different recognition schemes against different offsets as already observed when considering genuine score distributions (compare Fig. 6) is confirmed also with respect to EERs.

Overall, these results reveal that proper protection is only achieved when encrypting between 5% and 25% of the JPEG2000 packet data (significantly depending on the recognition scheme applied) and that encryption should start right at the begin of the JPEG2000 bitstream.

V. Conclusion

We have proposed to selectively encrypt the JPEG2000 codestream of normalised iris texture to achieve a low-cost yet highly secure protection of iris sample data. Comparing the security assessment done in case of directly decoding the encrypted data to the case error-concealment has been done during decoding reveals that security is highly over-estimated in case the assessment does not assume an informed attacker (who would apply error-concealment in decoding). We have found that (i) encryption should always start at the start of the bitstream and that (ii) the amount of data required to be encrypted for decent protection highly depends on the actual recognition system applied to the data. Thus, protection equivalent to full encryption can be achieved when encrypting 1/60 – 1/12 of the data amount of a full iris sample encoded in a JPEG2000 file. It turns out that the amount of data required to be encrypted directly corresponds to the recognition performance ranking of the different recognition schemes seen on clear data. Therefore, taking future improvements in iris recognition technology into consideration, we recommend to encrypt 50% of the normalised texture JPEG2000 packet data, still being only 1/6 of the data amount of a full iris sample encoded in JPEG2000. In future work, we will explicitly compare the proposed approach to an encryption of full iris sample data in terms of required encryption effort and achieved security and will analyse the reason for observed differences.

Acknowledgment

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

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] R. W. Ives, R. P. Broussard, L. R. Kennell, and D. L. Soldan, "Effects of image compression on iris recognition system performance," *Journal of Electronic Imaging*, vol. 17, pp. 011 015, doi:10.1117/1.2 891 313, 2008.

[3] S. Rakshit and D. Monro, "Effects of sampling and compression on human iris verification," in *Proceedings of the IEEE International Conference on Acustics, Speech, and Signal Processing (ICASSP 2006)*, Tolouse, France, 2006, pp. II–337–II–340.

[4] ——, "An evaluation of image sampling and compression for human iris recognition," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 605–612, 2007.

[5] J. Daugman and C. Downing, "Effect of severe image compression on iris recognition performance," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 52–61, 2008.

[6] S. Matschitsch, M. Tschinder, and A. Uhl, "Comparison of compression algorithms' impact on iris recognition accuracy," in *Proceedings of the 2nd International Conference on Biometrics 2007 (ICB'07)*, ser. LNCS, S.-W. Lee and S. Li, Eds., vol. 4642. Springer Verlag, 2007, pp. 232–241.

[7] S. Jenisch, S. Lukesch, and A. Uhl, "Comparison of compression algorithms' impact on iris recognition accuracy II: revisiting JPEG," in *Proceedings of SPIE, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, San Jose, CA, USA, Jan. 2008, p. 68190M ff.

[8] J. Hämmerle-Uhl, C. Prähauser, T. Starzacher, and A. Uhl, "Improving compressed iris recognition accuracy using JPEG2000 RoI coding," in *Proceedings of the 3rd International Conference on Biometrics 2009 (ICB'09)*, ser. LNCS, M. Tistarelli and M. Nixon, Eds., vol. 5558. Springer Verlag, 2009, pp. 1102–1111.

[9] J. Hämmerle-Uhl, M. Karnutsch, and A. Uhl, "Evolutionary optimisation of JPEG2000 Part 2 wavelet packet structures for polar iris image compression," in *Proceedings of the 18th Iberoamerican Congress on Pattern Recognition (CIARP'13)*, ser. Springer LNCS, vol. 8258, Havana, Cuba, 2013, pp. 391–398.

[10] ——, "Recognition impact of JPEG2000 part 2 wavelet packet subband structures in polar iris image compression," in *Proceedings of the 19th International Conference on Systems, Signals and Image Processing (IWSSIP'12)*, B. Zovko-Cihlar, M. Rupp, and C. Mecklenbräuker, Eds., 2012, pp. 13–16.

[11] J. Hämmerle-Uhl, E. Tillian, and A. Uhl, "Recognition impact of JPEG2000 Part 2 wavelet packet subband structures in IREX K3 iris image compression," *International Jounal of Information and Electronics Engineering (Proceedings of ICSIA'14)*, vol. 5, no. 1, pp. 51–54, 2015.

[12] C. Rathgeb, A. Uhl, P. Wild, and H. Hofbauer, "Design decisions for an iris recognition sdk," in *Handbook of Iris Recognition*, second edition ed., ser. Advances in Computer Vision and Pattern Recognition, K. Bowyer and M. J. Burge, Eds. Springer, 2016.

[13] C. Rathgeb, A. Uhl, and P. Wild, "Effects of severe image compression on iris segmentation performance (best poster award)," in *Proceedings of the IAPR/IEEE International Joint Conference on Biometrics (IJCB'14)*, 2014.

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

[15] F. Dufaux, S. Wee, J. Apostolopoulos, and T. Ebrahimi, "JPSEC for secure imaging in JPEG2000," in *Applications of Digital Image Processing XXVII*, A. G. Tescher, Ed., vol. 5558. SPIE, Aug. 2004, pp. 319–330. [Online]. Available: http://link.aip.org/link/?PSI/5558/319/1

[16] 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.

[17] ——, "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, Singapore, 2016, pp. 241–253.

[18] ——, "Sensor dependency in efficient fingerprint image protection using selective jpeg2000 encryption," in *Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF'17)*, Coventry, United Kindom, 2017, pp. 1–6.

[19] 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.

[20] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Efficient iris recognition by characterizing key local variations," *IEEE Transactions on Image Processing*, vol. 13, pp. 739–750, 2004.

[21] L. Masek, "Recognition of Human Iris Patterns for Biometric Identification, Master's thesis, University of Western Australia, 2003."

[22] J.-G. Ko, Y.-H. Gil, J.-H. Yoo, and K.-I. Chung, "A novel and efficient feature extraction method for iris recognition," *ETRI Journal*, vol. 29, no. 3, pp. 399 – 401, 2007.

[23] D. Monro, S. Rakshit, and D. Zhang, "DCT-based iris recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 586–595, 2007.