Efficient Fingerprint Image Protection Principles using Selective JPEG2000 Encryption

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

***Abstract*—Biometric system security requires cryptographic protection of sample data under certain circumstances. We introduce and assess low complexity selective encryption schemes applied to JPEG2000 compressed fingerprint data. From the results we are able to deduce design principles for such schemes which will guide to finally design recognition system aware encryption schemes with low encryption complexity and decent protection capability.**

I. Introduction

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

The certainly most relevant standard for compressing image data relevant in biometric systems is the ISO/IEC 19794 standard suite on Biometric Data Interchange Formats where in the most recently published version, only JPEG2000 is included for lossy compression of fingerprint images. 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) also supports only JPEG2000 for applications tolerating lossy compression.

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.

To cope with these demands for protecting template data (but not sample data) and enabling template matching in the encrypted domain, various flavours of template protection schemes have been developed, termed biometric cryptosystems and cancelable biometrics [2]. While these techniques provide sufficient computational efficiency for practical employment, most approaches are restricted to verification, biometric recognition accuracy is decreased in many techniques, and security concerns have arisen for some approaches. As an alternative approach, matching in an homomorphic encrypted domain [3], [4] has been suggested – while providing satisfying security and suited for identification applications in principle, the low computational efficiency prevents its usage in large-scale identification scenarios currently.

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

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

II. Efficient Encryption of Fingerprint Data

A. JPEG2000 Encryption in the Biometric Context

A large variety of custom image and video encryption schemes have been developed over the last years [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. In a JPEG2000 codestream either packet headers or packet body data (or both) may be encrypted. In the biometric context, the protection of packet headers is not particularly necessary: First, the data contained in the header facilitates the generation of a strong JPEG2000 fingerprint suited for unique identification of the specific image being compressed (but this hardly poses a security threat as a second image of the identical trait will exhibit a very different JPEG2000 fingerprint due to the intra-subject variability) [8]. Second, only a rough approximation of the pictorial data can be obtained based on header data [7]. Therefore, 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], [9].

B. Selective JPEG2000 Encryption Approaches

In the following, we introduce three different selective encryption techniques how to apply encryption to different parts of the JPEG2000 codestream. Those methods are useful for determining how much data need to be protected by encryption when distributing encryption differently.

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 three 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. For format compliance, 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 [10].

The "Absolute Encryption" mode (see Fig. 1) encrypts each packet data byte starting right after the first EPH marker. This is done until the given amount of encryption (in % of the overall data) is reached. This is the classical mode applied to many embedded or scalable data streams assuming that the (perceptually) most relevant information is stored at the start of the stream.

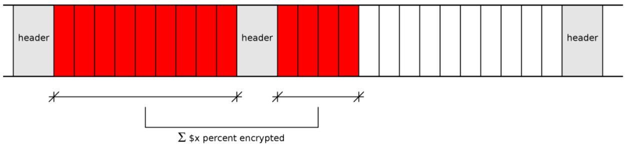

Figure 1. Absolute Encryption mode

"Sequential Encryption" (see Fig. 2) encrypts a given percentage of each packet within the file. The encryption is started with the first byte after each EPH header. The amount to be encrypted in each packet needs to be computed based on the number of packets and the amount of data to be protected.

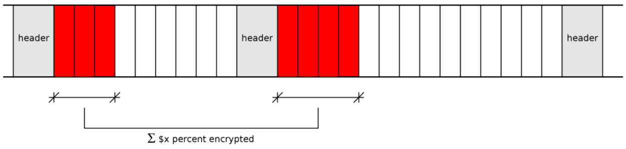

Figure 2. Sequential Encryption mode

In "Distributed Encryption" (see Fig. 3), the specified amount of encryption is introduced with uniform spacing between single encrypted bytes. Distances between encrypted bytes are calculated on per packet basis. The protected information is uniformly distributed within each packet and does not start right after each packet header.

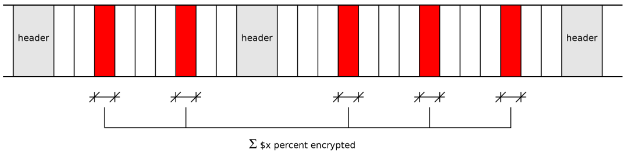

Figure 3. Distributed Encryption mode

Sequential and Distributed Encryption are used to investigate, if other information than the perceptually most relevant one (as covered by Absoute Encryption when applied to data stored in layer progressive order as done in our experiments) is of specific value in fingerprint recognition.

1) Security Assessment: When assessing the security of format compliantly encrypted visual data, the data can simply be decoded with the encrypted parts (called "direct decoding"). Due to format compliance, this is possible with any given decoding scheme, however, the encrypted parts introduce noise-type distortion into the data which kind of overlay the visual information still present in the data (see Figs. 4, 6, and 8). 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"). The JJ2000 version used in the experiments includes the patches and enhancements to JPEG2000 error concealment provided by [11].

As visible in Figs. 4 and 6 even after error concealment attacks ridge and valley information can still be present, which could be improved further with fingerprint specific quality enhancement techniques (thus, images like those cannot be assumed to be sufficiently secured). Only the error concealment example in Fig. 8 does no longer exhibit any fingerprint related structures which could be exploited by an attacker.

The general assessment of the security of low quality encrypted visual data (as obtained by direct decoding or error concealment attacks) is difficult. Although classical image and video quality metrics (IVQM) like SSIM or even PSNR have been repeatedly applied to such data, it has been shown recently that this does not correlate well to human perception [12]. Moreover, the general quality appearance to human observers is not at all relevant in our setting. Only the assessment of forensic fingerprint experts would meake sense in terms of human judgement.

However, in our case, security assessment does not need tdoes not need too 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.

2) Assessment of Computational Savings: The computational efficiency of selective encryption schemes strictly depends on the employed encryption primitives and not only on the reduction of the amount of data to be encrypted. In particular, additional computational cost is caused by the JPEG2000 codestream parsing effort to determine encryption startpoints and the multiple encryption initialisiations. Thus, Sequential and Distributed Encryption are clearly less efficient as compared to Absolute Encryption. Therefore, Absoute Encryption of 3% of a JPEG2000 file with AES would suffice with actually 3% of the computational cost of a full encryption with AES, while Distributed Encryption of 3% of a JPEG2000 file might eventually cause the same cost as full AES encryption, e.g. in case of highly efficient encryption routines but very costly encryption initialisation.

III. Fingerprint Recognition

In minutiae-based matching schemes, 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.

IV. Experiments

A. 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 ordering. Subsequently they are encrypted using the different variants with increasing amount of data encrypted and subsequently either directly decoded or decoded with enabled error concealment with the JJ2000 variant mentioned [11].

The procedure used for matching the decoded / encrypted fingerprint images is chosen to be the same as FVC demands for performance evaluation; the probe image is decoded / encrypted while the gallery images are in plaintext. Overall, we will consider equal error rate (EER) and receiver operating curves (ROC) to compare the protection capabilites of the different encryption schemes. Obviously, higher EER corresponds to better data protection as well as worse ROC behaviour is preferred for better data protection.

B. Experimental Results

Table I compares the EER as obtained by Absolute, Sequential, and Distributed Encryption variants when encrypting up to 3% of the packet data. Already at first sight it gets clear that (i) under error concealment EER are lower (less secure) as compared to direct decoding for all three methods and (ii) for all techniques but Sequential Encryption under error concealment an EER of 50% is achieved which means that these techniques do not deliver any sensible recognition on the protected data.

Table I. EER [%] - Encryption variants under NBIS

	Absolute		Sequential		Distributed	
% enc	direct	err.conc	direct	err.conc	direct	err.conc
0.0	9.01	9.01	9.01	9.01	9.01	9.01
0.5	47.67	26.04	45.55	30.56	42.25	41.58
1.0	49.21	34.00	49.95	37.42	50.64	47.23
1.5	50.22	40.66	50.05	39.82	50.03	51.08
2.0	50.42	44.77	50.32	41.27	48.59	49.02
2.5	51.29	46.97	50.96	38.50	48.40	50.03
3.0	51.58	49.47	49.24	41.46	52.23	49.83

Distributed Encryption reaches high EER with the lowest amount of data encrypted which suggests that only encrypting data at the start of the bitstream or at the start of each header is not enough for optimal employment of encryption. Sequential Encryption under error concealment does not even reach the targeted 50% EER with 3% of data being encrypted.

In Fig 4 corresponding image examples for Absolute Encryption are given. Also the visual impression confirms that error concealment indeed is able to reveal data which seems to be protected under direct decoding.

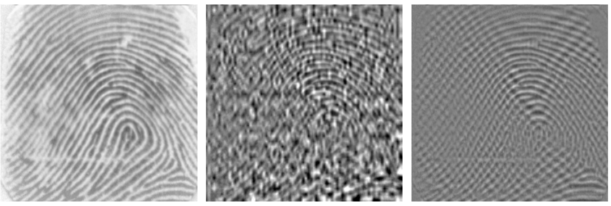

Figure 4. Examples - Absolute Encryption (original, 0.5% encrypted with direct reconstruction and error concealment, respectively)

Fig. 5 displays the recognition performance in terms of ROC measured on data encrypted with Absolute Encryption for increasing amount of encryption. Results as suggested by EER values are confirmed. When considering error concealment, 3% of the data should be encrypted to reach a protection level which is already seen at encrypting 1% of the data using direct decoding. Thus, the assessment using direct decoding is severely misleading since it assumes a somewhat dumb attacker without deeper knowledge.

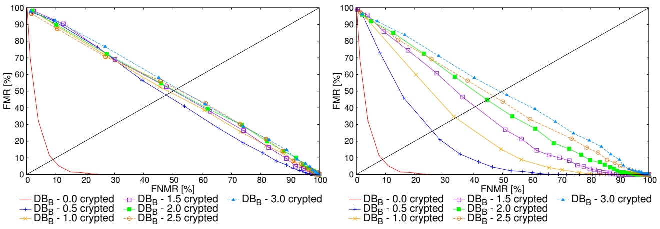

Figure 5. ROC - Absolute Encryption - direct reconstruction vs. error concealment attack

Fig. 6 shows visual examples of applying Sequential Encryption which reveals that even when encrypting 3% of the data, ridges and valleys are still visible (quite clear under error concealment) which can be exploited by NBIS to some extent as already seen in Table I. Thus, more data needs to be encrypted to achieve proper security.

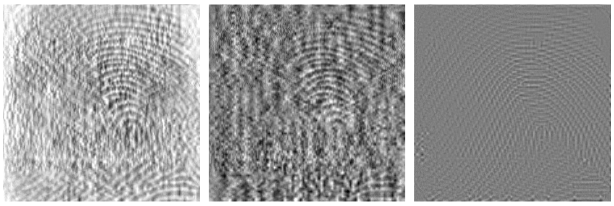

Figure 6. Examples - Sequential Encryption (direct reconstruction when 0.5% and 3.0% encrypted, error concealment with 3.0% encrypted)

Fig. 7 displays ROC results for Sequential Encryption. While being clearly more secure compared to Absolute Encryption under error concealment for a low amount of encrypted data, the desired decrease of ROC behaviour for higher data amounts cannot be observed. Obviously, this is not the perfect strategy as well.

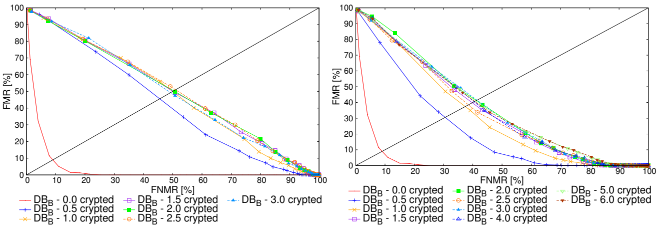

Figure 7. ROC - Sequential Encryption - direct reconstruction vs. error concealment attack.

As the last set of examplary images, Fig. 8 shows example fingerprints if protected by Distributed Encryption. While it gets clear that 0.5% encryption is not sufficient, encrypting 3% of the data turns out to provide a decent protection of fingerprint image content. Even after arror concealment, no useful ridge and valley information is left in the image.

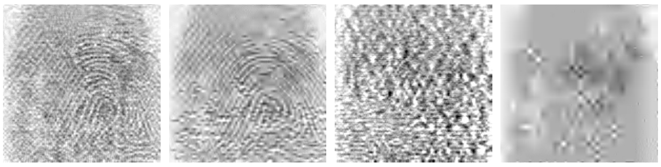

Figure 8. Examples - Distributed Encryption (0.5% encrypted with direct reconstruction and error concealment; the same for 3.0% encrypted)

Fig. 9 confirms this observation. There is hardly a difference between direct decoding and error concealment application (which is good for security) and the amount of data to be protected is very low (starting from 1% encryption, ROC is very poor).

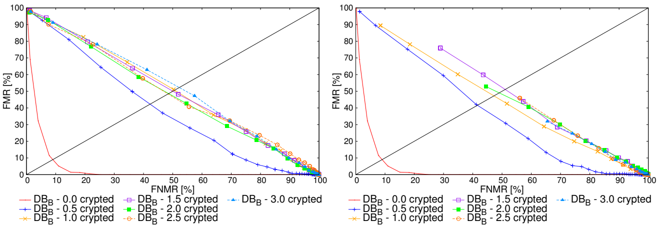

Figure 9. ROC - Distributed Encryption - direct reconstruction vs. error concealment attack.

V. Conclusion

We have seen that it indeed makes a difference which selective encryption strategy is used (especially when considering error concealment attacks) and that the best variant does not correspond to the classical strategy as used on embedded / scalable data formats (which would be Absolute Encryption). However, the best performing technique in terms of security exhibits the highest computational effort since it requires the parsing and encryption of single bytes in the packet data.

We have identified encryption schemes which provide decent security when encrypting 3% - 5% of the JPEG2000 packet data only (which corresponds to reducing encryption effort by more than 95% for non format-compliant encryption schemes).

ACKNOWLEDGMENT

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

REFERENCES

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

[2] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 3, 2011.

[3] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Cogniat, and R. Sirdey, "Recent advances in homomorphic encryption," *IEEE Signal Processing Magazine*, vol. 2, no. 30, pp. 108–117, 2013.

[4] A.-R. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient privacy-preserving face recognition," in *Proceedings of the International Conference on Information, Security, and Cryptology (ICISC'09)*, ser. Springer LNCS, vol. 5984, 2010, pp. 229–244.

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

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

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

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

[9] ——, "Efficient transparent JPEG2000 encryption with format-compliant header protection," in *Proceedings of IEEE International Conference on Signal Processing and Communications, ICSPC '07*. Dubai, UAE: IEEE, Nov. 2007, pp. 1067–1070.

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

[11] ——, "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.

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