SECURITY ANALYSIS OF A CANCELABLE IRIS RECOGNITION SYSTEM BASED ON BLOCK REMAPPING

Stefan Jenisch and Andreas Uhl

Department of Computer Sciences
University of Salzburg, Jakob-Haringer-Str. 2, A5020 Salzburg, Austria

ABSTRACT

Cancelable biometric systems are designed to provide intrinsic protection for biometric templates in case of a database breach. In this paper a security survey of a cancelable iris recognition system is conducted. It uses block permutation and remapping of the iris texture as a strategy for template protection.

Two adjunctive scenarios and their impact on the security of the system are examined. First off it is assumed that an attacker got a hold on a single iris template. In the second scenario it is presumed that multiple templates of the same biometric characteristic are available to an attacker. The scenario of a so called "Coalition Attack".

The test runs conducted suggest that the system does offer some resistance against a template theft but sacrificing overall system performance and usability for it.

***Index Terms*—** Iris recognition, Cancelable biometrics, Security analysis, Coalition attack

1. INTRODUCTION

One major disadvantage of biometric authentication systems is that in case they become compromised, they are compromised for good. Because unlike a password replacing a biometric characteristic (eg. a finger or an eye) is, as far as current medical research suggests, not an easy task.

The research on the field of cancelable biometrics tries to compensate for that lack.

The basic idea is to manipulate the biometric data, like an iris scan, by interweaving some sort of key into it. In case the system becomes compromised the users can be re-enrolled with the same biometric characteristic using a different key.

Thereby the interweaving of the key should make it impossible for an attacker to regain the full featured biometric data of a user merely from thieving a template out of a biometric database. According to Ratha *et al.* [1] this can be done in the image domain before feature extraction or thereafter in consideration of the respective extraction algorithm. In the domain of iris recognition several ideas for cancelable systems have been discussed already [2, 3, 4].

This paper sets its focus on the security of a custom made iris recognition system based on the feature extraction algorithm of Ma *et al.* [5] which is supplemented by a permutation and remapping algorithm manipulating the biometric data in the image domain [6, 7].

Section 2 contains a short description of the system while Section 3 and 4 shed some light on the performance and vulnerability of it.

This work has been partially supported by the Austrian Science Fund, TRP project no. L554

2. THE CANCELABLE BIOMETRIC SYSTEM

The algorithm proposed by Ma *et al.* starts with the extraction of the iris texture. The annular iris shape is unwrapped and extrapolated into a rectangular iris texture of 512x64 pixels (Figure 1 (a)).

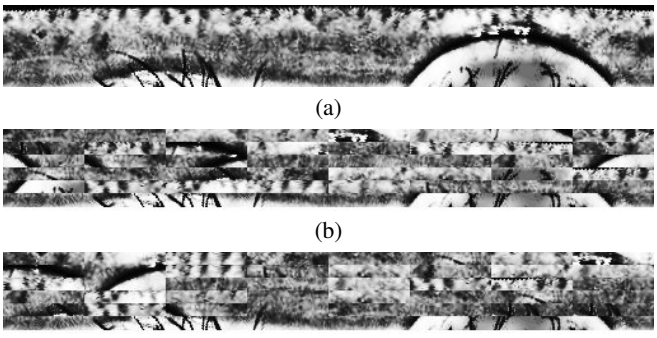
After the unwrapping there are still some fragments of the pupil found at the top of the iris texture. To remove those the texture is shifted upward by three rows of pixels while at the bottom three "blank" rows are inserted. Furthermore fourteen rows at the bottom of the texture are neglected as a tribute to eyelids and eyelashes.

Subsequently, ten signal bands are derived by averaging the luminance values of five succeeding rows of pixels together, beginning at the top of the texture.

In the next step the signal bands are concatenated in the respected order and a wavelet transformation is performed on using a quadratic spline wavelet. The resulting signal is then turned into a alternating sequence of 0 and 1, switching between values at the positions of maximas and minimas in the signal.

The comparison of two iris images is merely the calculation of the Hamming distance between two of those derived bitstrings.

Additionally, a bit mask is extracted from the iris texture marking the areas covered by the eyelids and eyelashes on the bottom of the texture. The bit mask is later incorporated into the matching process by leaving out every bit of the bitstring associated with an area concealed by an eyelid or eyelash when calculating the Hamming distance.



(a)

(b)

(c)

Fig. 1*:* A plain, a permuted and a remapped iris texture

2.1. Interweaving the key - permutation and remapping

Naturally the permutation and remapping process takes place after the extraction of the iris texture but before derivation of the signal bands.

First the texture is partitioned into blocks of a fixed size (eg. 64x10 pixels). In regard to the feature extraction algorithm and subsequently in respect to the eyelids and eyelashes the last fourteen rows of pixels are excluded from the partitioning. Then two operations are carried out:

- **Permutation:** The blocks of the texture are rearranged according to a permutation key. In Figure 1 (b) a permutation of an iris texture is shown.
- **Remapping:** The former step of randomization of blocks is an invertible operation. Anybody in possession of the permutation key is able to undo this operation without any effort. To provide protection against a compromised key the remapping operation is performed. It duplicates some of the blocks atop of others eliminating them from the iris texture, thus making a full reconstruction of the iris texture impossible. The process takes two parameters: The number of blocks used as a source for duplication and the count of how many times these blocks should be reused as a source for the duplication process. In Figure 1 (c) a remapped iris texture is shown.

  Additionally, when selecting a source block the aforementioned bit mask can be consulted to determine how much valuable iris texture is concealed by an eyelash or lid. Blocks with too much concealed area can be ignored as a source for the remapping process. This ensures that a sensible amount of iris texture is provided to the matching process instead of duplicating eyelids and lashes all over the place.

Naturally the bit mask is updated accordingly in both steps. Further details of the matter are given in [6] and [7].

3. VULNERABILITY ANALYSIS OF THE SYSTEM

Since the block permutation leaves a vulnerability in case of a compromised permutation key it has to be consider less secure. This is why the focus of the analysis is aimed onto the remapping process.

Essentially the remapping process conceals information from the attacker by removing blocks from the texture. The removed pieces can be used later on for a re-enrollment of the user. But the question remains: How much iris texture has to be removed by the remapping process in the first place to lock out the attacker for good?

Considering an acceptance threshold of 60% of coinciding bits for the system more than 40% of bits have to be removed. Or more precisely, the corresponding amount of iris texture has to be eliminated by the remapping process. A threshold of 60% is assumed because the utilized biometric system usually reaches an optimum concerning the balance between "False Match Rate" (FMR) and "False Non Match Rate" (FNMR), i.e. "Equal Error Rate" (EER), around this value when turning off the permutation and remapping operations.

Furthermore the attacker is able to guess some missing pieces of the puzzle by filling the gaps with random noise. Using this method it is expected that he will be able to guess about half of the missing feature bits (i.e. template) correctly. This implies that an attacker starting with 50% of known template bits and guessing 25% correctly will achieve access to the system since the attacker will be able to synthesize an iris template with 75% of coinciding bits.

This circumstance requires removal of another 40% of iris texture settling the amount of "has to be removed" iris texture to over 80%. Thus, leaving less than 20% of the iris texture for the original matching process.

Now this will prevent an attacker from gaining access to the system if he was able to obtain a single iris template of a user. But what if he was able to obtain several templates, each of which containing different parts of the iris texture ("Coalition Attack")?

No. of iris templates	Expected % of iris texture known to the attacker
1	20%
2	30%
3	33.3%
10	38%
50	39.6%
100	39.8%

Table 1: Progression of a coalition attack

It is most likely that some information the attacker extracts from the differently remapped iris templates is identical. In case of two differently remapped textures on average about half of the iris texture will be identical while the other half will provide new texture information.

In case of a system with a threshold of 60%, a remapping process leaving little less than 20% of original iris texture to the system and an attacker who was able to obtain two iris templates of the same user with different remapping will have about 30% of iris texture at his hands. This is because he knows little less than 20% of the whole iris texture from the first template and additionally gains a little less than 10% from the second one (10% texture identical to the first template + 10% unknown texture). Thus, it is most likely that he will succeed when attempting to gain unprivileged access since he will be able to guess about 35% of additional texture pushing it all up to 65% and past the acceptance threshold of the system.

The formula

$$c + \left(\frac{c}{n}\right) * (n-1) \tag{1}$$

allows to calculate the expected percentage of iris texture known to the attacker after he obtained n templates from an eye with c percent of texture left behind by the remapping process. With the first template the attacker gains c percent of the iris texture. Every additional iris template will potentially get the attacker about $c/n * (n-1)$ former unknown information.

Equivalently the formula can be written as:

$$c * \left(2 - \frac{1}{n}\right) \tag{2}$$

To illustrate the expected progression of such a coalition attack in Table 1 some results for a given n and for a value of $c = 20\%$ are listed. It can be seen in the table the gain of iris texture stagnates at about 40%.

To prevent such an coalition attack from being successful this formula can be used to calculate the maximum amount of iris texture allowed to be left behind by the remapping process by inserting it into the equation:

$$t > c * \left(2 - \frac{1}{n}\right) + \frac{100\% - c * \left(2 - \frac{1}{n}\right)}{2} \tag{3}$$

On the left hand side of the equation the matching threshold of the system t is found, expressed in percent of matching bits. The right hand side represents the information usable to the attacker. Again c stands for the percent of texture left by the remapping process and n for the number of templates obtained by the attacker. Ad-

ditionally, the right hand side is extended to tribute the fact that the attacker is able to guess half of the iris texture.

Transforming the formula it becomes:

$$2 * t - 100\% > c * \left(2 - \frac{1}{n}\right) \tag{4}$$

Now taken the case the attacker is able to get a hold on an infinite number of iris templates of a user we extend the formula to:

$$\lim_{n \to \infty} \left(2 * t - 100\% > c * (2 - \frac{1}{n})\right) \tag{5}$$

Assuming further that 60% of matching bits serve as a threshold for the system, the maximum amount of texture allowed to be left by the remapping process has to be:

$$2 * 60\% - 100\% > 2 * c \tag{6}$$
$$\equiv 10\% > c$$

So to be secure according to the expectation values this cancelable biometric system has to leave less than 10% of texture to the subsystem performing the matching. According to [1] odds are that this will influence the overall performance of the system negatively.

4. EXPERIMENTS

As a first step a test run has been conducted extracting iris textures from the CASIA V3 interval iris database [1] and matching them against each other excluding the permutation and remapping process to establish a basis of comparison. The "Receiver Operating Characteristic" (ROC) curves bringing FMR and FNMR in relation with each other is displayed in Figure 2. Without the obfuscation process the system settles at an EER of 1.2.

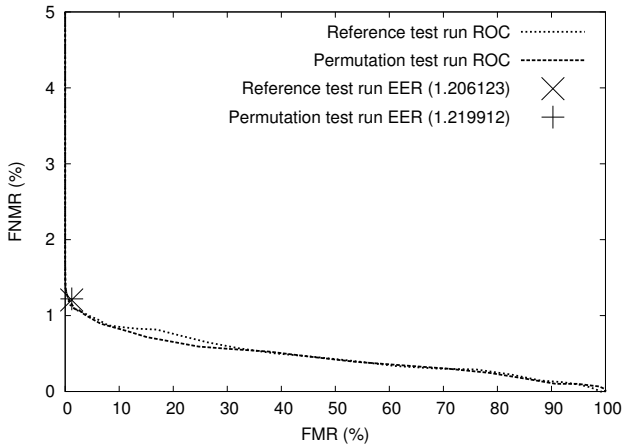


Fig. 2: ROC of the reference and of a "permutation only" test run

When introducing the permutation process into the system the performance does not significantly increase or decrease. In Figure 2 the ROC curve of a "permutation only" test run are shown. Based on [6] for this run and all succeeding experiments a blocksize of 64x10 pixel was chosen, partitioning the iris texture into 40 segments. The average EER for ten "permutation only" test runs was 1.223 with a minimum or maximum of 1.199 and 1.267.

[1] http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

No.	Texture left	EER	No. source blocks used for remapping	No. of reuses of source block
1:	62.1%	0.8526	10	2
2:	62.9%	1.0942	10	1
3:	43.3%	0.8147	10	3
4:	34.2%	0.8266	13	3
5:	25.0%	0.8408	10	4
6:	23.4%	0.8169	6	6
7:	20.0%	0.8588	8	5

Table 2: Parameters and EER of test runs showing the improvement when reducing the amount of iris texture

When introducing the remapping process into the system the performance of the system increases. In Table 2 the parameters and EER values of several test runs are listed. In columns two and three the amount of texture left behind by the remapping process and their EER values are listed. All EER values are below the score of the reference run of 1.2. The last two columns list the parameters passed to the remapping process. For instance, in the last listed run eight random blocks where selected and copied over five other randomly selected blocks leaving behind 20% of texture. The system still achieves an EER of 0.8588 with so little information left behind by the process.

The increase in performance may be explained by the fact that the system uses a key per user (as opposed to a key per database). This introduces additional information into the system referencing a user besides his iris texture.

Furthermore Rathgeb *et al.* [8] found that certain parts of the iris texture are more reliable than others. They demonstrated that a system using only these parts can outperform a system using the whole texture.

So it comes to no surprise that the system seems to be strongly dependent on the selection of the source blocks. This can easily be observed when conducting several test runs with the same parameter set. For example, when the fifth test run from Table 2 was repeated ten times the EER values of those runs oscillated between 0.94 and 1.39 with a mean value of 1.12 and a variance of 0.02.

The influence of the block selection onto the EER gets even more evident when comparing test runs which incorporate information about the position of eyelids and lashes for block selection with runs using pure random selection.

In Table 3 test runs with integration of the bit mask turned on and off are listed below each other. For instance, the test runs A1 and A2 use the same parameters for the remapping process (see column two, three and four) but A2 achieves a better EER due to the incorporation of the bit mask (see last column). As can be seen in column five, for A2 the maximum amount of masked bits allowed in a source block for the remapping process was 20%. Choosing this parameter value in test run A2, 99.4% of unmasked iris texture is left behind to the matching process while in A1 only 85.6% are left (see column six).

Looking again at Table 2 it can be seen that as long as 100% to 20% of iris texture are left behind by the remapping process the system performs quite well when comparing the EER values to the initially given reference with an EER of 1.2.

Unfortunately this changes when entering the realm below the 20% barrier which as formerly pointed out has to be undergone to circumvent one-time attacks for a system with a threshold of 60% matching bits. And it gets worse when going below the 10% barrier which has to be undergone to prevent coalition attacks.

No.	No. source blocks used for remapping	No. of reuses of source block	Max. allowed masked bits on blocks	Percent of unmasked bits	Texture left	EER
A1:	4	10	10.0%	—	85.6%	2.846
A2:	4	10	10.0%	20%	99.343%	1.244
B1:	2	20	5.0%	—	84.803%	10.57
B2:	2	20	5.0%	20%	99.423%	3.924
C1:	1	40	2.5%	—	85.071%	25.897
C2:	1	40	2.5%	20%	99.713%	14.012

Table 3*:* Incorporation of the iris mask into block selection influencing EER

No.	No. source blocks used for remapping	No. of reuses of source block	Percent of unmasked bits	Texture left	EER
1:	8	5	83.247	20.0%	1.49
2:	5	8	83.376	12.0%	1.807
3:	4	10	85.600	10.0%	2.846
4:	3	13	85.141	9.79%	3.946
5:	2	20	84.803	5.0%	10.57
6:	1	40	85.071	2.5%	25.897

Table 4*:* Test runs with less than 20% of iris texture left, showing the escalation of the EER in this realm

In Table 4 the EER values and parameters of test runs below the 20% barrier are listed. It can bee seen that below the 10% barrier the EER increases rapidly. Figure 3 shows the ROC curve of a test run containing only 5% of original iris texture. All those test runs have been performed omitting the incorporation of the iris mask for block selection.

It is presumed from the test runs B1, B2 and C1, C2 found in Table 3 that the incorporation of the iris mask will improve the EER values of the test runs, but still they will be far from an EER of 1.2 achieved by the reference run.

5. CONCLUSION

Summing it up, the system has to be considered still vulnerable at texture values above and around 10% for a threshold of 60% matching bits. Adding extra security against coalition attacks recommends to leave less than 10% of texture behind going below 8% to 5% for this setup.

Unfortunately the EER values of the cancelable biometric system goes up rapidly when leaving less then 10% of iris texture to the matching process increasing the FNMR as well as the FMR.

Incorporating these two facts it is highly questionable if the system is suitable for practical application.

However when using a higher threshold the strength of the system against coalition attacks improves. Given a threshold of 80% matching bits the remapping process has to leave less than 30% of iris texture behind to prevent coalition attacks according to probability theory. Though a higher threshold increases the FNMR, which again questions usability of the system for everyday use.

Hence, there is always a tradeoff between security and usability of a system.

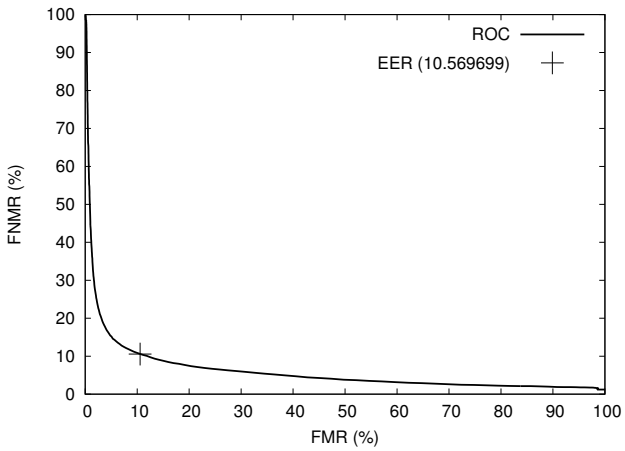


Fig. 3*:* ROC curve of a test run containing 5% of iris texture (Mind the change of scale along the y-axis)

6. REFERENCES

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[2] S. C. Chong, A. T. B. Jin, and D. N. C. Ling, "High security iris verification system based on random secret integration," *Computer Vision and Image Understanding*, vol. 102, no. 2, pp. 169–177, 2006.

[3] S. C. Chong, A. T. B. Jin, and D. N. C. Ling, "Iris authentication using privatized advanced correlation filter," in *Proceedings of the 1st International IAPR Conference on Biometrics (ICB'06)*, 2006, vol. 4642 of *Springer Lecture Notes on Computer Science*, pp. 382–388.

[4] J. Zuo, N. K. Ratha, and J. H. Connel, "Cancelable iris biometric," in *Proceedings of the 19th International Conference on Pattern Recognition 2008 (ICPR'08)*, 2008, pp. 1–4.

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

[6] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *ISC '09: Proceedings of the 12th International Conference on Information Security*. 2009, pp. 135–142, Springer Berlin / Heidelberg.

[7] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschernig, and A. Uhl, "Transforming rectangular and polar iris images to enable cancelable biometrics," in *Image Analysis and Recognition*, vol. 6112 of *Lecture Notes in Computer Science*, pp. 276–286. Springer Berlin / Heidelberg, 2010.

[8] C. Rathgeb, A. Uhl, and P. Wild, "Incremental iris recognition: A single-algorithm serial fusion strategy to optimize time complexity," in *In Proceedings of the 4th IEEE International Conference on Biometrics: Theory, Application, and Systems 2010 (IEEE BTAS'10)*. 2010, pp. 1–6, IEEE Press.