Subsurface and Layer Intertwined Template Protection Using Inherent Properties of Full-Field Optical Coherence Tomography Fingerprint Imaging

Kiran B. Raja[†] R. Raghavendra[†] Egidijus Auksorius[‡] Christoph Busch[†]
[†]Norwegian Biometrics Laboratory, NTNU - Gjøvik, Norway
[‡]Institute of Physical Chemistry, Polish Academy of Sciences, Poland.
{kiran.raja; raghavendra.ramachandra; christoph.busch} @ntnu.no
eauksorius@ichf.edu.pl

Abstract

The emergence of Full Field-Optical Coherence Tomography (FF-OCT) for fingerprint imaging has shown it's ability in addressing and solving the drawbacks of traditional fingerprinting solutions such as spoofing attacks, low accuracy for abraded fingerprint. With the availability of multiple internal fingerprints (from subsurface captured at different depths), it is also essential to consider the aspects of ideal biometrics where the privacy of the fingerprint data is preserved. In this work, we propose a new framework for fingerprint template protection, highly customized to FF-OCT by exploring the interplay between subsurface. As a first of it's kind work attempting template protection for FF-OCT fingerprints, we explore deeply learnt features to derive first level of template for subsurface fingerprint image. We further propose to intertwine subsurface level templates to provide better and robust templates. With the set of extensive experiments on a FF-OCT fingerprint database of 200 *unique fingerprints with a total of* 2400 *images, we demonstrate reliable biometric performance resulting in EER of* 5.69% *for unprotected template at first layer (subsurface) of fingerprint in FF-OCT, an EER of* 5.86% *for the protected templates at same layer and EER of* 5.08% *with the final protected templates with proposed intertwining of subsurface fingerprint. Further, through the security analysis, we also validate the strength of the proposed approach with near ideal unlinkability.*

1. Introduction

Authenticating an individual based on various biometric characteristics has become ubiquitous way of verifying identity in various secure access control applications. A number of biometric characteristics such as face, iris, fingerprint and palmprint have become widely used for verification and identification applications. The vulnerability due to presentation attacks through lifted fingerprints and the production of artefacts based on silicone and other material, the traditional problem of cuts, abrasions and burns on the fingerprint has resulted in loss of biometric performance and loss of trust in classical fingerprint solutions [20].

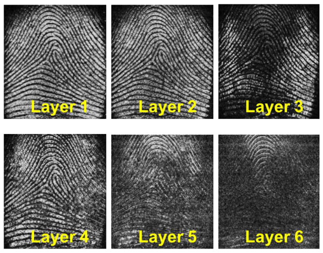

Figure 1: Sample fingerprint imaged at various subsurface depth captured using FF-OCT device. The Layer-1 to Layer-6 corresponds to images acquired at the depth of $70\mu m$ to $420\mu m$ in the steps of $70\mu m$. The varying information across different layers can be noticed due to attenuation of the light by various tissues in the subsurface of the fingerprint.

The need for capturing the fingerprint in a reliable manner cannot be undermined. However the newer image acquisition technologies have emerged for capturing not just the external/surface fingerprint, but also internal fingerprints. These newer approaches have demonstrated to handle the problems arising due to surface degradation or loss of outer fingerprints as a result of injuries and also address the presentation attacks [2, 4, 32, 15, 28]. Optical coherence tomography (OCT) is one such approach that is able to acquire subsurface images from deep within living tissue, such as the finger [14]. An improved version with Full Field-OCT (FF-OCT) based fingerprint sensors was recently developed [2, 3]. The FF-OCT sensors are able to acquire the full volumetric (3D) data by translating the reference reflector in small steps and strategically pick only a set of images to record at different depths below the external fingerprint. The data captured using such OCT sensors have demonstrated good biometric performance for different subsurface imaging lengths [28, 6]. Apart from the conventional fingerprint that is recorded from the top of the stratum corneum and apart from sweat ducts that can be recorded from the inside of the stratum corneum, a low contrast fingerprint pattern could also be captured inside the stratum corneum.

While the new field of FF-OCT is promising to address the traditional challenges of abrasions, captures beneath skin can result in partial fingerprint instead of full fingerprint structure as shown in Figure 1. Further, it can be noted from Figure 1 that not all the layers can provide full fingerprint information including the minutiae positions due to imaging challenges beneath skin. While it is convenient for commercial algorithms (for instance, (Neurotech Verifinger [22])) to extract minutiae from external fingerprint images and thereby to provide robust performance, they do not perform optimally for subsurface fingerprints obtained from OCT/FF-OCT.

Despite the promising solutions offered by the new generation sensors against presentation attacks, the threat of template level attacks on the databases remain unaddressed. Thus, the necessity of template protection can be underlined even for the fingerprint data captured through new generation of sensors. Further, template protection schemes for such data is also necessary to preserve the privacy of the fingerprint images in accordance to EU-General Data Protection Regulations (GDPR) [9]. The template protection scheme should further strive to achieve ideal properties that allow to revoke the template under compromise situations. Further the standardised framework for biometric information protection in ISO/IEC 24745 requires the unlinkability of individual protected biometric templates, which are stored in multiple services, while maintaining the recognition accuracy of the biometric system [17, 5]. It is further noted that most of the template protection schemes for fingerprint recognition today are customized for traditional sensors such as optical/capacitive sensors which typically capture only the external fingerprint with good minutia details. Although the new generation of fingerprint sensors like FF-OCT and subsurface fingerprint imaging sensors are emerging, the problem of template protection is not addressed for FF-OCT in the literature to the best of our knowledge.

1.1. Related Works and Challenges

A number of approaches have been adopted to deal with the problem of biometric template protection [29, 26, 25, 24, 13] for multiple modalities including fingerprint images captured through traditional sensors [18, 8, 11, 30, 11, 31, 10]. The template protection schemes has been explored traditionally by employing the minutia points from fingerprint from conventional sensors through well used Minutiae Cylinder Code (MCC) [7, 8, 11]. Taking a similar approach, the next set of works used the minutia vicinity to create better template protection schemes [30, 11]. In a different paradigm, the authors in [31] provide a template protection scheme using the topology and structure information. The next set of works in the similar direction employed the strengths of minutia vicinity and complemented the strengths of Bloom filters to robust templates, specifically for fingerprints [1].

Although a plethora of works have proposed approaches for fingerprint template protection, due to the inherent nature of imaging in FF-OCT, these approaches cannot be directly employed to obtain optimal biometric performance after template protection. A primary reason is the different structural information such as ridges, valley, bifurcations and minutia information revealed across layers can be different compared to external fingerprint alone, especially when the external fingerprint is damaged due to abrasions or cuts. Thus, a template protection scheme for such FF-OCT fingerprints needs to fully utilize the layers under the external fingerprint to obtaining complementary features to derive robust templates. It was also reported in [19] that even commercial state-of-the-art fingerprint SDK (Neurotech Verifinger [22]) do not perform ideally across subsurface fingerprints in FF-OCT fingerprints due to differing/missing information and *the reported results indicate the need for customized and reliable feature extraction in addition to minutia in FF-OCT images. A direct implication of such missing minutia information renders the current template protection scheme based on minutia information sub-optimal for FF-OCT images with certain limitations in biometric performance.*

1.2. Contributions

Motivated by such factors and to employ the different subsurface images of FF-OCT fingerprint images to extract the complementary features to design a better template protection scheme, we intuitively explore the power of deep-Convolutional Neural Networks (CNN). The CNNs come with the inherent advantage of providing complementary features in the pipeline of feature extraction, for e.g., at various points of *fully-connected-layers* within the CNNs. With number of works that have reported impressive accuracy with such CNNs for fingerprint recognition [23, 33], we employ a similar idea to first extract discriminative information and thereafter use it for reliable template protection design by using different subsurface fingerprint images. While addressing the need of template protection for FF-OCT, we also propose a novel framework with subsurface level intertwined protected templates that is not only robust for biometrics but also provide high degree of unlinkability. Further, to assert our idea of exploring multiple subsurface fingerprint for robust template protection, we perform the experiments on a currently available large scale FF-OCT fingerprint database with 200 subjects. Specifically, we employ a set of 5 subsurface images from different depths (in the range of $70 - 420\mu m$ in the step size of $70\mu m$) from the FF-OCT fingerprint database whose details are briefed in the Section 3. The proposed framework performs very similar in biometric performance when compared to unprotected fingerprint recognition indicating the applicability of proposed approach for the deployment. The summary of our contributions can therefore be listed as below:

- We present the first work for fingerprint recognition from FF-OCT imaging sensors by employing the features from deep neural networks to fully leverage the complementary/supplementary information from different subsurface across various lengths of imaging. The state-of-art results are achieved by fine-tuning the AlexNet CNN [21] for the task of sub-surface fingerprint imaging in FF-OCT domain.
- Further, we present the first work and a novel framework for template protection for FF-OCT fingerprint images by employing multiple feature extraction layers (*Fully-Connected Layer 6 (fc6)* and *Fully-Connected Layer 7 (fc7)*) within fine-tuned CNN.
- Through the experiments on the presently available and largest FF-OCT fingerprint database [19] that was acquired with a novel FF-OCT fingerprint sensor [3], we demonstrate that the proposed framework can be employed for individual subsurface fingerprints with very high accuracy.
- As another novel and customized scheme for template protection for FF-OCT fingerprint images, we propose a layer intertwined architecture with high biometric performance and near ideal unlinkability. With the set of experimental results, we also demonstrate the applicability of proposed approach through extensive experiments and provide an analysis of security level of proposed template protection.

In the remainder of the paper, we present the proposed approach in Section 2 and then we briefly describe the FF-OCT fingerprint image database in Section 3. Subsequently evaluations through experiments are outlined in Section 4 and the results are discussed in the same section. Finally, we provide security analysis in Section 5 and the potential future works are listed in Section 6.

2. Proposed Approach

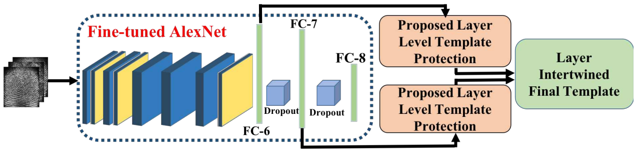
Fine-tuned AlexNet
FC-6
Dropout
FC-7
Dropout
FC-8
Proposed Layer Level Template Protection
Proposed Layer Level Template Protection
Layer Intertwined Final Template

Figure 2: Proposed template protection framework for FF-OCT fingerprint images.

Figure 2 presents the framework of the proposed approach for FF-OCT fingerprint template creation. As observed from the schematic of proposed approach, it can be seen that the features for the proposed template protection scheme are obtained through the fine-tuned deep CNN - AlexNet [21]. The specific choice of AlexNet comes from the applicability of the network to handle a small volume of data and yet provide superior biometric performance (for instance, for palmprint recognition [23]). Given a FF-OCT fingerprint image for a subsurface s, we obtain the Region of Interest (ROI) by manually cropping regions outside of fingerprint pattern. This is specifically done to remove all the biasing factors that may be introduced due the nature of FF-OCT imaging. The cropped ROI corresponding to subsurface s, represented by I_s is further resized to 227×227 pixels to comply with the input layer of AlexNet. With a chosen subset of fingerprints from 10 different subjects, we perform the fine-tuning to tailor AlexNet for the task at hand. In order to adapt the network easily, we bump the learning rate of the final layers and convergence is achieved in a relatively smaller time. With such adaptations, we learn the weights of the newer layer without modifying the network in the initial stages of AlexNet. Specifically, in our proposed framework we have employed a *weight learning rate factor* of 10 and *bias learning rate factor* of 20.

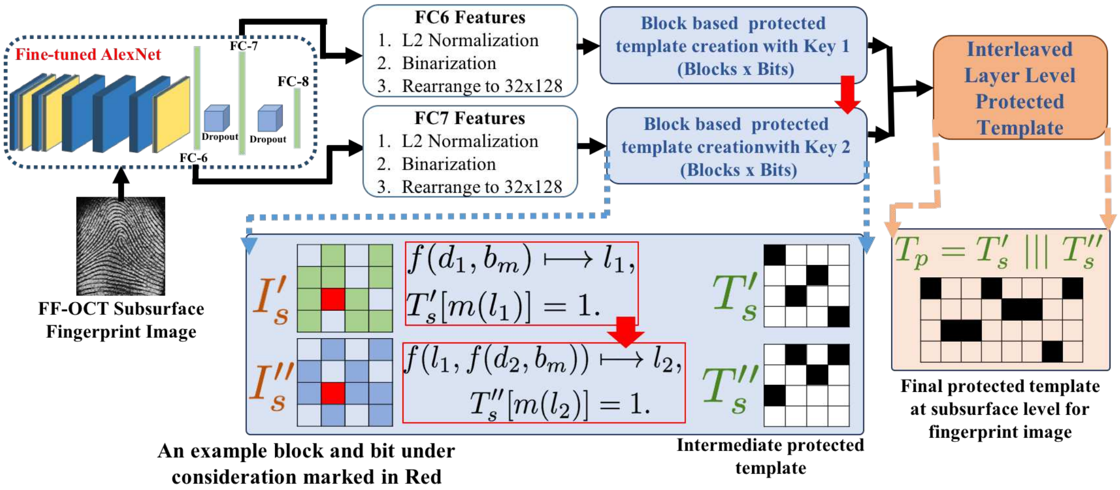
Fine-tuned AlexNet
FC-7
FC-8
Dropout
Dropout
FC-6
FF-OCT Subsurface Fingerprint Image
FC6 Features
1. L2 Normalization
2. Binarization
3. Rearrange to 32x128
FC7 Features
1. L2 Normalization
2. Binarization
3. Rearrange to 32x128
Block based protected template creation with Key 1 (Blocks x Bits)
Block based protected template creationwith Key 2 (Blocks x Bits)
Interleaved Layer Level Protected Template
I'_s
$f(d_1, b_m) \longmapsto l_1,$
$T'_s[m(l_1)] = 1.$
T'_s
I''_s
$f(l_1, f(d_2, b_m)) \longmapsto l_2,$
$T''_s[m(l_2)] = 1.$
T''_s
$T_p = T'_s \; ||| \; T''_s$
An example block and bit under consideration marked in Red
Intermediate protected template
Final protected template at subsurface level for fingerprint image

Figure 3: Core principle of intertwined layer level template protection. The red arrow in the image indicates the interrelation between the features from two different feature set from same subsurface fingerprint.

Further, for each image processed through the fine-tuned AlexNet, we extract the features from fully connected layers $fc6$ and $fc7$ as represented by I_s^{fc6} and I_s^{fc7} for the subsurface fingerprint s. As the features from $fc6$ and $fc7$ amount to 4096 features for each layer and real valued in nature, we apply the $L2$ normalization to center the features with $zero - norm$.

$$I_s^{fc6} = \frac{I_s^{fc6}}{||I_s^{fc6}||}; \qquad I_s^{fc7} = \frac{I_s^{fc7}}{||I_s^{fc7}||}$$

As features from $fc6$ and $fc7$ layers are not equivalent, such normalization across the features from those two layers aids us in retaining the discriminative information even after normalization. Specific choice of $L2$ normalization is to retain the features without any explicit knowledge of feature space and also make the normalization to be non-sparse. An additional motivation stems from the rotation invariance of $L2$ normalization for a given set of features. As the features post-normalization is in the range of $[-1, 1]$, we simply adopt binarization by a hard threshold to transform the features from real-valued domain to binary domain as formulated below:

$$I'_s = \begin{cases} 1, & \text{if } I_s^{fc6} \geq 0 \\ 0, & \text{otherwise} \end{cases} \quad I''_s = \begin{cases} 1, & \text{if } I_s^{fc7} \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

where I'_s and I''_s represent binarized features from $fc6$ and $fc7$ respectively. Given the features are complementary from both $fc6$ and $fc7$, employing the template protection directly will lead to protected binary templates with large collision rates. As a secondary problem, challenges may arise due to linkability of templates across different databases of protected templates as reported in earlier works [16]. In order to account for these two factors, we present a new formulation of protected template creation and also introduce database-specific/application-specific key through a bijective function (XOR) that not only helps in maintaining unlinkability but also provides a means of revokability when the templates are compromised. The specific formulation of our proposed approach can be seen from Figure 3. Given I'_s and I''_s, we first reorganize the features to a matrix of size 32×128 for each of them. The rearranging of features also helps in introducing diffusion and creating a new neighbourhood relation to achieve better

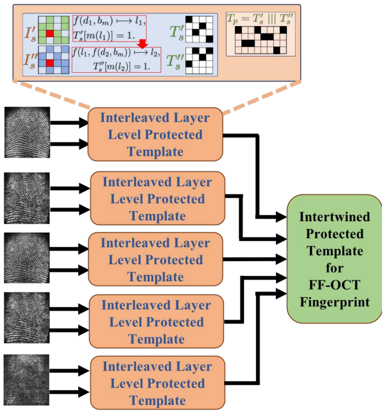
I'_s
$f(d_1, b_m) \longmapsto l_1,$
$T'_s[m(l_1)] = 1.$
T'_s
I''_s
$f(l_1, f(d_2, b_m)) \longmapsto l_2,$
$T''_s[m(l_2)] = 1.$
T''_s
$T_p = T'_s \; ||| \; T''_s$
Interleaved Layer Level Protected Template
Interleaved Layer Level Protected Template
Interleaved Layer Level Protected Template
Interleaved Layer Level Protected Template
Interleaved Layer Level Protected Template
Intertwined Protected Template for FF-OCT Fingerprint

Figure 4: Fully intertwined template protection employing both inter-layer templates and all subsurface images from the FF-OCT fingerprint. The reader is referred to Figure 3 to obtain the details of core principle of layer level template protection.

templates. Further, we divide the rearranged features into number of blocks with a fixed bit size as given by $blocks \times bits$, which is further represented by $L \times B$ for the sake of simplicity. For each chosen block m of a specific bit size b, we create protected templates T'_s and T''_s corresponding to I'_s and I''_s using three following specific steps: (i) create the template by setting the bit of the location (l_1) provide by bijective function (XOR) with the help of database-specific key d_1 for the chosen block m and the bit location b_m of I'_s.

$$\begin{gathered} f(d_1, b_m) \longmapsto l_1, \\ T'_s[m(l_1)] = 1. \end{gathered} \tag{1}$$

(ii) for the corresponding selected block in I''_s, set the bit at location (l_2) using a bijective function and the database-specific key d_2 and the location l_1 computed previously

$$\begin{gathered} f(l_1, f(d_2, b_m)) \longmapsto l_2, \\ T''_s[m(l_2)] = 1. \end{gathered} \tag{2}$$

(iii) in the third step, we introduce another level of diffusion by interleaving the protected templates T'_s and T''_s to derive final layer intertwined protected template T_p for a given subsurface image.

$$T_p = T'_s \interleave T''_s \tag{3}$$

While the above Equation 3 provides a template protection scheme that is suitable for a single layer of the FF-OCT fingerprint, it does not inherently exploit the characteristics of FF-OCT images. Specifically, the number of images obtained from the subsurface stack s is not fully employed to derive a better protected template. Thus, we propose another approach building on the concepts outlined before and employing the stack of subsurface images. Considering the s subsurface fingerprint images and the features from $fc6$ and $fc7$ for each of these subsurface images, it is intuitive to create a multi-bucket intertwined protected template by obtaining the protected template for each layer as provided above. We further consider that different subsurface images of FF-OCT show correlated information leading to correlated protected templates. In order to address this and minimize such a risk, we introduce unique keys for each subsurface such that unlinkability keys total to $d_1, d_2, \ldots d_{2*s}$. It can be further noted that the number of keys can be exactly equal to number of subsurface images such that the key used for T'_s of layer can be used for T'_{s+2} for instance. Thus, for a given set of s subsurface images in the range $s \in \{1, 2, \ldots s\}$, one can derive 5 protected templates $T^f_p \in \{T_{p1}, T_{p2}, \ldots T_{ps}\}$ for a given set of key pair $d_1, d_2, \ldots d_{2*s}$ corresponding to each subsurface image.

$$\begin{gathered} T^f_p = \{T_{p1} \interleave T_{p2} \interleave T_{p3} \interleave T_{p4} \interleave T_{ps}\} \\ \text{using keys } \{d_1, d_2, \ldots d_{2*s}\} \text{ for } s \in \{1, 2, \ldots s\} \end{gathered} \tag{4}$$

However, considering a set of features to be similar across different subsurface images of FF-OCT, this may potentially lead to random guessing attacks, where under the worst possible condition, all the subsurface templates may be compromised. In order to address this limitation, we further propose an intertwined and interleaved layer architecture in the Figure 4. Further, it should be noted from the Figure 3 that the approach is highly configurable both with respect to the number of FF-OCT layers, number of blocks and the number of bits within each block.

$$\begin{gathered} f(l_{n-1}, f(d_n, b_m)) \longmapsto l_b, \\ T''_s[m(l_b)] = 1. \end{gathered} \tag{5}$$

when n is $fc7$ features of a specific layer and m is the block and b is the bit under consideration for a location l within the block m.

3. Database

This section presents the FF-OCT fingerprint image database employed in this work to demonstrate the applicability of the proposed approach. The FF-OCT fingerprint image database [19] consists of images collected from FF-OCT sensor [3] from 200 unique fingers from different subjects. The data consists of fingerprint images from the subjects in the age-group of 20-40 years whose external fingerprints are not deliberately damaged due to manual labour, but consists of abrasions arising out of everyday activity. The database is composed in such a manner that each of the unique finger was captured in two different sessions resulting in a total of 400 images from 200 unique fingerprint instances. Further, each finger was imaged using the FF-OCT sensor which can capture 6 different subsurface images corresponding to 6 layers of depth such as $70\mu m, 140\mu m, 210\mu m, 280\mu m, 350\mu m$ and $420\mu m$. The database in total consists of 2400 finger print images captured using FF-OCT sensor from 200 fingers in 2 different sessions. Figure 1 presents one such sample fingerprint captured at 6 different depth starting from $70\mu m, 140\mu m, 210\mu m, 280\mu m, 350\mu m$ and $420\mu m$ represented by $Layer - 1, Layer - 2, Layer - 3, Layer - 4, Layer - 5$ and $Layer - 6$ respectively. Due to minimal information available in the image corresponding to $420\mu m$ for many subjects (verified experimentally in [19]), we discard this information and employ only the layers $1 - 5$ for the evaluation of proposed template protection scheme.

4. Experiments and Results

In this section, we first present the baseline evaluation of the FF-OCT fingerprint recognition using the deep-CNN network (AlexNet) for all subsurface images and the fused subsurface fingerprint image for each subject. Of the available 200 unique fingerprints, we employ a small subset of images from 10 different subjects for both fine-tuning the CNN and also to configure the parameters of the proposed template protection. Further to compare the baseline results obtained from the fine-tuned CNN, we present the results from the commercial-off-the-shelf (COTS) Neurotech Verifinger SDK [22] which has reported state-of-art results in NIST fingerprint benchmarking. We present the recognition rate through the Equal Error Rates (EER in %) to report the symmetrical error rates with respect to both False Match Rate(FMR) and False Non-Match Rate (FNMR) under the fact that there is no Failure To Capture (FTC).

4.1. Baseline Results

Table 1 presents the results for subsurface fingerprint recognition for layers corresponding to $70\mu m, 140\mu m, 210\mu m, 280\mu m, 350\mu m$. It can be observed that COTS performs with an EER of 2.08% for the subsurface images corresponding to $140\mu m$ while ideal result is seen with fine-tuned AlexNet with CrossEntropy classifier for all subsurface. The ideal results can be attributed to learning mechanism for the set of data. However, as our intention is to use the features from $fc6$ and $fc7$ for template protection, we provide the results just by employing features from fine-tuned AlexNet with a simple Cosine distance measure. As one can anticipate, the results are slightly degraded due to simple distance measure as compared to CrossEntropy based classifier within AlexNet. The results in the Table 1 indicate an EER of 5.69% for combined features from $fc6$ and $fc7$ with cosine distance. Further, we fuse multiple subsurface image features [19, 22] to evaluate the performance and the EER drops to 0% for AlexNet with CrossEntropy. Similar performance can be seen with COTS using the multiple subsurface images in the enrolment [22]. With these results, we proceed further to evaluate the proposed template protection approach by employing the features from $fc6$ and $fc7$ as detailed further.

4.2. Results for template protection scheme

As one of the goals of our proposed template protection approach is also to design an efficient scheme, we aim at binarizing the features such that the templates can be stored in compact binary formats. Thus, we simply threshold the real valued features from $fc6$ and $fc7$ layers using a hard threshold of 0 as explained in Section 2 [1]. Owing the nature of binary features, we adopt a simple Hamming Distance (HD) to measure the similarity of the templates. All the results are further reported using binarized features from $fc6$ and $fc7$ layers using HD measures.

Table 1: Verification performance obtained for layer (subsurface) wise fingerprints images.

Protocol	EER (%)				
	Layer-1	Layer-2	Layer-3	Layer-4	Layer-5
COTS - Layer v/s Layer	2.57	2.08	3.00	2.27	6.24
AlexNet (CrossEntropy) [21]	0	0	0	0	0
AlexNet (Cosine)	5.69	5.69	5.87	5.90	6.95
Fused Subsurface v/s Fused Subsurface COTS [22]	**0.00**				
Fused Subsurface v/s Fused Subsurface AlexNet (CrossEntropy) [21]	**0.00**				

Table 2: Performance of proposed template protection across subsurface fingerprint images.

	Subsurface 1	Subsurface 2	Subsurface 3	Subsurface 4	Subsurface 5
Unprotected	5.69	5.69	5.87	5.90	6.95
Configuration (*Blocks* × *Bits*)	**Protected Templates - Subsurface depth Wise**				
4x4	**5.70**	**6.70**	**6.21**	**6.46**	**8.14**
8x4	6.32	7.31	6.61	8.05	9.70
12x4	6.75	6.86	7.51	8.10	10.35
16x4	7.00	7.17	7.87	7.99	10.18
20x4	10.67	11.66	7.47	13.07	12.69
32x4	26.97	26.76	11.55	26.81	31.36
4x8	**5.86**	**6.62**	**5.39**	**6.91**	**8.81**
8x8	7.06	6.37	6.35	7.66	9.99
12x8	7.88	8.34	8.30	8.94	11.35
16x8	9.67	11.20	10.55	9.72	13.18
20x8	13.53	13.23	10.98	13.04	16.93
32x8	19.07	18.48	13.96	16.84	21.30

Experiments were further performed for evaluation of proposed template protection scheme for subsurface images and also on the fused features. Further to evaluate the robustness of our proposed scheme and estimate the performance across different configurations, we present the results for different configurations in the Table 2. We note the following observations from the Table 2:

- The proposed template protection scheme for subsurface fingerprint image corresponding to $70\mu m$ results in an EER of 5.7% while it increases by 1% for layers 2-4. It can be further noted that EER increases to 8.14%.
- The drop in the performance for subsurface 5 is primarily due to missing fingerprint details

[1] Experimental evaluation did not change over different values of hard threshold for binarization schemes

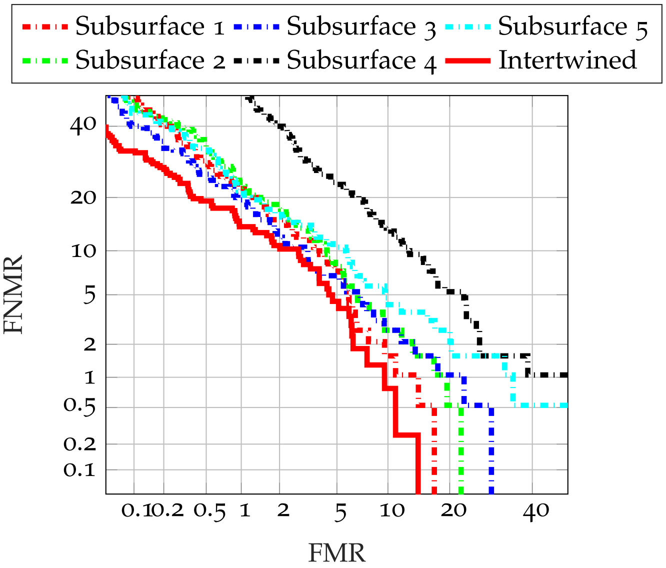

Figure 5: DET Curves for proposed template protection for different subsurface of FF-OCT fingerprint images and final intertwined protected template.

- when compared to other subsurface as it can be noted from Figure 1.
- It can further be noted that the error rates increase linearly with the increase in the size of blocks for the protected template with bit size of 4 indicating a better template protection mechanism under lower block sizes. A large increase can be seen when the block size increase to 32 blocks deeming it not an ideal candidate configuration for the proposed approach. Thus, we do not increase the block size to next level.
- Generalizing the observation, it can be seen that the lower size of blocks yields better accuracy in the protected domain for the task at hand.
- The most important observation is the antagonistic nature of proposed template protection scheme across different subsurface fingerprint images and the scalability of approaches for different bit sizes for smaller block widths.

Table 3: Performance of Intertwined Subsurface Template Protection for FF-OCT Fingerprint. Note - S* represents the unprotected performance for multiple subsurface fingerprints.

Unprotected	S1 - 5.69	S2 - 5.69	S3 - 5.87	S4 - 5.90	S5 - 6.95	
Protected Templates - Intertwined Subsurface Templates						
Configuration	4x4	8x4	12x4	16x4	20x4	32x4
EER (%)	5.09	5.88	5.52	6.00	6.54	19.52
Configuration	4x8	8x8	12x8	16x8	20x8	32x8
EER (%)	5.08	6.00	6.78	7.39	11.75	14.48

Further, similar observations can be made when the templates are fused using the proposed approach as given by Equation 5. As noted from the Table 3, fused templates reduce the error rates as against the subsurface fingerprint based templates alone. Lower error rates can be attributed to fusion of $fc6$ and $fc7$ features from different subsurface fingerprint images and the subsurface fingerprints.

4.3. Limitations and Future Works

Although the proposed approach results in low EER as depicted in the Figure 5, a careful observation indicates that there is potential for improvement in terms of FMR and FNMR. The proposed approach needs to further analyze the strategies for reducing the errors at both the ends of FMR and FNMR which will carried in the future works.

5. Security Analysis - Unlinkability

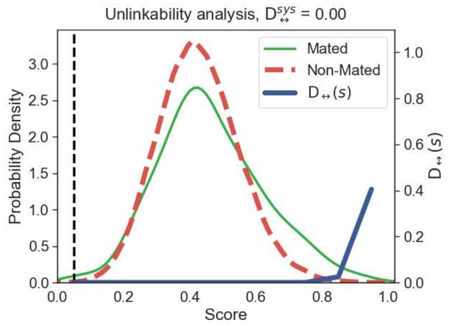

Figure 6: Unlinkability analysis of proposed approach on the configuration of 4 *blocks* × 8 *bits* according to Unlinkability metrics [12].

We conduct the unlinkability analysis through the recently proposed framework [12] to establish the robustness[27] of our proposed approach. As it can be observed from the Figure 6, the proposed template protection scheme results in ideal unlinkability with $D^{sys}_{\leftrightarrow} = 0$[12]. It can be further observed from the Figure 6 that the distribution of mated scores and non-mated scores overlap significantly and this indicates the low chances of guessability attacks exemplifying the antagonistic nature of proposed scheme for threats on protected templates.

6. Conclusion

In this work, we address a new problem to provide template protection scheme for new generation of fingerprint sensors - FF-OCT, which can typically capture multiple subsurface fingerprint images at various depths. While multiple subsurface can provide complementary/supplementary information including partial minutia, ridge and valleys, such information does not result in optimal recognition performance with current state-of-art systems based on minutia alone. In this work, we have proposed to employ deep CNNs to extract complementary features, first to improve the fingerprint recognition, secondly to leverage it for template protection using the subsurface fingerprints and intertwined protected template creation. Through the experimental evaluation, we have demonstrated the effectiveness of proposed approach with $EER = 5.08\%$ with near ideal unlikability ($D_{\leftrightarrow}^{sys} = 0$). In what remains for future works, the strength of minutiae information can be included to improve the proposed template protection scheme to reach ideal biometric performance.

Acknowledgement

This work was partially carried out under the funding of the Research Council of Norway under Grant No. IKTPLUSS 248030/O70.

References

[1] N. Abe, S. Yamada, and T. Shinzaki. Irreversible fingerprint template using minutiae relation code with bloom filter. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–7. IEEE, 2015. 2

[2] E. Auksorius and A. C. Boccara. Fingerprint imaging from the inside of a finger with full-field optical coherence tomography. *Biomedical optics express*, 6(11):4465–4471, 2015. 1, 2

[3] E. Auksorius and A. C. Boccara. Fast subsurface fingerprint imaging with full-field optical coherence tomography system equipped with a silicon camera. *Journal of biomedical optics*, 22(9):096002, 2017. 2, 3, 5

[4] A. Bicz and W. Bicz. Development of ultrasonic finger reader based on ultrasonic holography having sensor area with 80 mm diameter. In *Biometrics Special Interest Group (BIOSIG), 2016 International Conference of the*, pages 1–6. IEEE, 2016. 1

[5] J. Breebaart, B. Yang, I. Buhan-Dulman, and C. Busch. Biometric template protection. *Datenschutz und Datensicherheit-DuD*, 33(5):299–304, 2009. 2

[6] R. Breithaupt, C. Sousedik, and S. Meissner. Full fingerprint scanner using optical coherence tomography. In *Biometrics and Forensics (IWBF), 2015 International Workshop on*, pages 1–6. IEEE, 2015. 2

[7] R. Cappelli, M. Ferrara, and D. Maltoni. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12):2128–2141, 2010. 2

[8] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. Goh. Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion*, 18:161–174, 2014. 2

[9] European Council. Regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). April 2016. 2

[10] M. Ferrara, D. Maltoni, and R. Cappelli. Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, 7(6):1727–1737, 2012. 2

[11] M. Ferrara, D. Maltoni, and R. Cappelli. A two-factor protection scheme for mcc fingerprint templates. In *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–8. IEEE, 2014. 2

[12] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch. General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, 13(6):1406–1420, 2018. 7

[13] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch. Multi-biometric template protection based on bloom filters. *Information Fusion*, 42:37–50, 2018. 2

[14] I. Grulkowski, J. J. Liu, B. Potsaid, V. Jayaraman, A. E. Cable, and J. G. Fujimoto. Ultrahigh speed oct. *Optical Coherence Tomography: Technology and Applications*, pages 319–356, 2015. 2

[15] F. Harms, E. Dalimier, and A. C. Boccara. En-face full-field optical coherence tomography for fast and efficient fingerprints acquisition. In *SPIE Defense+ Security*, pages 90750E–90750E. International Society for Optics and Photonics, 2014. 1

[16] J. Hermans, B. Mennink, and R. Peeters. When a bloom filter is a doom filter: security assessment of a novel iris biometric template protection system. In *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the*, pages 1–6. IEEE, 2014. 4

[17] ISO/IEC JTC1 SC27 Security Techniques. ISO/IEC 24745:2011. information technology - security techniques - biometric information protection, 2011. 2

[18] Z. Jin, M.-H. Lim, A. B. J. Teoh, and B.-M. Goi. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 42:137–147, 2014. 2

[19] Kiran B. Raja, E. Auksorius, R. Raghavendra, A. C. Boccara, and C. Busch. Robust verification with subsurface fingerprint recognition using full field optical coherence tomography. In *Computer Vision and Pattern Recognition Workshops (CVPRW), 2017 IEEE Conference on*, pages 646–654. IEEE, 2017. 2, 3, 5, 6

[20] Kiran B. Raja, R. Raghavendra, S. Venkatesh, M. Gomez-Barrero, C. Rathgeb, and C. Busch. A study of hand-crafted and naturally learned features for fingerprint presentation attack detection. In *Handbook of Biometric Anti-Spoofing*, pages 33–48. Springer, 2019. 1

[21] A. Krizhevsky, I. Sutskever, and G. E. Hinton. Imagenet classification with deep convolutional neural networks. In F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, editors, *Advances in Neural Information Processing Systems 25*, pages 1097–1105. 2012. 3, 6

[22] Neurotechnology. VeriFinger SDK. 2, 6

[23] D.-L. Nguyen, K. Cao, and A. K. Jain. Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge. In *2018 International Conference on Biometrics (ICB)*, pages 9–16. IEEE, 2018. 3

[24] V. M. Patel, N. K. Ratha, and R. Chellappa. Cancelable biometrics: A review. *IEEE Signal Processing Magazine*, 32(5), 2015. 2

[25] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29(4):561–572, 2007. 2

[26] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, 40(3):614–634, 2001. 2

[27] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, and B. Preneel. Criteria towards metrics for benchmarking template protection algorithms. In *2012 5th IAPR International Conference on Biometrics (ICB)*, pages 498–505. IEEE, 2012. 7

[28] C. Sousedik, R. Breithaupt, and C. Busch. Volumetric fingerprint data analysis using optical coherence tomography. In *Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the*, pages 1–6. IEEE, 2013. 1, 2

[29] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, 92(6):948–960, 2004. 2

[30] B. Yang and C. Busch. Parameterized geometric alignment for minutiae-based fingerprint template protection. In *2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, pages 1–6. IEEE, 2009. 2

[31] W. Yang, J. Hu, and S. Wang. A delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement. *IEEE transactions on Information Forensics and Security*, 9(7):1179–1192, 2014. 2

[32] X. Yu, Q. Xiong, Y. Luo, N. Wang, L. Wang, H. L. Tey, and L. Liu. Contrast enhanced subsurface fingerprint detection using high-speed optical coherence tomography. *IEEE Photonics Technology Letters*, 29(1):70–73, 2016. 1

[33] F. Zhang, S. Xin, and J. Feng. Combining global and minutia deep features for partial high-resolution fingerprint matching. *Pattern Recognition Letters*, 2017. 3