論文の内容の要旨

A Study on Optimization of Security and Convenience in Biometric Identification
（ID レス生体認証における安全性と利便性の最適化に関する研究）

氏名　村上　隆夫

Biometric identification, which recognizes an individual based only on physiological or behavioral characteristics, is nowadays used for commercial applications such as computer login, physical access control, and time and attendance management. It has a potential to provide the best authentication solution with regard to security and convenience because it does not require a user ID, password, nor card but recognizes a user based on his/her biometrics (i.e. something you are). In biometric identification, however, the following factors cause problems with security and convenience, and become serious as the number of enrollees increases: (1) false accepts; (2) wolves and lambs who cause false accepts against many others; (3) false rejects; (4) the number of biometric inputs; (5) response time. False accepts, wolves, and lambs are factors which affect security, while false rejects, the number of inputs, and response time are factors which affect convenience. They are related to each other, and have prevented biometric identification from being applied to large-scale applications. The goal of this study is to optimize security and convenience in biometric identification in terms of these factors.

Firstly, we make an attempt to optimize false accepts, false rejects, and the number of inputs. We focus on MSPRT's (Multi-hypothesis Sequential Probability Ratio Tests), multi-hypothesis tests which can minimize the average number of observations, and propose two sequential fusion schemes in identification: the PPSI (Posterior

Probability-based Sequential Identification) scheme and the LRSI (Likelihood Ratio-based Sequential Identification) scheme. The PPSI scheme is based on MSPRT and can minimize the average number of inputs (referred to as ANI), while the LRSI scheme is a simpler one which can be carried out quickly. Then we prove that the LRSI scheme can also minimize ANI by proving that this scheme is equivalent to MSPRT. We also discuss the conditions to achieve the optimality, and show the effectiveness of the two schemes through experimental evaluation using the NIST BSSR1 Set1, a multi-modal score dataset (one face and two fingerprints).

Secondly, we make an attempt to further optimize response time. To this end, we turn our attention to metric space indexing methods which have been developed in the area of similarity search, and focus on pseudo-score based indexing schemes which compute, for each object in the database, a pseudo-score which is easily computed and highly relevant to a score (distance or similarity), and compute scores in order of the pseudo-score. We first propose the PPS (Posterior Probability-based Search) scheme which normalizes each pseudo-score to the posterior probability of being in the answer to the range query. We proved that the PPS scheme has an optimal property with regard to the number of score computations and the expected number of retrieval errors. We also showed that it outperforms the two state-of-the-art schemes: the standard pivot-based indexing scheme and the permutation-based indexing scheme, through experimental evaluation using various kinds of datasets from the Metric Space Library. We then make an attempt to combine metric space indexing and sequential fusion, and propose the PPSS (Posterior Probability-based Sequential Search) scheme, a modification of the PPS scheme to use not only pseudo-scores at the current input but past pseudo-scores and scores as information sources. We also propose a technique which optimizes the number of pivots (biometric templates selected from the database to compute pseudo-scores) with regard to retrieval errors. We demonstrate that our proposals significantly reduce the number of score computations of the PPSI scheme while keeping false accepts, false rejects, and the number of inputs, using a large-scale multi-modal dataset (1800 enrollees; one face and two fingerprints) obtained by combining the NIST BSSR1 Set3 and the CASIA-FingerprintV5.

Finally, we attempt to optimize the trade-off between security against wolves and lambs and convenience in terms of the number of inputs and false rejects. To clarify our target, we first introduce a taxonomy which classifies wolves into three categories (zero-effort wolves, non-adaptive spoofing wolves, and adaptive spoofing wolves) and lambs into two categories (zero-effort lambs and spoofing lambs). Then, we propose the MLRSV (Minimum Likelihood Ratio-based Sequential Verification) scheme as a

sequential fusion scheme in verification. We prove that this scheme has security against wolves and lambs, except for adaptive spoofing wolves, and minimizes ANI and false rejects under some conditions. We also discuss the conditions to achieve the security and optimality, and propose an input order decision scheme based on the KL (Kullback-Leibler) divergence to further reduce ANI in the case where the KL divergence differs from one modality to another. We finally demonstrate the effectiveness of our proposals using a multi-modal (one face and eight fingerprints) dataset obtained by combining the NIST BSSR1 Set3 and the CASIA-FingerprintV5.