at enrollment and authentication, by definition, two-factor authentication is yielded which may increase the security but does not affect the accuracy of biometric authentication.

A significant increase of recognition rates can be caused by unpractical assumptions during performance evaluations. If user-specific transforms are applied to achieve CB these transforms have to be considered compromised during inter-class comparisons. Otherwise biometrics becomes meaningless as the system could rely on secret tokens parameters without any risk [102]. Secret tokens, be it transform parameters, random numbers or any kind of passwords are easily compromised and must not be considered secure [1]. Thus, performance evaluations of approaches to CB have to be performed under the so-called “stolen-token scenario” where each impostor is in possession of valid secret tokens (the same applies to BCSs in case secret tokens are applied). Fig. 13 illustrates how inter-class distances may change with or without considering the stolen-token scenario. If different tokens are applied for each subject a clear separation of intra-class and inter-class distributions is achieved by adopting a new threshold. In contrast, if secret tokens are considered compromised accuracy

2) Revocable Biotokens: Boult et al. [149], [150] proposed cryptographically secure biotokens which they applied to face and fingerprints. In order to enhance security in biometric systems, biotokens, which they refer to as Biotope™, are adopted to existing recognition schemes (e.g. PCA for face).

Operation mode (see Fig. 15): each measured biometric feature $v$ is transformed via scaling and translation resulting in $v' = (v - t) \cdot s$. The key idea is to split $v'$ into a stable part $g$ termed integer and an unstable part $r$. For face biometrics the authors suggest to simply split real feature values into an integer part and a fractional part (e.g. 15.4 is splitted into 15 and 0.4). Since $g$ is considered stable, and a “perfect matching” is claimed to be feasible at authentication, comparisons can be performed in the encrypted domain. A one-way transform of $g$, denoted by $w$ is stored as first part of the secure biometric template. As second part of the template the unencoded $r$ which has been obscured via the transform, as well as $s$ and $t$ are stored. At authentication features are transformed applying $s$ and $t$ onto a residual region defined by $r$. Then the unencrypted $r$ is used to compute the local distance within a “window”, which is referred to as robust distance measure, to provide a perfect match of $w$. However, since a perfect match is required only for a number...