subject are untraceable.

Several other applications for the use of BCSs and CB have been suggested. In [10] biometric ticketing, consumer biometric payment systems and biometric boarding cards are suggested. VoIP packages are encrypted applying biometric keys in [181]. A remote biometric authentication scheme on mobile devices based on biometric keys is proposed in [182] and a framework for an alternative PIN service based on CB is presented in [183]. In [184] helper data-free key-generation is utilized for biometric database hashing. Privacy preserving video surveillance has been proposed in [185].

B. Potential Attacks

Several attacks have been encountered to infiltrate conventional biometric systems [4], [186]. The technologies of BCS introduced in which a subjects and the attackers template are merged into one single template used to authenticate with the system. The Biometric Encryption™ algorithm [20] is highly impacted or even compromised by these attacks. Adler [189] proposed a “hill-climbing” attack against the Biometric Encryption™ algorithm in which a sample biometric input is iteratively modified while the internal comparison score is observed. Nearest impostor attacks [190] in which distinct parts of a large set of biometric templates is combined to obtain high match scores could be applied even more effectively. Keys bound in fuzzy commitment schemes [15] have been found to suffer from low entropy (e.g. 44 bits in [32]) reducing the complexity for brute force attacks [35]. Attacks which utilize the fact that error correction codes underlie distinct structures have been suggested [10], [190]. Attacks based on error correction code histograms have been successfully con-