APPLICATION OF SOFT DECISION DECODING FOR REED SOLOMON CODES IN BIOMETRIC SYSTEMS

B. Assanovich, Ayad Merawiy Abdullah

Error-correcting codes (ECC) are widely used in communication systems, and information security applications, where it is important to ensure access security with noisy input data. In recent years, the non-binary code constructions have attracted the particular interest because of their flexibility high efficiency at low signal-to-noise ratio. In this abstract we propose to use the new error-and-erasure decoding algorithm based on Reed Solomon (RS) symbol reliability. This algorithm applies the Soft Decision Decoding (SDD) technique for RS ECC by the search for the "unreliable" RS symbols calculated as absolute value of the deviation in magnitude relative to its mean for a current biometric measurement. It is an iterative method and can be easily realized with hardware or/and software components with low complexity compared to Hard Decision Decoding (HDD).

The SDD procedure is performed on the basis of the updating the erasure vector, in which the elements are cyclically shifted in case of failure appearance in the HDD algebraic method. The decoding procedure ends when decoding is successful and the message (key R) is found, or after all possible cyclic shifts of the initial erasure vector are completed. Since the positions of the most unreliable symbols will be at the beginning of the vector of indices K, correct decoding is achieved after a few shifts.

We have studied the biometric authentication system (BAS) [1] that uses a known Fuzzy Commitment (FC) scheme and several RS codes constructions and two types of helper data (HD1 and HD2) obtained from the biometric measurements at the enrollment stage. In our experiments we found that the application of a proposed SDD technique for RS code resulted in better efficiency (code rate) of RS code with SDD compared to RS (63,15) and RS (31,9) ECC concatenated with linear code and separately with repetition codes (3,1,1). Several experiments have been carried out to train neural network (stacked autoencoder) for 10 different groups of 40 users each, randomly selected from the UvA-NEMO database. For this compiled dataset the encoding-decoding procedures were modeled using the above-mentioned ECC. For processed 200 subjects from the dataset, the real-valued data with lengths of 63 and 31 elements obtained from SAE and equidistantly quantized have been encoded with non-binary RS codes. We applied the RS code (63,31), which made it possible to expand the cryptographic key to |R|=21*=126 bits in the absence of the 2nd coding stage with efficiency 126/63*6=0.33. The proposed SDD algorithm was used with erasure vector lengths of 21-19 elements. In the following experiments, we also examined the coding of two blocks of RS code (31,17), which made it possible to obtain the total key length |R|=2*17*5=170 bits with an efficiency of 85/170=0.5. The EED decoding was used as in previous experiments with erasure vector lengths of 6-5 elements.

The simulation of BAS has shown the possibility of achieving FRR values of no more than 0.7% and 0.3% for crypto keys of size 170 and 126 bits for biometric feature data dimensions of 63, 31 elements and simplify the overall structure of a biometric system.

References

1. Assanovich B., Kosarava K. Authentication System Based on Biometric Data of Smiling Face from Stacked Autoencoder and Concatenated Reed-Solomon Codes // Communications in Computer and Information Science. 2022. Vol 1562. P. 205–219.