S-RANDOM INTERLEAVER LEADING TO HIGHER MINIMUM DISTANCE FOR TURBO CODES

BY

LUCIAN TRIFINA, VALERIU MUNTEANU and DANIELA TĂRNICERIU

A method to design a small length S-random interleaver is proposed. It is matched to a component code of a turbo code with both trellises terminated, which leads to higher minimum distance. The design is based on the elimination of those bit sequences that can lead to low distances of the code words. A higher minimum distance of the resulted turbo code has as consequence the decrease of the "error-floor" phenomenon, fact that is obvious from the asymptotic curves of the error rates.

SCALING COEFFICIENT DETERMINATION OF EXTRINSIC INFORMATION FROM THE MAX-LOG-MAP DECODING ALGORITHM USED IN DUOBINARY TURBO CODES

BY

LUCIAN TRIFINA, VALERIU MUNTEANU and DANIELA TĂRNICERIU

The Max-Log-MAP (maximum *a posteriori*) decoding algorithm for nonbinary turbo codes is more advantageous than MAP algorithm and even than Log-MAP algorithm, because it has a smaller complexity and it doesn't require channel noise variance estimation. Scaling of extrinsic information with a coefficient smaller than 1 leads to improved performance, but determination of scaling factor is made by repeated simulations. A computing relation of scaling coefficient depending on the mean and the standard deviation of extrinsic information is proposed. This relation removes the disadvantage of repeated time-consuming simulations needing large computing resources.

DATA STRUCTURES DIVERSIFICATION FOR AN IMPROVED EFFICIENCY OF ENCRYPTION TECHNIQUES

BY

LUMINIŢA SCRIPCARIU and PETRUŢ DUMA

The main goal of improving the encryption techniques is to minimize the risk of taking-over the information by any cryptographic attack. Increasing the length of the encryption key and of the input data block represents a limited solution as admitted complexity and processing time of the encryption algorithm. We propose a new design way of encryption space structure, with more dimensions and a random distribution of data on a lot of boxes in order to reduce the correlations between contiguous input data symbols. More than that, an extra combination of data with a white noise sequence could be used as a red herring against cryptanalysis. The proposed method ensures an increased size of the input block, of the encryption key length and smaller chances of any cryptographic attack.