Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 62 (2015) 297 – 302

Procedia Computer Science

The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

Second-Order Spline-Wavelet Robust Code under Non-Uniform Codeword Distribution

Alla Levina[1], Sergey Taranov[1]

[a]*ITMO University, Kronverskiy av. 49, St.Petersburg, 197101, Russia*
[b]*ITMO University, Kronverskiy av. 49, St.Petersburg, 197101, Russia*

Abstract

In computer science, robustness is the ability of a computer system to cope with errors during execution. Robust codes are new nonlinear systematic error detecting codes that provide uniform protection against all errors, whereas classical linear error-detection code detects only a certain class of errors. Therefore, defence by the linear codes can be ineffective in many channels and environments, when error distribution is unknown. The probability of error masking can increase depending on codeword distribution. However, mapping the most probable codewords to a predefined set can reduce the maximum of the error masking distribution.

The algorithm proposed in this paper is based on the second-order wavelet decomposition of B-splines under non-uniform nets. In this paper, we propose a general approach to the algorithm construction of spline-wavelet decompositions of linear space over an arbitrary field. This approach is based on the generalization of calibration relations and functional systems, which are biorthogonal to basic systems of relevant space. The obtained results permit the construction of second-order spline-wavelet robust code.

Peer-review under responsibility of organizing committee of The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)

Keywords: Robust code; spline-wavelet decomposition; non-uniform distribution; Gray mapping

1. Introduction

Modern error injection techniques allow an adversary to attack cryptographic devices by inducing errors of any multiplicity. The errors can be induced into every part of the codeword. One of the most efficient countermeasures against these attacks are error detecting codes. Error detecting codes are widely used for telecommunication channels. They ensure the reliability and security of devices from soft and hard errors, and also side channel attacks. Side channel attacks can be detected with relatively high probability by security-oriented codes. Security-oriented codes are robust and partially robust codes. Currently, the problem of finding new constructions of robust and partially robust codes is actual. Different types of robust codes, partially robust codes, and minimum distance robust codes were offered in [2,3,6,8]. One disadvantage of robust codes is that these codes assume that the information bits are

* Alla Levina. Tel.: +7-911-243-3693. Email address: alla_levina@mail.ru
** Sergey Taranov. Tel.: +7-921-750-3490. Email address: serg.tvc@mail.ru

Peer-review under responsibility of organizing committee of The 2015 International Conference on Soft Computing and Software Engineering (SCSE 2015)
doi:10.1016/j.procs.2015.08.453

uniformly distributed and are not known to an attacker. In practice, however, there are codewords that are much more likely to appear than others.

This article explores the robustness of code, that is derived from second-order spline-wavelet transforms. In this paper we show that using a specific method of net selection and element discarding, the second-order spline-wavelet reconstruction formula can be transformed to a coding function of robust code. The article examines the robustness ability of second-order spline-wavelet code in case of non-uniform codeword distribution. Gray mapping most probable codeword of proposed code to a predefined set can be used to reduce the maximum of the error masking probability.

2. Theory of the spline-wavelet decomposition

Piecewise functions (second-order splines) have been used in mathematics since Euler. Spline theory was developed in the middle of the XX-th century. The term spline was introduced in mathematics by Isaac Schoenberg (1946) and splines were used for theoretical investigations until 1960. Since 1960, however, splines have also been used for computer simulations in science, engineering and techniques. Wavelet is mathematical function used to divide a given function or a continuous-time signal into different components. Experiments of using wavelets decomposition of splines on grids for simulations of information stream are provided [10,11].

Let $\mathbb{Z}$ be the set of all integers. On finite or infinite interval (α,β) of the real axis $\mathbb{R}^1$ consider the net: $X \triangleq \{x_j\}_{j\in\mathbb{Z}}$,

$$X: \quad \ldots < x_{-1} < x_0 < x_1 < \ldots, \tag{1.1}$$

$$\text{for which } \alpha = \lim_{j\to-\infty} x_j,\ \beta = \lim_{j\to+\infty} x_j, \forall j \in \mathbb{Z}. \tag{1.2}$$

(The same result is valid for the finite net, enough to consider the trace of all objects in the interval embedded in (α,β)). Segments $[x_j, x_{j+1}]$ are called elementary net segments of the net X. Denote the linear space of functions that are continuously differentiable in points of the open interval (α,β) as $C^1(\alpha,\beta)$. On the net X, consider polynomial second-order spline ω_j ($j \in \mathbb{Z}$):

$$\omega_j(t) = (t - x_j)^2 (x_{j+1} - x_j)^{-1} (x_{j+2} - x_j)^{-1}, \text{for } t \in [x_j, x_{j+1}); \tag{1.3}$$

$$\omega_j(t) = (x_{j+2} - x_j)^{-1}(x_{j+2} - x_{j+1})^{-1}(x_{j+3} - x_{j+1})^{-1} \times \Big[(x_j - x_{j+2} - x_{j+3} + x_{j+1})\, t^2 - 2(x_{j+1}x_j - x_{j+2}x_{j+3})\, t +$$

$$+ x_j x_{j+1} x_{j+3} - x_j x_{j+2} x_{j+3} + x_j x_{j+1} x_{j+2} - x_{j+1} x_{j+2} x_{j+3}\Big], \text{for } t \in [x_{j+1}, x_{j+2}); \tag{1.4}$$

$$\omega_j(t) = (t - x_{j+3})^2 (x_{j+3} - x_{j+2})^{-1} (x_{j+3} - x_{j+1})^{-1}, \text{for } t \in [x_{j+2}, x_{j+3}], \tag{1.5}$$

$$\omega_j(t) = 0 \quad \text{for } t \notin [x_j, x_{j+3}], \text{so} \ \ \text{supp}\ \omega_j [x_j, x_{j+3}]. \tag{1.6}$$

In the space $C^1(\alpha,\beta)$ we consider the linear functionals $g^{(i)}$, $i \in \mathbb{Z}$ defined by formula

$$\langle g^{(i)}, u\rangle \triangleq u(x_{i+1}) + (x_{i+2} - x_{i+1}) u'(x_{i+1})/2$$

$$\forall u \in C^1(\alpha,\beta). \tag{1.7}$$

For a fixed $k \in \mathbb{Z}$ let

$$\overline{x}_j \triangleq x_j \text{ for } j \le k-1, \ \ \overline{x}_j \triangleq x_{j+1} \text{ for } j \ge k, \quad \xi \triangleq x_k$$

and consider the new net $\overline{X}$: $\ldots < \overline{x}_{-1} < \overline{x}_0 < \overline{x}_1 < \ldots$.

Second-order splines $\overline{\omega}_j$, based on the new net $\overline{X}$, are represented by formulas (1.3) – (1.6) with replacement nodes x_j of the net X on the nodes $\overline{x}_j$ of the net $\overline{X}$. Obviously, for $j \notin \{k-3, k-2, k-1\}$, splines $\overline{\omega}_j$ coincide with splines discussed previously:

$$\overline{\omega}_j(t) \equiv \omega_j(t), \forall j \le k-4; \overline{\omega}_j(t) \equiv \omega_{j+1}(t), \forall j \ge k. \tag{1.8}$$