Chaotic sequences based image encryption

Kirill Trofimov

Institute of Radioelectronics

Riga Technical University

Riga, Latvia

kirils.trofimovs@edu.rtu.lv

Sergej Umnov

Riga, Latvia

sergejs.umnovs@edu.rtu.lv

Abstract— **In this paper we propose an image encryption method based on chaotic sequences produced by a pair of Vilnius oscillators. The solution is provided as a VHDL model and is tested against implementation in Matlab.**

*Index terms—***vilnius oscillator, image encryption, chaos**

I. Introduction

Image encryption is a common process in modern communication and storage systems. It is used to protect confidentiality and integrity of digital images from unauthorized access. Considering the omnipresence of visual data, it's processing takes a considerable amount of compute resources. Chaos-based image encryption supposedly provides a higher data rate and compute efficiency than traditional image encryption methods. In this paper, a simple chaotic system is used[1] as a pseudo-random number generator. A bitstream produced by the generator is then used to diffuse the pixel data of the plain image, resulting in a cipher image. The result of this research is a VHDL model that implements both the Vilnius oscillator and the image encryption process.

II. Methods

Chaotic sequences that are required for encryption are produced using a pair of Vilnius oscillators that produce values x_k and y_k, where k is an index of a sample of oscillator readings. These values are then used to produce a single random bit comparsion, as shown in formula (1).

$$f(x_k, y_k) = \begin{cases} 1 \text{ if } x_k \geq y_k \\ 0 \text{ if } x_k < y_k \end{cases} \quad (1)$$

The PRNG bit is then used to transform
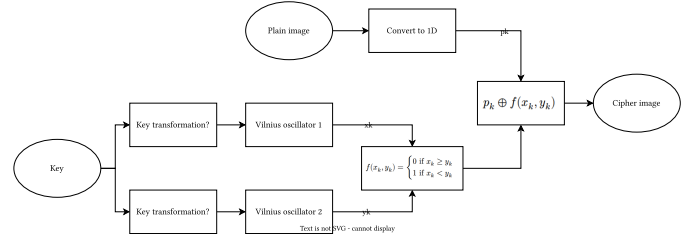
A. Vilnius oscillator

III. Results

IV. Conclusion

References

[1] A. Tamasevicius, G. Mykolaitis, K. Pyragas, and V. Pyragas, "A simple chaotic oscillator for educational purposes", *European Journal of Physics*, vol. 26, pp. 61–63, 2004, doi: 10.1088/0143-0807/26/1/007.