Modified Baptista type cryptosystem via matrix secret key.

ABSTRACT

In 1998, M.S. Baptista proposed a chaotic cryptosystem using the ergodicity property of the simple low-dimensional and chaotic logistic equation. Since then, many cryptosystems based on Baptista's work have been proposed. However, over the years research has shown that this cryptosystem is predictable and vulnerable to attacks and is widely discussed. Among the weaknesses are the non-uniform distribution of ciphertexts and succumbing to the one-time pad attack (a type of chosen plaintext attack). In this Letter, our objective is to modify the chaotic cryptographic scheme proposed previously. We use a matrix secret key such that the cryptosystem would no longer succumb to the one-time pad attack.

Keyword: Chaotic cryptosystems; Ergodicity; Cryptanalysis; Logistic map; Secret key.