Improved digital signature protocol using iterated function systems.

ABSTRACT

In this paper, a novel digital signature protocol is proposed. It is based on the iterated function system attractor, which is regarded as an emerging method. The idea behind our proposed method is based on selecting a known fractal set and then finding the attractor of the affine transformation functions. The attractor is then used in the encryption and decryption of a hash function to ensure the protection of the document from eavesdropping and integrity during the transmission. The properties and software implementation of the proposed protocol are discussed in detail. A comparison is made with the Rivest, Shamir, and Adleman cryptosystems, which shows that it performs better.

Keyword: Cryptography; Digital signature; Iterated Function Systems (IFS); Fractal; Attractor; Hutchinson operator W.