

Abstract

Nel presente lavoro viene mostrato un sistema per realizzare un codice crittografico, che sia utilizzabile per garantire un alto livello di segretezza usando tecniche di Information Fusion (IF). Nel dettaglio, si è deciso di fondere due codici; uno generato tramite un algoritmo di crittografia a chiave pubblica e uno creato mediante l'utilizzo di formule matematiche innovative basate sui frattali.

La tecnica di Information Fusion utilizzata è stata presentata in precedenza con un differente utilizzo ed opportune modifiche. Infatti, nel precedente lavoro, veniva creato un codice di accesso identificativo, mentre, in questo, viene generata una chiave crittografica fortemente casuale da utilizzare in ambito di cifratura.

La scelta di utilizzare i frattali per generare una sequenza numerica da fondere con codici utilizzati nella cifratura a chiave pubblica è vincolata alla caratteristica randomica di tali strutture. Questo porta all'idea di utilizzare queste caratteristiche per applicazioni crittografiche quali One-Time-Pad. La tecnica di fusione modificata è denominato F&NIF (Fractal & Numerical Information Fusion).