جمهورية العراق
وزارة التعليم العالي والبحث العلمي
الجامعة المستنصرية
كلية التربية

نظام فوضوي مبتكر في تشفير الصورة

أطروحة
مقدمة الى كلية التربية في الجامعة المستنصرية
وهي جزء من متطلبات نيل درجة دكتوراه فلسفة في
علوم الرياضيات

من قبل

صادق عبدالعزيز مهدي

بأشراف

أ. م. د. عبد علي حمودي و أ.م .د. سالم علي عباس

١٤٣٧هـ ٢٠١٦م

المستخلص

هذه الاطروحة تقدم نموذج رياضي ليمثل نظام تشفير لا خطي فوضوي مبتكر ذات عشرة أبعاد ويحتوي على عشرة ثنائيات لا خطية وكذلك يحتوي احد عشر معلمة حقيقية موجبة ، تم التحقق من السلوكيات الديناميكية الفوضوية عن طريق تحليل النظام المبتكر . حيث قمنا بتحليل النظام المبتكر من خلال صور الطور او الحالة ، نقاط التوازن ، التبدد ، التماثل والثبات ، حساب قوى لابنوف ، البعد الكسوري ، الشكل الموجي ، والحساسية للشروط الابتدائية ، وتأثير المعلمات على النظام الفوضوي المبتكر، الرسم التخطيطي للتشعب ، والجواذب للنظام المبتكر ، ان المحاكاة العددية تمت باستخدام برنامج الـ MATEMATICA من اجل توضيح صور الطور والخصائص الاخرى للنظام الفوضوي المبتكر. ومن تحليل النتائج ، تبين بان النظام المبتكر **غير مستقر** ، ويمتلك **ستة** قوى لابنوف موجبة ، والذي يعني ان النظام يمكن ان ندعي بانه نظام سوبر شديد الفوضى ، بالإضافة الى ذلك تم الحصول على بُعد لابنوف للنظام الفوضوي المبتكر والذي قيمته يساوي 9.97191 وهو ما يعني ان بُعد لابنوف من النظم الكسورية . ومن الشكل الموجي للنظام الفوضوي المبتكر تبين بانه لا دوري ولديه حساسية عالية للشروط الابتدائية .

ونظراً للعلاقة الوثيقة بين الفوضى والتشفير يمكن استخدام نظام التشفير الفوضوي المبتكر المقترح في تشفير وفك شفرة جميع انواع متعدد الوسائط ومنها النصوص ، الصور ، الرسوم ، والصوت ، والفيديو . تم اقتراح خوارزمية جديدة لتشفير الصورة الملونة من خلال الجمع بين انتشار قيم مواقع الصورة والمفاتيح التي تولدت من النظام الفوضوي المبتكر. وقد تم تحليل أداء الخوارزمية من خلال اجراء التحليلات الإحصائية والتحليلات التفاضلية مثل : تحليل المدرج التكراري ، وتحليل معامل الارتباط، وتحليل انتروبية المعلومات ، تحليل مساحة المفتاح، تحليل حساسية المفتاح، تحليل ذروة نسبة الإشارة إلى الضوضاء (PSNR) ، تحليل معدل تغيير عدد النقاط الصورية (NPCR) ، تحليل معدل التغيير الموحد للكثافة اللونية (UACI) .

وأظهرت النتائج أن الخوارزمية لديها اداء جيد للتشفير و**ذات امنية عالية جداً** نظراً لحجم مساحة المفتاح الذي يمكن ان يصل الى $2^{970} \approx 10^{294}$ وهو ما يعني كبير جداً ، وان الخوارزمية ذات حساسية عالية لإجراء تغييرات صغيرة في المفتاح والذي يجعل الخوارزمية في مأمن من هجمات القوة الوحشية ، وبالتالي فإن حجم مساحة المفتاح كبير بما فيه الكفاية لمقاومة العديد من أساليب الهجوم الإحصائية. بالإضافة الى ان الخوارزمية **ذات سرعة عالية جداً** في التشفير وفك التشفير . تم استخدام برنامج الـ MatlabR2010a لتنفيذ الخوارزمية واجراء التحليلات.