CONVITE À COMUNIDADE

A Coordenação do Programa de Pós-Graduação em Engenharia Elétrica UFSJ/CEFET-MG tem o prazer de convidar toda a comunidade para a sessão pública de apresentação e defesa da dissertação "CRIPTOGRAFIA DE IMAGENS BASEADA EM EXTENSÕES INTERVALARES NATURAIS E NO ERRO DE PRECISÃO FINITA".

MESTRANDO: LUCAS GIOVANI NARDO

BANCA EXAMINADORA:

Prof. Dr. Erivelton Geraldo Nepomuceno – UFSJ (Orientador)

Prof. Dr. Janier Arias García – UFMG (Coorientador)

Prof. Dr. Eduardo Nunes Gonçalves – CEFET-MG

Prof. Dr. Bruno Henrique Groenner Barbosa – UFLA

LOCAL: Sala 3.16 do Prédio do DEPEL, Campus Santo Antônio - UFSJ

DATA: 09 de dezembro de 2019 – segunda-feira

HORÁRIO: 13h30

Resumo do trabalho:

É inerente à natureza humana manter o controle sobre o acesso à informação. Por esse motivo, a busca por um processo de criptografia eficiente e seguro é de suma relevância. A criptografia de imagens é um tópico muito importante nessa área, uma vez que as imagens podem mostrar diversas informações, como os objetos em uma cena, a aparência de uma pessoa, o local, as especificações técnicas de projetos, dentre outras. Vários artigos usam sistemas caóticos para criptografar imagens, no entanto, recentemente, pesquisas têm mostrado que alguns algoritmos de criptografia de imagens são facilmente violados, e, até mesmo, não passam em testes estatísticos quando são esperados valores rigorosos. Uma justificativa para tal problema é a degradação de sistemas caóticos devido à precisão numérica finita dos computadores digitais. Com relação a essa limitação, esta dissertação formula dois processos de codificação de imagens, explorando a precisão numérica finita presente em computadores; bem como utilizando extensões intervalares naturais de sistemas caóticos. Tais extensões intervalares são matematicamente equivalentes, porém são distintas do ponto de vista computacional. Dessa maneira, esse aspecto é utilizado para produzir uma sequência criptográfica baseada no limite inferior do erro, o qual apresenta propriedades pseudo-aleatórias satisfatórias. Os autores adotaram, ora o sistema contínuo do circuito de Chua como sistema caótico, ora um sistema discreto com múltiplas perturbações no mapa logístico. Como resultado, as sequências criptográficas geradas passaram nos testes do NIST. Além disso, várias imagens de referência foram efetivamente criptografadas, mostrando-se seguras contra vários ataques. Por fim, mostrou-se, também, que os algoritmos possuem complexidade da ordem de $O(n^2)$.

Palavras-chave: Encriptação de imagem; Extensão intervalar natural; Limite inferior do erro; Circuito de Chua; Mapa logístico; Caos; Computação Aritmética.