

Grayscale Digital Stego w/ Modified Arnold Transformations

Matthew Seaworth, Sean Soderman, Dylan Soderman

July 1, 2014

1 Project Description

We are using a modified Arnold's Transform(AT) to permute the spatial coordinants of the bitplanes in the message images before embedding in order to increase entropy of the least significant bits(LSB) in the coresponding steganography images. The hiding technique is simply LSB substitution relying on the scrambled images difficulty to unscramble and the natuarally chaotic resultant information. The project will consist of a scrambler, periodic computer, embbeder, extractor, and unscrambler.

2 General Approach

The original Arnold's Transform matrix is changed to include the values i and i plus one as the entries in the first row. Then several of these matrixes are applied to the image for a number of times in a particular order known only by the sender and reciever. This requires a transfer of private keys beforehand to user the correct AT matrices and the correct number of rotations. The period of the AT of an arbitrarily sized matrix can be given by the least common multiple of the period of the independent factors of the side length (N). A set of numbers are independent factors of another number if their multiple equals that number and they share a greatest common divisor of one. Furthermore, the period of the power of a prime number can be computed by multiplying the period of the prime number by a power of the prime number which has the exponent of one less than the original number; however, the period of the original prime number for an arbitrarily modified AT must be computed through brute force, but this substantially reduces the computation time of nonprimes.

The program must take inputs of a cover image, secret data formatted to be a single bit plane in the same size as the cover image, a duple list in text form containing AT offsets as well as the number of times to apply that specific AT. These inputs will result in a stego image being created. The program may also take the inputs of a stego image and the text list of duples to extract and order the LSB plane containing the correct stego image. This program only plans to cover gray images currently. If computation of the periods proves to be too time consuming the program will contain a thrid part which just computes the periods and will subsequently append them to the duple to allow expedient extraction. Nevertheless, the ultimate goal of this project is to produce a working product with little perceptibility, high usage, and security. It should be noted that this method is not lossless and results in minute distortion of the data making it a poor choice for information requiring high fidelity.

References

- [1] Minati Mishra, Ashanta Ranjan Routray, and Sunit Kumar: *"High Security Image Steganography with Modified Arnold's Cat Map"* International Journal of Computer Applications, pp. 16-20, Vol. 37, January 2012.
- [2] Li Bing, Xu Jia-wei: *Period of Arnold transformation and its application in image scrambling* Journal of South Central University of Technology, pp. 278-282, Vol. 12, October 2005.