An Asymmetric Elliptic Curve Algorithm to Increase Entropy and Decrease Computation Time of Iris Recognition

Vishnubhatla, Sasank

The objective of this research was to implement an iris recognition system with a self-developed elliptic curve algorithm or hash. It was hypothesized that if this elliptic curve hash could be created, then it must have a greater entropy or smaller computation time compared to the standard MD5 and SHA-1 hashes. To test the hypothesis, the iris recognition system was written in Python with the OpenCV library. This iris recognition system is faster than standard systems because the extraction of the iris was done on a grayscale image, not a red green blue (RGB) image. The elliptic curve hash was created to increase the entropy and decrease computation time of iris recognition. To test the elliptic curve hash, iris recognition system, and the hypothesis, images from the UBIRIS database were run through the system, and their hashes were collected. The computation times and the entropies were also noted. Then four, one-tailed T-Tests were run to compare the elliptic curve hash to the standard hashes. The analysis shows that the elliptic curve hash is more entropic and quicker than the other hashes at an alpha of 0.01. Thus, the hypothesis is supported because both criterion were upheld.

Awards Won: