A simple flexible cryptosystem for meshed 3D objects and images

Manal A. Mizher, Riza Sulaimana, Ayman M. Abdallab, Manar A. Mizher

In cryptography, the previous research generally appears ambiguous and complex to the novice researcher due to the use of complex mathematical equations and rules of cryptography. Moreover, many research approaches lack flexibility in their key length or in their level of encryption. Consequently, combining simplicity, flexibility, and reliability is not easily obtainable in a cryptosystem, especially for larger and more complex data items. Therefore, a new system, called Flexible cryptosystem based on Cellular Automata (FcCA), is proposed here as a novel simplified flexible cryptosystem based on cellular automata (CA). FcCA presents simplified techniques for making CA reversible while creating a robust flexible cryptosystem that performs lossless encryption of three-dimensional (3D) objects and images of different types. It uses pure random CA as a diffusion technique, and it employs a modified existing confusion technique by substituting the static start point with proposed multi-dynamic intersected start points. In addition, FcCA novelty includes using a combination of aspects: random configuration with open boundary conditions, g-th order memory independent-cell technique, and classification of two parts of the encryption key into subkeys. The length and complexity of FcCA subkeys can be controlled easily because the subkeys depend on flexible parameters. Testing and validation of FcCA scrambling level were performed with several criteria including correlation, entropy, peak signal to noise ratio, and value difference degree. Experimental results showed that FcCA has high flexibility, a high level of scrambling, and higher robustness of keys compared to other methods of encryption. In addition, sensitivity analysis showed FcCA to be highly sensitive to changes in the encryption key and encrypted images and objects. Overall, the properties of FcCA demonstrated its effectiveness as a cryptosystem for images and 3D objects.

Mizher, Manal A., Sulaimana, Riza, Abdallab, Ayman M., Mizher, Manar A., (2019), A simple flexible cryptosystem for meshed 3D objects and images, Journal of King Saud University - Computer and Information Sciences.