Abstract

Study of Cellular Automata (CA) as a modeling tool has received considerable attention in recent years. This thesis uses the concepts of GF$(2^p)$ CA theory to develop applications in authentication and watermarking. A cellular structure called Single Attractor Cellular Automata ($SACA$) is analytically characterized in this regard. Some special features of $SACA$ have given rise to a special hash function which leads to the construction of an one-way hash function. This one-way hash function has been employed to model $CA$ based authenticator ($CAA$). $CAA$ has been used to develop message authentication scheme and its efficiency has also been measured.

Watermarking for image authentication and copyright protection is another application area where the use of this $CAA$ has been explored. The $CA$ based authentication algorithm for message forms the base of the watermarking schemes proposed. We have developed a fragile watermarking scheme exclusively for image authentication and two $CAA$ based semi-fragile watermarking schemes for image authentication as well as copyright protection. One of the semi-fragile schemes is resistant to JPEG lossy compression while the other is resistant to JPEG2000 lossy compression. Superiority of the schemes over existing ones are shown through extensive experiments.