International Journal of Rough Sets and Data Analysis
Volume 3 • Issue 1 • January-March 2016

Chaotic Map for Securing Digital Content:
A Progressive Visual Cryptography Approach

Dhiraj Pandey, JSS Aacdemy of Technical Education, Noida, India
U. S. Rawat, Manipal University Jaipur, Jaipur, India

ABSTRACT

Progressive Visual Cryptography (PVC) is quite suitable for sharing sensitive digital data.Previous research on PVC, such as Fang et al. (2006) and W.P.Fang et al.(2008) were all carrying pixel-expansion problem and also gives a poor visual quality on the recovered stacked image. Recently, Hou&Quan (2011) have developed a progressive scheme for secret sharing. It is observed that shares generated by the scheme are free from pixel expansion problem, but shares are not fully secure. In this paper, a new progressive sharing algorithm based on logistic chaotic map has been proposed to overcome the said limitation of Hou (2011) scheme. The irregular outputs of the logistic map are used to encode a secret digital information carrying image. The performance of the algorithm in the scheme of Hou (2011) is critically analyzed and compared with new suggested scheme. Empirical results are presented to showcase the performance of the authors' proposed scheme in terms of its effectiveness (imperceptibility and security) and feasibility.

KEYWORDS

Digital Secret Sharing, Logistic Map, Progressive Visual Cryptography, Unexpanded Shares, Visual Cryptography

INTRODUCTION

Research into the making digital content secure has been steadily growing. Conventional security techniques take more computational time and space, compared to visual cryptography based approach of securing data. A large number of visual cryptography techniques have appeared in the literature. These techniques can be divided into two main classes: traditional visual cryptography (TVC) and the progressive visual cryptography (PVC). The traditional approach has been widely studied by many researchers and suggested variants of strategy for protecting the content. Cheating detection and prevention has been suggested by many researchers for traditional schemes (Chen&Horng, 2012;Liu&Lin, 2011; Tsai *et al.*, 2007). A common drawback of using the TVC based technique is the loss of contrast and pixel expansion problem. One may overcome issues of TVC, using PVC based approaches. The concept emerged as Progressive Visual Cryptography has been explored by

DOI: 10.4018/IJRSDA.2016010102

many researchers. This topic has gained a wide and equal attention from academician, researchers, and software developers. A computational framework for digital implementation of dynamic visual cryptography based on chaotic oscillations is presented by many researchers (Petrauskiene *et al.*, 2014), but an effective experimental implementation of a chaotic progressive visual cryptography remains an open question in the literature. A chaotic response can be generated by applying periodic force to a nonlinear system.

The main objective of this paper is to investigate the security nature of existing progressive schemes along with the feasibility of using a chaotic map for improving security in shares of PVC.

A chaotic sequence based PVC technique has been proposed here that uses 1-D chaotic map. This paper is organized as follows: Brief review of various visual cryptography based schemes and its utility for digital content security has been described in the next section. Comment about Hou&Quan (2011) scheme has been analyzed in section of critical analysis. The design of their scheme would not disclose any secret information on shares if L is distributed uniformly, but on some critical chosen value of L between 1 to n, scheme caused the severe security problem. A detailed description of the proposed algorithm is given in the section of the proposed algorithm. Experimental results showcasing performance and security of the proposed algorithm are presented in the next section. Different similarity measures (PSNR, MSSIM) have been considered to evaluate the performance. Comparison with existing PVC based schemes along with detailed performance comparison with respect to Hou&Quan (2011) are presented in comparison section. Some concluding remarks along with future directions are given in the last section of the article.

REVIEW OF TRADITIONAL AND PROGRESSIVE VISUAL CRYPTOGRAPHY SCHEMES

In this section, a detailed review has been presented in related research of visual cryptography and their schemes for digital content security.

Traditional VCS Scheme

A new cryptographic paradigm was designed based on the pixel level operation (Naor& Shamir,1995). They termed this visual cryptography and introduced it as a method for encrypting images. In the (2, 2) VC scheme secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed on transparencies. Stacking the two shares does decryption and the secret image can be seen by the naked eyes without any complex cryptographic computations. As suggested in the scheme, if a pixel in the original image was black, the sub pixel in the superimposition of the two shares will be fully black. Similarly, if a pixel in the original image was white, the sub-pixel in the superimposition of the two shares will be black and white. However, because the pixels are small and situated very close together, the human eye averages the relative contributions of the black and white pixels, resulting in a gray pixel. Neither of the shares generated, reveals any information about the original image, but when both are stacked, a representation of the original image can be seen. Visual cryptography scheme using random number has been suggested to apply the visual cryptography scheme for color images (Kandar *et al.,* (2011). Watermarking algorithm to improve the security of secret has also been suggested (Rawat& Raman, 2012; Ross&Othman, 2011). Several algorithms to perform computation on medical imaging techniques (Dey *et al.,* 2012; Dey *et al.,* 2013; Dey *et al.,* 2014) and its security issues (Dey *et al.,* 2012; Araki *et al.,* 2014; Araki *et al.,* 2012; Roy *et al.,* 2012) have been proposed by researchers.