Intelligent Automation and Soft Computing, Vol. 16, No. 3, pp. 433-447, 2010
Copyright © 2010, TSI® Press
Printed in the USA. All rights reserved

A PERVASIVE SECRET SHARING SCHEME FOR EMBEDDED VISUAL COMMUNICATION SYSTEM

CHUL-UNG LEE[1], HYOUNG JOONG KIM[1], JONG HYUK PARK[2], SANG-SOO YEO[3], AND JAESOO YANG[4]

[1]*Korea University*
Seoul 136-701, Korea
{leecu, khj-}@korea.ac.kr

[2]*Department of Computer Science and Engineering,*
Seoul National University of Technology, Korea
parkjonghyuk1@hotmail.com

[3]*Mokwon University*
Daejon 302-318, Korea
ssyeo@mokwon.ac.kr

[4]*Kwangwoon University*
Seoul 139-701, Korea
jaesooyang@gg.go.kr

ABSTRACT—A simple secret sharing scheme for secure visual communications is presented in this paper. Secret sharing schemes allow a group of participants at different locations to share a secret (i.e., an image) among them by splitting it into n pieces ("shares" or "shadows"). In case of the (k, n) secret sharing scheme only a group of k qualified participants among n (where $k \leq n$) can reconstruct the secret. This paper presents an (n, n) secret sharing scheme. This scheme randomizes one share after another by executing XOR operations with random seeds derived from an initial seed. This scheme can also be used as an image encryption scheme. This scheme is resistant to collusion attacks.