Abstract

Visual cryptography encodes a secret binary image (SI) keen on share of unsystematic binary sample. If the share is xeroxed against transparencies, the key figure is often visually decrypted by means that of superimposing a skilled subset of transparencies, however no secret data is obtained from the superposition of a forbidden subset. The binary model of the N allocates, although, contain no visual consequence and hinder the objectives of visual cryptography. The perfect security condition of VC scheme needs the strict demand where any t-1 or fewer transparencies cannot extract much knowledge regarding the key. The secret image is at the same time embedded into color halftone shares. Visual cryptography (VC) could be a secret sharing method of decay a secret picture into n transparencies, and consequently the stack of any t out of n transparencies disclose the key content. A HVC generate procedure is projected that can make an option for secret halftone image into color half-tone shares. In [1], authors centre of attention how to securely distribute video contents to an assured collection of persons for the period of a testing time period in cloud-based multimedia systems, and propose a cryptographic come within reach of, a provably secure time domain attribute-based access
control (TAAC) scheme, to secure the cloud-based video content sharing.

References

20. C.C. Wu, L.H. Chen, “A Study on Visual Cryptography” National Chiao Tung University,
Taiwan, R.O.C., 1998.

Index Terms

Computer Science
Control Systems

Keywords

Cloud computing, multimedia, time-domain, TAAC (time-domain attribute-based access control), content video sharing.