{tag}

Authors:

B. Padhmavathi

P. Nirmal Kumar

M. A. Dorai Rangaswamy

{bibtex}pxc3876571.bib{/bibtex}

Abstract

The growing possibilities of modern communications require a special means of confidential and intellectual property protection against unauthorized access and use. Cryptography provides important tools for the protection of information and they are used in many aspects of computer security. This paper makes use of encrypted secret sharing to increases the security level of hidden data and to provide Mutual Authentication of the users. The visual cryptography scheme is a perfect secure method that encrypts a secret image by breaking it into shadow images. A distinctive property of visual cryptography scheme is that one can visually, without computation, decode the secret by superimposing shadow images. The property of visual secret sharing in reversible style provides more security. This method not only can fast decode without causing pixel expansion but also increase the secret-hiding ratio. Random-Grid Algorithm is used to create secret shares without pixel expansion. This paper extends the capabilities of the Visual Cryptography as a mere secret sharing technique to a Novel Mutual Authentication provider. If one stacks two transparencies(shares) together straightforwardly, a secret image will appear. Stacking two transparencies after reversing one of the transparencies, another secret image will unveil. An attempt is made to provide two transparency three-way mutual authentication by

using Visual cryptography in the reversible style.

References

M. Naor and A. Shamir, .Visual Cryptography,. Advances in Cryptography -EUROCRYPT'94, Lecture Notes in Computer Science 950, 1995, pp. 1-12.

- H.Yan, Z. Gan, and K. Chen, "A cheater detectable visual cryptography   scheme," (in Chinese) J. Shanghai Jiaotong Univ., vol. 38, no.1, 2004.

- G.-B. Horng, T.-G. Chen, and D.-S. Tsai, "Cheating in visual   cryptography , " Designs, Codes, Cryptog., vol. 38, no. 2, pp. 219–236, 2006.

- M.A.Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images," International Journal of Computer Science and Network Security (IJCSNS), Vol. 9 , No. 4, pp. 71-78, 2009.

- A.Dorairangaswamy,B.Padhmavathi,'An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images, Proceedings IEEE Conference. TENCON 2009,Vol 1.

- B.Padhmavathi,M.A.Dorairangaswamy,P.Nirmal Kumar, 'A Robust Blind & Invisible Watermarking Scheme for Share Authentication in Visual Cryptography to prevent Cheating Attacks',Proc Intnl Conf ICISA 2010 Chennai,India.

- Wen-Pinn Fang,"Non-expansion Visual Secret Sharing in Reversible Style", IJCSNS, VOL.9 No.2, February 2009

- Wen-Pinn Fang, "Visual Cryptography in reversible style,"IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26?2007, 11, 28.

- Wen-Pinn Fang and Ja-Chen Lin, "Visual Cryptography with Extra Ability of Hiding Confidential Data" Journal of Electronic Imaging, 15, 2006, 4.

- O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, Vol. 12, No. 6,   pp. 377 - 379, 1987.

- S. J. Shyu, "Image encryption by random grids," Pattern Recognition, Vol. 40, Issue 3, pp. 1014 - 1031, 2007.

- Shamir, Visual cryptanalysis, Proceedings of the Eurocrypt 98, Espoo, 1998, pp.201-210.

- M. Naor, A. Shamir, Improving the contrast via the cover base, in M.Lomas (Ed.), Visual Cryptography II, presented at Security in Communication Networks, Amale, Italy, Sept.1996.

Index Terms

Computer Science   Security

Keywords

Visual Cryptography in Reversible style   Pixel Expansion   Random Grid Algorithm   Secret transparencies

Share Stacking