Paper ID: 13161003

Emperor International Journal of Finance and Management Research [EIJFMR] ISSN: 2395-5929

IMPLEMENTATION OF VISUAL CRYPTOGRAPHY FOR BIOMETRIC IMAGE WITH HASHING AND STEGANOGRAPHY FOR SECURED AUTHENTICATION

EIJFMR
Oct-5th 2016
www.eijfmr.com

Mrs.K. BANUPRIYA
Department of Computer Science and Engineering,
Adhi College of Engineering and Technology,Chennai
Mrs. T.SHERIN
Department of Computer Science and Engineering,
Adhi College of Engineering and Technology,Chennai

Received :8th September 2016
Accepted :29th September 2016
Published : 5th October 2016
Reviewer : Dr.B.Narayana Babu

Abstract

Visual cryptography schemes suffer from the drawback of large pixel expansion of share images and bad visual quality of the recovered image. To provide secrecy, we go for pixel expansion and increasing number of shares, this causes the bad visual quality of the recovered image. In this paper, we construct (n, n)-VCS and OR and XOR operations are used for share creation and stacking process, which proves better in contrast and pixel expansion. The proposed method uses additional matrix to increase the secrecy of the message in XOR operation. The use of visual cryptography is explored to preserve the privacy of an image by decomposing the original image into two shares (known as sheets) that are stored in separate database servers (one with user and one with server) such that the original image can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image. Once the original image is revealed to the user it can be used as the password.

Introduction

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, fingerprints, iris, gait, and voice. A biometric authentication system operates by acquiring raw biometric data from a subject (e.g., face image) extracting a feature set from the data and comparing the feature set against the templates stored in a database in order to identify the subject.

The template of a person in the database is generated during enrollment and is often stored along with the original raw data. This has heightened the need to accord privacy to the subject by adequately protecting the contents of the database. For protecting the privacy of an individual enrolled in a biometric database. To proposed storing a transformed biometric template instead of the original private template or a cancelable biometric.