Chapter 10

Diophantine Equations for Enhanced Security in Watermarking Scheme for Image Authentication

Padma T
Sona College of Technology, India

Jayashree Nair
AIMS Institutes, India

ABSTRACT

Hard mathematical problems having no polynomial time algorithms to determine a solution are seemly in design of secure cryptosystems. The proposed watermarking system used number theoretic concepts of the hard higher order Diophantine equations for image content authentication scheme with three major phases such as 1) Formation of Diophantine equation; 2) Generation and embedding of dual Watermarks; and 3) Image content authentication and verification of integrity. Quality of the watermarked images, robustness to compression and security are bench-marked with two peer schemes which used dual watermarks.

INTRODUCTION

The past two decades have witnessed revolutionary advancements in the areas of technology and communication. The availability of cheap technological solutions has initiated and nurtured newer avenues in business, entertainment and collaboration, where digital multimedia represents a primary source of communication due to its huge expressive capability. The advancements have also facilitated the efficient storage and proliferation of digital multimedia and along with it issues like data vulnerability and fraud. The rampant availability of digital media processing tools has made copying and manipulation of multimedia an easy task.

DOI: 10.4018/978-1-5225-2053-5.ch010
This vulnerability has necessitated the need for inherent mechanisms in multimedia applications to ensure 1) trust worthiness of the media - to prove ownership, protect copyright and to certify the integrity of the media for assurance that the received media is from an authorized source and is identical to the original one and 2) security during the storage and transmission. Any act or attempt of modification on the digital medium is called an attack and security mechanisms are the methods intended to prevent, detect or recover from a security attack.

Authentication is the act of ensuring trust worthiness of digital media and watermarking is a preferred technique used to implement it. Security of a watermark based authentication scheme lies in the complexity and randomness involved in the watermark generation and embedding process. This is to prevent or make it complex for an adversary to detect, read, remove or tamper with the watermark or watermarked image. Mathematical problems that are hard to solve like RSA, Diffie-Hellman key exchange scheme, El-Gamal and Elliptic curve cryptosystems (ECC) have always been favorites in the design of secure cryptosystems where a polynomial time algorithm does not exist as on date to determine whether there is a solution to the problem or not. Number theory based approaches have been used in literature to generate secret keys and pseudorandom sequences but they involve the use of very large seeds with hundreds of digits. Managing and sharing large keys between the communicating parties is complex and leads to its compromise. They are seldom adopted due to the nature of complex computations and time involved.

Diophantine equation is an algebraic equation relating integer quantities. They are expressed usually in two or more unknowns such that only integer solutions are sought or allowed. Solvability of higher order Diophantine equations is a hard problem and is considered a prospective candidate in the design of secure cryptosystems.

The objective is this study is to design a secure, hierarchical, blind and content based image authentication scheme in the Discrete Wavelet Transform (DWT) domain. Diophantine equations that are hard to solve or those with large number of unknown variables are used as the building block in ensuring security of the scheme. Compression, exposure to channel noise and security being important concerns during the regular storage and transmission of images, the proposed scheme is designed to be robust to common incidental noise and fragile to malicious manipulations especially common attacks like collusion, counterfeiting, cut/copy paste and brute force attacks.

**IMAGE AUTHENTICATION**

According to Cox and Miller (2002), digital image authentication is the act of verifying the integrity and authenticity (or credibility) of digital images, i.e. to check if the image has undergone any tampering since its creation. Judging the authenticity of an image is hard, if not impossible, and a judgement cannot be made unless it passes certain tests of integrity and authentication confirmation. An image authentication system is expected to detect manipulations, localize it and to some extent recover the manipulated or altered regions. Measures are needed to ensure that the image is protected against illegal tampering and manipulations. Authentication mechanisms do not protect the image from being stolen or copied.

Image authentication techniques, in general, consist of a stamping stage and a verification stage. During the stamping stage, an authentication code like an external logo or a watermark generated from the image is incorporated with the image. During the verification stage, the authentication code extracted from the query image and the authentication code generated from the query image or original watermarked image are correlated to judge the authenticity of the image. Watermarking techniques have been proposed in