J. Vis. Commun. Image R. 40 (2016) 1–13

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher quaternion chaining ☆

Bartosz Czaplewski

Gdansk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Teleinformation Networks, Gabriela Narutowicza 11/12, 80-233 Gdansk, Poland

ARTICLE INFO

Article history:
Received 28 January 2016
Revised 4 June 2016
Accepted 13 June 2016
Available online 15 June 2016

Keywords:
Fingerprinting
Quaternions
Joint fingerprinting and decryption
Collusion attack
Traitor tracing

ABSTRACT

This paper addresses the problem of unauthorized redistribution of multimedia content by malicious users (pirates). In this method three color channels of the image are considered a 3D space and each component of the image is represented as a point in this 3D space. The distribution side uses a symmetric cipher to encrypt perceptually essential components of the image with the encryption key and then sends the encrypted data via multicast transmission to all users. The encryption involves rotation, and translation of points in 3D color space using quaternion algebra. Each user has a unique decryption key which is different from the encryption key. The differences between the common encryption key and the individual user's decryption key cause the decrypted image to contain minor changes which are user's fingerprint. A computer-based simulation was conducted to examine the method's robustness against noise, compression, and collusion attacks.

1. Introduction

Today we are witnessing the constant threat of unauthorized redistribution of multimedia, i.e. piracy, which causes financial and moral losses to the authors and distributors of multimedia content. This paper addresses the problem of piracy in the context of multimedia distribution services, e.g. video-on-demand services, video streaming. This paper presents a new method of protecting multimedia against piracy. The proposed method is a new joint fingerprinting and decryption method for color images which is used as a tool for pirate tracing.

There are two ways to protect distributed multimedia: encryption and digital fingerprinting [1]. The goal of encryption is to ensure that only subscribed users with proper decryption keys are able to use distributed multimedia. However, after decryption the data loses its protection and may be illegally redistributed by malicious users, i.e. pirates. In order to maintain security after decryption it is necessary to use a digital fingerprint, which is a tool to trace pirates. Digital fingerprinting is a data hiding technique in which data is protected by unique sequences, called fingerprints. Each fingerprint identifies an individual user and is embedded in the image in such a way that it remains invisible to the human eye or at least does not bother the user. Fingerprints can be embedded in the spatial domain [2,3] or in the transform domain, e.g., in the discrete cosine transform (DCT) domain [2,4–6] or in the wavelet transform domain [7]. If the pirate redistributes his or her copy, an analysis of the embedded fingerprint should allow to identify that pirate.

It should be assumed that pirates will perform attacks intended to remove fingerprints from their copies or disable existed fingerprints in order to safely distribute a pirate copy. Thus, embedded fingerprints must be robust against the removal performed by a single pirate or a group of pirates, i.e. so-called collusion attacks [8–10]. In collusion attacks each pirate owns a fingerprinted copy and they combine them to generate a pirated copy with a heavily damaged fingerprint that cripples pirate tracing.

Fingerprinting methods can be divided into three groups depending on the place where the fingerprints are embedded. The most basic approach is transmitter-side fingerprinting [11,12]. In this concept fingerprints are embedded on the transmitted side and then copies are encrypted and sent to the users *via* multiple unicast transmissions. The second approach is in-network fingerprinting [13]. In this concept fingerprints are embedded as the data travels through the network by using special network devices that embed their own watermarks in the transmitted data. Finally, the last approach is receiver-side fingerprinting. In this concept fingerprints are embedded on the receiver side while the transmitter sends only one encrypted copy *via* multicast transmission. The most promising receiver-side fingerprinting

☆ This paper has been recommended for acceptance by M.T. Sun.
E-mail address: bartosz.czaplewski@eti.pg.gda.pl

http://dx.doi.org/10.1016/j.jvcir.2016.06.006
1047-3203/

methods belong to the group called Joint Fingerprinting and Decryption (JFD) [4,14–17].

JFD methods combine encryption and fingerprinting by introducing an unusual feature – fingerprinting performed during decryption. The distribution side encrypts multimedia by using the encryption key and then sends the encrypted data *via* multicast transmission. Each user has a unique decryption key which is different from the encryption key and which allows to decrypt the data in order to obtain multimedia with some minor changes. These changes are imperceptible to the human eye and are unique for each user, hence they are the user's fingerprint. The only operation to be performed on the distribution side is encryption. Moreover, data is encrypted only once, regardless of the number of users. At the same time the only operation performed on the receiving side is decryption, which also introduces a fingerprint into the data at the same time. Most importantly, there is only one copy of the data that is sent over the network, which thus leads to a minimum demand for bandwidth. The above properties make JFD methods highly scalable.

Note that in JFD methods the priority is to trace a pirate (or pirates) by fingerprinting, which is also the focus of this paper. The purpose of the cipher in JFD methods is to take advantage of multicast transmission rather than to provide a high security level. Typically, JFD methods provide low security level, i.e. the image is encrypted by obscuring the most important elements of the image in such a way that the content of the encrypted image is partially visible, but the quality degradation is so significant that an unauthorized user is not able to comfortably watch the protected content.

This paper presents the first quaternion-based joint fingerprinting and decryption method for color images. This method was previously briefly stated in [18] and now, in this article, the method is fully presented and an extensive simulation results are discussed. In this method three color channels (or one luminance channel and two chrominance channels) of the image are considered a 3D space and each component of the image is represented as a point in this 3D space. The encryption involves rotation and translation of these points in 3D color space. Lessons learned from the field of computer graphics show that quaternions are most suitable to describe rotations in 3D space. Due this fact, it was decided that quaternion calculus will be the main tool used in the proposed JFD method. The distribution side uses a symmetric cipher to encrypt perceptually essential components of the image with the encryption key, which is common for all the users, and then sends the encrypted data *via* multicast transmission to all users. Each user has a unique decryption key which is different from the encryption key. The differences between the common encryption key and the individual user's decryption key cause the decrypted image to contain minor changes which are imperceptible to the human eye and are unique across all users. Therefore these changes are the user's fingerprint. Embedded fingerprints are spread over the entire image. Furthermore, the proposed method inherits high scalability from the general principle of JFD.

In the proposed method fingerprints are embedded in the DCT domain. The method uses the well-known fact that it is possible to increase robustness by embedding fingerprints in perceptually essential components of the image without sacrificing overall image quality after a return to the spatial domain [11,19]. By embedding fingerprints only in perceptually essential components, i.e. low-frequency components, the method is robust to compression as compression damages only the perceptually unessential, high-frequency components of the image. Robustness against compression has been verified in the experiments we conducted. Consequently, low-pass filtering, scaling, and shrinking of the image should have a small impact on embedded fingerprints since such processing also damages only the unessential high-frequency components of the image.

However, a much greater threat than compression or noise addition are collusion attacks. In collusion attacks, a group of pirates analyze their fingerprinted copies and together generate a pirate copy with a highly damaged fingerprint. Experiments performed for the proposed method verified robustness against collusion attacks and collusion attacks combined with compression. Since collusion attacks are the greatest threat to digital fingerprinting, these attacks were the main focus of the presented experiments.

The structure of the paper is as follows. The background and the contribution were presented in Section 1. Related work significant to the development of the proposed method is listed in Section 2. Section 3 provides a brief introduction to quaternion algebra. Section 4 describes the proposed JFD method based on quaternion rotation. The experimental results of pirate tracing in the presence of various attacks are presented in Section 5. The conclusions are discussed in Section 6.

2. Related work

The first method using the JFD approach was the Chameleon [14], which was implemented by Anderson and Manifavas for audio data. The Chameleon is a stream cipher based on lookup tables. In this method the decryption changes only the least significant bits of protected data, so the embedded fingerprint does no perceptual degradation. However, embedded fingerprints are very vulnerable to collusion attacks. The Chameleon can trace pirates with high probability only if the number of pirates is up to 4.

Another method, designed by Kundur and Karthik [4], was based on scrambling image DCT coefficients. In this method the low-frequency DCT coefficients are divided into subsets and their signs are reversed depending on the key. The receiver has a unique key that can decrypt only a portion of the subsets. The remaining subsets remain encrypted and their combination is the user's fingerprint. Unfortunately, the embedded fingerprints are visible, which can reduce image quality to an unacceptable level. Moreover, the method has a very limited robustness against collusion attacks [4].

Adelsbach et al. [15] designed the Fingercasting scheme. This is a generalization of the Chameleon cipher that embeds spread-spectrum watermarks into audio-visual content. The main difference is that the lookup table entries are uniformly distributed, randomly chosen elements and that the XOR operation is replaced by a modular addition. Katzenbeisser et al. [20] improved the Fingercasting method by applying a collusion-resistant code as proposed by Tardos [21]. The main drawback of this method is the size of the lookup table and a trade-off between security and the length of the fingerprints.

Another DCT-based method, although not a JFD method, was Li et al.'s fingerprinting with blind detection [22]. In this method, anti-collusion codes are used as fingerprints and the selected DCT coefficients of the image are quantized according to the fingerprints. The unique feature of this method is blind detection, i.e. the fingerprints can be extracted without the original image, which is not common among fingerprinting methods.

Recently, several JFD methods based on vector quantization (VQ) have been proposed [23–26]. The first method [23] encrypts images *via* permutation and codeword substitution by using static key-trees. The second method [24] uses dynamic key-trees in order to replace permutation. Fingerprinting is done based on a set of pre-designed key-trees that are unique for each user. The security of Lin et al.'s method [23] has been verified and enhanced in Li et al.'s paper [25]. The concept of a JFD method utilizing VQ was developed further in a recent paper [26] which proposes a JFD method based on side match vector quantization (SMVQ).