Multi-Keyed Hierarchical Image Authentication

Kenta WATANABE, Masaaki FUJIYOSHI, and Hitoshi KIYA
Tokyo Metropolitan University, Hino, Tokyo 191–0065, Japan
E-mail: watanabe-kenta2@sd.tmu.ac.jp, mfujiyoshi@m.ieice.org, kiya@sd.tmu.ac.jp Tel: +81–42–585–8454

Abstract—This paper proposes a hierarchical image authentication method with multiple keys. The proposed method reversibly hides a keyed hash value of an image block to the block. The method gets multiple keys from one managed key by a hash chain, and different keys are for different hierarchical layers. The proposed method is resistant to key leakage.

I. INTRODUCTION

Image authentication methods have been studied to verify the integrity of images. The key-based hierarchical image authentication method [1] based on the reversible data hiding scheme [2] reduces encryptions to one and serves efficient tamper localization by utilizing the hierarchical structure, but its vulnerability to key leakage. This paper proposes a reversible image authentication method using hash chain-based multiple keys and a keyed hash function. The proposed method is resistant to key leakage and discards an encryption.

II. CONVENTIONAL METHOD

The conventional efficient method [1] reversibly hides a hash value of an image block to the block by the algorithm based on the reversible data hiding scheme [2], in which lower layer consists of smaller blocks and the top layer is the image itself as shown in Fig. 1. Thanks to this layered structure, this method needs to encrypt a hash value only in the top layer and it omits tamper detection in lower blocks of an upper genuine block. Though this method is efficient, it is vulnerable to key leakage as well as ordinary key-based authentication methods.

III. PROPOSED METHOD

The proposed method generates L keys from only one managed key by a hash chain, and different keys are for different layers in a hierarchical embedding of the hash value of an image block to the block by the algorithm based on the reversible data hiding scheme [2], in which lower layer consists of smaller blocks and the top layer is the image itself as shown in Fig. 1. Thanks to this layered structure, this method needs to encrypt a hash value only in the top layer and it omits tamper detection in lower blocks of an upper genuine block. Though this method is efficient, it is vulnerable to key leakage as well as ordinary key-based authentication methods.

IV. EXPERIMENTAL RESULTS

Figure 3 shows tamper detection and localization results by the proposed method. Due to the hierarchical embedding, the proposed method localizes tampered areas in a coarse-to-fine manner (Fig. 3 (a)) as well as the conventional method [1]. The proposed method detects tampering in the second layer even the image is determined to be genuine in the top layer.

V. CONCLUSIONS

This paper has proposed a hierarchical image authentication with multiple keys generated through a hash chain. A keyed hash value of an image is reversibly hidden to the image in the hierarchical layered manner in which different keys are for different layers. These features makes the proposed method resistant to key leakage.

REFERENCES