Volume : 4 | Issue : 3 | Mar 2015 ISSN - 2250-1991

Research Paper Technology

An Improved Cryptographic Method in Watermark Encoding

Marius Rogobete | Alstom GRID, Software Development, Bucharest, Romania

Ciprian Racuciu | Titu Maiorescu University, Science and Information Technology, Bucharest, Romania

ABSTRACT

The actual cryptographic process used to encode/decode hide watermarking message is using a classical flowchart, based on a private cryptographic key applied, together with the watermarking message, on a cryptographic algorithm. The encoded message resulted is embed into DCT's coefficients, for JPEG format or into pixel's LSB, for bitmap format.
The new proposed method computes two keys from the primary, private key.
In addition, the watermarking message is dividing in two sub-messages, and every sub-message is encode with a particular key and a different encoder.
Every encoded message is write in different coefficients (one into coefficients with odd indexes, and the second into coefficients with even indexes).
In this way, the robustness against force attack is increasing significant, and the invisible watermark becomes more efficient on the host image protection.

KEYWORDS | hide watermarking; watermark encoder; watermark decoder; cryptographic private key.

INTRODUCTION

The copyright protection and authenticity (content verification) are concepts of major importance in multimedia. For example, a watermarking message is hiding in an image for protection. In this way, it is possible to check the hide message, in order to authenticate the image or to verify the image integrity.

A potential deterrent of malicious modifications or even duplications of digital images seem very difficult in the current multimedia. In the classical watermark embedding, the watermarking message is encrypted using a cryptographic algorithm and a private key. Then, the encrypted message is embedded into image. The authorized user can decrypt the message extracted from image and then, can test the image integrity. A necessary condition for successfully decryption is the possession of the associated key because the verification procedure is based on public algorithms and public key..

The encryption break prevention is depended on the key length; if the key is longer, the prevention is better. For such a method, the prevention method could be the most significant weakness as once the message is extracted from the host image and the decoder is identified, it is directly vulnerable to piracy.

General Presentation

The watermarking methods are related to steganography methods, which hides messages within other data for secret communication. The methods are identical but the proposed targets are different: the watermarks protect the host data while steganograms protect the message hidden it in host data.

Regarding to the image, the invisible digital watermarks are defined as small alteration of the image data. There are two watermarking schemes.

Watermarking with private key for copyright protection, when each provider posses a unique private key, used together with a public or private algorithm to produce the watermark image, that is distributed to customers; the provider can examine the images for the watermark existence, using a public key, the detection algorithm and his private key.

Watermarking with public key for content verification, where the described process has an additional pubic key associated to the private key, which can demonstrate the watermark existence without disclosing the private key.

The reason to use two types of keys is that private key aims to protect the provider and public key aim to protect the customer.

This approach improves the cryptographic schema using two private keys derivated from primary private key and subsequently two cryptographic algorithms. The process is completed with the watermark embedding into image, when the coefficients of alteration are different.

Cryptographic schema description

The new cryptographic schema integrated into watermarking framework is reliable, extremely effective against malevolent attacks, and not affect the perceived data quality.

The perceptual similarity is recovered by the capability of a software detector to distinguish the watermarks. However, different keys should not produce similar watermarks and using two private keys instead the primary private key will create different watermark.

Based on this assumption we have developed a new method that read the primary private key and split it in two keys (fig. 1), if at least one word of the primary key is found in hardcoded keywords list kept by the watermarking framework.

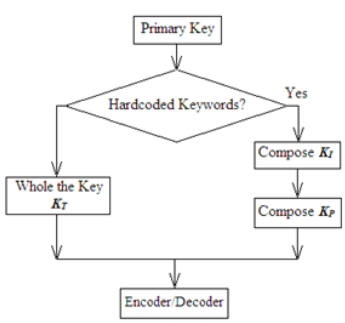

Fig. 1 Composing derivate keys from primary key

If the primary key is split, then the watermarking message is divided in two substrings of length approximately equal (rounded the word), fig. 2.

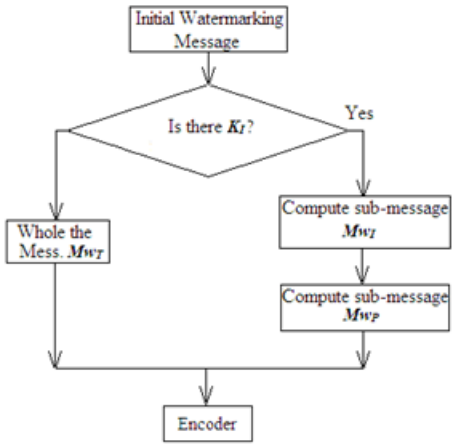

Fig. 2 Formatting sub-strings from main message

Therefore, the watermarking framework will encrypt every watermark sub-string, using assigned key and cryptographic algorithm (encoder), fig. 3. The encrypted watermarks are then embedded into image's AC of DCT coefficients, for JPEG format, or bitmap's pixels

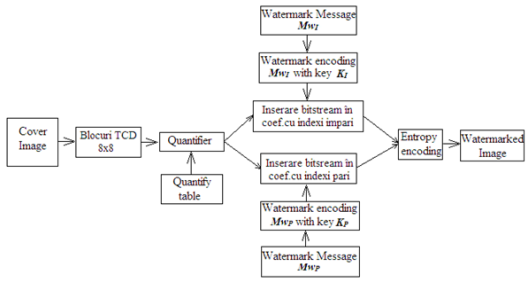

Fig. 3 The encryption process using two cryptographic keys (JPEG format).

The watermarking extraction (fig.4) could be performed if and only if the interested user is in the posses of the both cryptographic keys and both decoders. More of this, the rule to extract the encrypted message from image should be known.

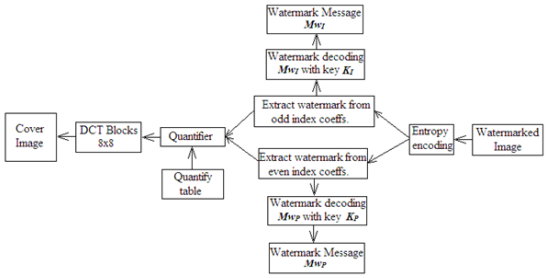

Fig. 4 The decryption process using two cryptographic keys (JPEG format).

In this way the weakness of classical method is eliminate and the framework prevents better the encryption break.

Conclusions

In practice, the existence of watermarking in an image is indicated with a degree of certainty. This degree depends of the detector D that is characterized, usually, by a small probability of error. The errors produced by detector are false positive or false negatives.

For the presented method, the detector errors are increasing substantially, no one of the used detectors being not able to extract the correct embedded sub-messages.

From the decryption point of view, the decoder framework that attack the hide watermark needs at least $n!*(n-1)^2$ more time of execution.

Finally, the presented method increases significant the robustness for watermarking embedding against force attack. The protection against attack on decryption is also improved using double private keys and two cryptographic algorithms.

REFERENCES

[1] Ciprian Răcuciu – Criptografia şi securitatea informaţiei, Editura Renaissance, Bucureşti, 2000 | [2] Ciprian Răcuciu, Dan Laurenţiu Grecu – Metode şi sisteme criptografice secvenţiale, Editura Ericom, Bucureşti, 2008 | [3] 29. Sun, Q., Ye, S., Lin, C.-Y., Chang, S.-F.: A crypto signature scheme for image authentication over wireless channel. International Journal of Image and Graphics 5 (2005) 1–14 | [4] Wee, S., Apostolopoulos, J.: Secure scalable streaming enabling transcoding without decryption. In: Proceedings of the IEEE International Conference on Image Processing. Volume 1. (2001) 437–440 | [5] Katzenbeisser, S.: On the integration of watermarks and cryptography. In: Proceedings of the 2nd InternationalWorkshop on DigitalWatermarking. Volume 2939 of Lecture Notes in Computer Science. (2003) 50–60 | [6] 21. Lin, E., Delp, E.: Temporal synchronization in video watermarking. IEEE Transactions on Signal Processing, Supplement on Secure Media 52 (2004) 3007–3022 | [7] Harmancı, O., Kucukgoz, M., Mıhcak, K.: Temporal synchronization of watermarked video using image hashing. In: Security, Steganography and Watermarking of Multimedia Contents VII. Volume 5681 of Proceedings of SPIE. (2005) 370–380 | [8] M Rogobete, C Răcuciu, E. Rădoi "Original Methodology and Algorithm able to Identify Visible Noisy in Image and Video Stream", International Conference for Education and Creativity, 7th Edition, Bucharest, 2013 | [9] M Rogobete, C Răcuciu, "First and second order image statistics in specific image artifact detection", International Conference on Innovative Technologies, IN-TECH 2012 | [10] M Rogobete, C Răcuciu, "Using Potential Field Analysis into Image Artifact Detection Field", Indian Journal of Research, May, 2014 | [11] Cristian-Gabriel Apostol, Marius Rogobete, Dorin Marian Pîrloagă, Ciprian Răcuciu – Using the chaos theory and dynamic keys in digitalwatermarking, The International Conference NAV-MAR-EDU 2013, Constanţa 2013,Romania