Authenticity of digital images

Lucjan Hanzlik, Wojciech Wodo

Faculty of Fundamental Problems of Technology,
Wroclaw University of Technology,
Wybrzeze Wyspianskiego 27, 50-370 Wroclaw, POLAND,
E-mail: [first_name].[last_name]@pwr.wroc.pl

Abstract – Copyrights are a big issue these days, it is extremely easy to loose our intellectual property (in sense of digital images) and thus money, moreover it is hard to proof our rights in the court. Our digital pictures must be protected in such a manner that it should be easy to proof we are the legitimate owner of the image and it should be computationally hard to forge such proof. We present a sketch of a new solution for copyright protection of digital images using chameleon hash functions, signatures and steganography. It is an extension of previous work in this field. We introduce a probabilistic similarity method into our scheme, which convince the verifier at certain level about the owner of the picture.

Key words – steganogrphy, images, information hiding, chameleon hash, signatures, security, copyrights

I. Introduction

Nowadays almost every data could be found in the internet including pictures and videos. Users get used to publishing their own photography and use other people resources, but the copyrights issue is often omitted. In case of quoting somebody's work even without indicating the source we could let go the matter, but when it comes to commercial usage of these goods then the problem occurs. How to proof the ownership of the rights to the particular digital image? There are well known watermarks techniques (compare [1], [2], [3]) allowing to embedded additional data within the canvas of image, sound or video file. These methods use mostly steganographic algorithms like F5 [4] or jSteg [5] for embedding the information. But the question remains: it is that sufficient?

Author in the paper [6] sums up current usage of watermarks and steganography in sense of protecting images and propose new scheme for this purpose. In this work we extent that scheme by adding new features and security properties.

II. Chameleon Hash

One of the main assumptions for electronic signatures is that it is almost impossible to assign other message to the particular signature. We can use hash functions to sign a message, they have such a property that it is difficult to find a collision – i.e. for given x (calculated as $x = H(m_1)$) is hard to determine value of m_2 such that $x = H(m_2)$. There is however, such a family of hash functions with a special property. For those hash functions it is sufficient to know the secret s to find the collision in a easy way. They are called *chameleon hash functions*. Belowe we present example implementation of such functions based on the discrete logarithm problem. Let g be generator of a certain cyclic group, let m be the message for which we want to calculate hash function, let s be the secret for the given hash function and let g^s be the public key of this hash function. Further, to compute the hash function we pick r at random and calculate:

$$H_{gs}(m,r) = g^m \cdot (g^s)^r = h \qquad (1)$$

Having values for (m, r, h) everybody can verify that h is the value of the hash function (H_{gs}) for message m.

From the definition of hash functions it is hard to calculate tuple (m_2, r_2, h) (for the same h). However knowing s one can perform the following steps in order to calculate this tuple.

It is easy to see, that h will be the same in both cases if $m + s \cdot r == m_2 + s \cdot r_2$. Thus it is sufficient to calculate $r_2 = (m - m_2 + s \cdot r)/s$.

III. Picture Protections Algorithm

In this section we present the algorithms used to protect the copyright of pictures and how to proof ownership of it.

Actors:

First, we will define the actors in the system. We will distinguish three actors, namely:

- *TA* – trusted authority with a public set of keys, its job is to generate some cryptographic material for a given picture, that can be used to proof ownership of that picture,
- *U* – user, owner of the photography, sends the picture to the *TA*, to receive the cryptographic material, uses this material to proof ownership against a verifier,
- *V* – verifier, buyer or publisher of the photography, verifies the cryptographic material given by the owner of the photography.

Desired properties:

It is desired that picture protection system has the following properties:

- verifier is able to check the validity of the ownership without communication with *TA*,
- user is able to modyfy the picture slighty (e.g. tone and color correction) in such a way it is possible for a recognition procedure to link the original one with modified version,
- it is possible to present a undeniable proof for copyrights (e.g. in court)
- the whole procedure has to be quick and simple for a user, it means that obtaining cryptographic data should take only *one button click*

Proposal:

Let us assume that *U* on his way home meets a well-known actress in a untypical situation and apparently by an accident took the snapshot. The photography is worth huge amount of money and of course for that reason *U*, who wants to protect it send it for signing to *TA (*with public key g^x). Additionally, *U* picks at random secret s and sends g^s to *TA* as well. *TA* receives the photography, minimizes it to size of 128x128 pixels and signs (using key x) the following message (minimized photo $\| g^s$)

receiving signature s_1. Moreover *TA* signs the original photography with hash function H_{gs} receiving signatures s_2. Independently, to that there is a third signature s_3 under the original photography and a time stamp of receiving of the photography. After that *TA* sends to *U* (s_1, s_2 (and *r* value for hash function), s_3, minimized photo). User embeds signature s_3 within the original photography receiving a stegano photography. Next, U is looking for a collision for stegano photo in signatures s_2 receiving random value r_2. Now user *U* wants to sell photo to verifier *V*. *U* pass to *V* the stegano photo and signatures s_1, s_2, r_2, g^s and the minimized photo. Verifier compares minimized photo with the received stegano picture. If similarity of images is lower than 50%, the verifier aborts. Otherwise verifier checks s_1 (at the same time checks that g^s is assigned for this stegano photo). Subsequently V checks signature s_2 using hash function H_{gs}. In case, when a other potential owner of the photo appears, the process of identification of the real author takes place in court. Using the signature s_3 one can undoubtedly point the real owner of the photo.

Picture Edition and Picture Recovery:

The usage of cameleon hash functions allows to add two new features to picture copyright protection in comparison to the solution from [6]. The first feature allows to edit the original photography (i.e. crop, resize etc.) and recompute the *TA-s* signature s_2 such that the verification for the new picture will pass. Note that the edited photo must yield a similarity at least 50% in comparison to the minimized picture embeded in signature s_1. Now imagine that someone publishes a edited picture on the web. The second feature allows the legitimate owner to recover (i.e. regain the ownerships) the picture simply by recomputing the *TA-s* signature s_2. Note that both features rely on cameleon hash functions. The owner of the picture can, using the secret for public key g^s from signature s_1, find a collision for the new picture (which includes the signature s_3 embeded using steganography) such that the signature s_2 will be valid for the new picture.

Future Work:

The future work involves a implementation of the system. We are currently designing an application for smart phones, which makes it possible to instantly get a signature under a just taken photo. In addition, the designed application will be universal in the sense that user can specify the *TA* by its choice. This will give the application more reliance, since the user must not depend on a specific authority but can choose from numerous trusted and standard certificate authorities. Moreover, it will be platform independet.

Conclusion

In this paper we have proposed a new approach for protection of digital images and photography published on the web. Our goal was to design a scheme that allows to prove our rights to the image file immediately without necessity of revealing the original picture and without the communication with a trusted authority. The image processing and comparing algorithm provides us some certainty level of honesty, which is suitable for vast majority purposes.

A quite wide field of application for this and similar solutions are electronic documents like identity cards or passports, where the authenticity of the photography of the e-ID holder is a very important issue. Moreover, such an approach allows us to personalize the picture every time when we need to verify our identity.

References

[1] A. Kumar and Km. Pooja, “Steganography - A Data Hiding Technique”, International Journal of Computer Applications (0975 – 8887),Vol. 9– No.7, November 2010.

[2] N. V. Dharwadkar and B. B. Amberker, “Reversible Steganographic Scheme with High Embedding Capacity using Dual Cover Images”, SECRYPT 2012, pp.15-24, July 2012.

[3] P. Dong, J. G. Brankov, N. P. Galatsanos,Y. Yang and F. Davoine, “Digital Watermarking Robust to Geometric Distortions”, IEEE Transactions on Image Processing, Vol. 14, No. 12, December 2005.

[4] A. Westfeld, “F5-A Steganographic Algorithm High Capacity Despite Better Steganalysis”, IH 2001, LNCS 2137, pp. 289–302, 2001.

[5] D. Upham, “Steganographic algorithm Jsteg” [online]. Available: http:// zooid.org/paul/crypto/jsteg 1993.

[6] W. Wodo, “Autentycznosc fotografii i obrazow cyfrowych”, Interdyscyplinaronosc badan naukowych 2013, pp.446-449, June 2013.