ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 *2008. No. 6(86)*
ELEKTRONIKA IR ELEKTROTECHNIKA

ELECTRONICS
T170
ELEKTRONIKA

Digital Signature Approach for Image Authentication

R. Bausys, A. Kriukovas
Department of Graphical systems, Vilnius Gediminas Technical University,
Saulėtekio al.11, Vilnius, Lithuania; phone: +370 5 2744848; email: romas@fm.vgtu.lt

Introduction

Images in digital representation are widely used in our normal life nowadays. With rapid growth of computer processing power, the demand for authentication methods of digital image data increases. All methods used for the image verification can be classified in (a) watermark based and (b) digital signature based [1, 2]. In this paper we will present digital signature based method for image authentication and tamper localization establishment.

As in watermarking – digital signatures may be fragile or robust, sensitive to some modifications and insensitive to others. Terms "digital signature" and "watermark" sometimes are used interchangeable, methods when digital signature is extracted from the image and embedded as a watermark erase the difference between digital signature and watermarking methods [2].

Digital signature methods have taken few research directions – message authentication code (MAC, AMAC, AIMAC) [3], visual hash [4], robust hash [5] and digital signature itself [6]. But all these methods follow the same path – feature extraction and subsequent use of the feature for later authentication – with variations in features chosen, processing and extraction mechanisms.

First methods for digital signature were based on cryptographic digital signature functions [7]. But when the requirement to authenticate *content* rather than *file* became evident, the term *digital signature* has evolved and changed its meaning in multimedia authentication domain [8]. Robust *features*, extracted from the image, became basis of the new digital signature. Wavelet based hashing in [1] uses the idea that the inter-scale relationship is difficult to be destroyed by content preserving manipulations and hard to be preserved by content changing manipulations. Expanded traditional hash techniques by iterating over the message (e.g., an image) several times [3]. Soft-hashing was first proposed in [7], ability to estimate the limited number and location of the errors was presented in [3].

Some researches integrate the aforementioned methods with additional mechanisms like error correction codes (ECC). In some cases ECC is applied for the initial data, extracted features, digital signature itself or only parities of ECC are used [9] in order to further expand the methods of digital signature.

During the writing of this paper, Qibin Sun published his method for tamper localization using a digital signature [5]. This is second method that allows tamper localization in a digital signature scheme.

The proposed image authentication method can be easily integrated into PKI infrastructure [7]. Generated signature can be signed by authorized persons and published in the Internet. This allows interested parties to authenticate image in question and to locate tampered parts using trusted signature from the identified author of the image.

Proposed method

In our scheme we chose an approach based on convolutional codes where each m-bit information symbol to be encoded is transformed into an n-bit symbol. m/n is the code rate ($n \geq m$) and the transformation is a function of the last *k* information symbols, where *k* is the constraint length of the code. Block codes of length *n* and rank *k* are defined in a linear subspace C with dimension *k* of the vector space F_q^n where F_q is the finite field with *q* elements.

Block codes can be defined as a fixed length channel code - a block code takes a *k*-digit information word, and transforms this into an *n*-digit codeword. Let $T = \{t_1, \ldots, t_q\}$ ($q > 1$) be the channel alphabet. Code of length *n* is *q*-ary non-empty subset $C \subseteq T^n$.

We propose a new method that allows us to determine image authentication in semi-fragile way and to identify tampered pixels. For this two separate mechanisms are used. Respectively digital signature is composed of two parts – part A (authentication) and part TL (tamper localization). This composition disables oracle attack [10].

Digital signature part A is designed to achieve two objectives. First, it addresses the problem with digital signature based image authentication – it provides computationally efficient way to establish correct image-signature pair. For high-load applications (authentication centers) possibility to use clustering based approach is open. Second, it allows determining image authentication in semi-fragile way. It is insensitive to image content

preserving modifications and sensitive to operations that modify the image in a major way. Furthermore, design of the authentication mechanism integrates a backup option – human interaction.

We use DWT decomposition to generate low value version of the image for authentication purposes:

$$Wf(u,s) = \langle f, \psi_{u,s} \rangle = \int_{-\infty}^{+\infty} f(t) \frac{1}{\sqrt{s}} \psi^* \left(\frac{t-y}{s} \right) dt \quad (1)$$

$$\psi_{u,s}(t) = \frac{1}{\sqrt{s}} \psi \left(\frac{t-u}{s} \right) \quad (2)$$

In the algorithm DWT functions as a semi-fragile one way function, i.e. it is mathematically impossible to restore high value version of the image from the signature. The size of 3rd decomposition level is 1% of initial size of the image, time to calculate DWT is O(n). Part A is semi-fragile in this case, because 3rd (or higher) decomposition level is not influenced by minor modifications arising, for example, from file format changes.

Digital signature part TL extends basic ideas of ECC. Traditionally the image was restored by ECC and difference map between the image in question and restored image was generated. This difference map is adequate to tampering map. The disadvantage of this approach is that ECC is block-based (by definition) and there does exist a threshold of modifications that ECC scheme is capable to withstand. In case this threshold is violated, the restoration procedure of the block fails and location of tampered pixels cannot be determined. We constructed a new algorithm that does not need to restore the image in order to identify tampered pixels. The efficiency of the method is achieved integrating ECC with 2D image structure and this integration allows refining tamper localization for up to one pixel even if ECC by itself is not capable to restore the block. Furthermore, ECC ability to *restore* tampered pixels is not required for functionality of the algorithm; all that matters is ECC ability to *identify* tampered blocks.

In order to generate digital signature TL part, original image is down sampled to 4 MSB bits. This step increases robustness against minor changes, against content-preserving modifications and decreases the amount of data to be processed by the ECC by 50%. The downsampled image data is interleaved and forwarded to ECC process as initial data field F_q.

Further, F_q is partitioned into subsets $V_H(:)$ and $V_V(:)$. For a vector in each subset corresponding PCBs are calculated. The polynomial form of generator polynomial for the Reed-Solomon code we use is:

$$g(x) = G_{n-k-1}x^{n-k-1} + G_{n-k-2}x^{n-k-2} + \ldots + G_1x + G_0 \quad (3)$$

where parameters *n* and *k* based on numerical experiments were chosen to be equal to (17,13). We use the same polynomial over the intersecting subsets of F_q – additional algebraic relation is enforced *a priori* at encoder level in order to correlate subsets $V_H(:)$ and $V_V(:)$. We exploit this correlation to increase tamper localization up to one pixel.

Tamper localization procedure is based on the following logic: let $x \in F_q$. Tampered x` may be recognized by identifying discrepancies in PCBs and exploiting the correlation of subsets $V_H(:)$ and $V_V(:)$, without the expensive search of nearest word within the Hamming distance from x`.

From the defined logic follows that any x` from $V`_X(:)$ can acquire one of three possible states:

1) trusted := *error_count*($V`_X$) == 0;
2) uncertain := *error_count*($V`_X$) > 2;
3) damaged := *error_count*($V`_X$) < 3.

These states are correlated from the definition in generation process. Combining these states, the third, final state can be generated. Table 1 summarizes the logic of this layer:

Table 1. Logic of the states

State 1 ($V`_H$)	State 2 ($V`_V$)	Final state
Trusted	Trusted	Trusted
Trusted	Uncertain	Trusted
Trusted	Damaged	-
Uncertain	Trusted	Trusted
Uncertain	Uncertain	Uncertain
Uncertain	Damaged	Damaged
Damaged	Trusted	-
Damaged	Uncertain	Damaged
Damaged	Damaged	Damaged

However, ECC ability to *restore* tampered pixels gave rise to another interesting effect – we named it iterative restore process. The process is based on the fact that after the first ECC pass, the values of restored pixels can be used for the second pass, thus increasing the total amount of identified and corrected pixels.

This logic can be extended further to the process we shall call iterative restore process. Let us analyze the following situation, where state $V`_H$ of the pixel is "trusted" and state $V`_V$ is "uncertain". Final state in this case is "trusted". The following situation means that the amount of modifications in vector $V`_V$ exceeded the error correction capability of ECC . This means that part of the vector is damaged and part is trusted, but ECC has not enough information to locate these parts.

Two layers of interactive logic are possible now. First of all, we can check the pixel value in V_H and in V_V. If values are different, pixel in V_X (where V_X := *uncertain*(V_V,V_H)) is set to correct value and ECC process in run again for vector V_X. If, for example, the vector V_X had three damaged pixels (beyond ECC capability), now it has two and ECC can correct these errors. These two corrected pixels can be used again in iterative processes to identify, locate and correct other damaged pixels.

Second logic layer is used in case pixel values in V_H and V_V are identical – they both are correct. In this case pixel in vectors V_H/V_V is marked as "trusted" and ECC can take this additional data, this side information into account performing error localization and correction.

Algorithm. Digital signature generation

Proposed digital signature generation process involves the following steps:

1. Original image I is provided by the user. If secret behavior is required, secret key K has to be provided by

the user as well. If public behavior is expected, K is initialized to a known constant value.

2. Low value image I_L is generated from I using DWT as a semi-fragile one-way function.

3. Down sampled image I_d is generated from I. The I_d is interleaved, according to a pseudo-random number generator, initialized by K.

4. I_d is partitioned into subset V_H.

5. I_d is partitioned into subset V_V. Partitioning order has to be different from partitioning of V_H.

6. For each vector in V_H/V_V, ECC parities are calculated.

7. I_L and PCB_H/PCB_V are combined into a digital signature.

The size of the signature is mainly affected by tamper localization part – as the size of part A is approximately 1% of initial image size. Based on numerical experiments with the defined *n*, *k* parameters, the size of the PCBs is approximately 30% of original image.

The generated signature can be incorporated in PKI infrastructure and forwarded to 3rd party authentication center for secure storage. In case of any questions the center would confirm the author and the date the signature was received/the image was created. As it is impossible to regenerate original high value image from the signature, possible leakage of the signature from authentication center would present no commercial threat for the author.

Authentication establishment procedure

Image authentication process involves the following steps:

1. Suspected image I` is provided by the user. If secret key K was used, it should be provided too.

2. Digital signature S may be provided by the user. Alternatively, digital signature S may be found in the database of digital signatures (in case of authentication center).

3. Low value image $I`_L$ is generated from I`. Trust level of image-signature pair is established.

4. If I` was tampered, tamper localization procedure is executed and damage map is generated.

In order to check image authentication, a digital signature should be provided. If authentication center participates in the process, corresponding digital signature has to be found. In both cases low value image $I`_L$ is generated at first. Then it is used to find corresponding digital signature and to establish trust level of image-signature pair. In worst case even integration of human opinion is possible, as both $I`_L$ and I_L represent adequate human understandable images.

When sufficient trust level between image in question and digital signature has been established, it is possible to run complete tamper localization process. We would like to notice that correct image authentication is not a requirement for tamper localization part, i.e. image authentication helps to locate corresponding digital signature efficiently, to prevent oracle attack, to determine authentication of the image but if required tamper localization can be run without determining image authentication.

The efficiency of authentication establishment depends on the efficiency of wavelet decomposition process – O(n).

Tamper localization procedure

For tamper localization additional steps are performed:

1. Down sampled image I_d is generated from I. The I_d is interleaved, according to a pseudo-random number generator, initialized by K.

2. I_d is partitioned into subsets V_H/V_V.

3. Each vector in V_H/V_V is checked for tampering, additional logic is applied.

4. If I` was tampered, damage map and restored image I_R are generated.

Numerical experiments

Numerical experiments were performed with standard images, we present results for the Lena image. The image was affected by local attack – "LNK" and "LITHUANIA" added as a copyright signs. As we see, the method we propose performs successfully. The second attack was extension to the first attack – previously attacked image was additionally blurred (global attack). As we see, the first iteration is not enough to restore the image, and this gives as an opportunity to use second iteration. Analysis of the results is provided in table 2.

Experiment #1. Attacked Lena ("LNK" and "LITHUANIA").

Fig. 1. Attacked Lena

Fig. 2. Damage map

Fig. 3. Restored image. PSNR=50

Experiment #2. Attacked Lena from Experiment #1 was additionally blurred.

Table 2. Results from iterative process

	After iteration #1	After iteration #2
H vectors, detected as trusted	476	3’014
H vectors, detected as recovered	2’778	1’293
H vectors, detected as damaged	1’866	813
Amount of damaged pixels	16’400	5’153
Amount of lost pixels	9’881	2’557
Max amount of damaged px in one vector	9	8
Avg amount of damaged px in one vector	1.52	0.72

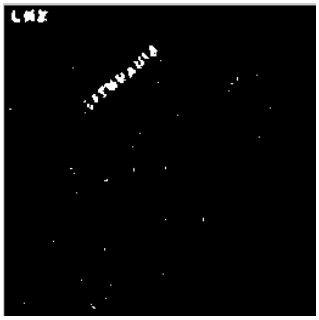

Fig. 4. Final damage map.

Fig. 5. Restored image after #2 iteration

The white pixels in Fig.5 is the result of mistakes in Reed-Solomon error detection codec. The rate of the mistakes is about 1%.

The black pixels are still lost in the current iteration. They may be restored in following iterations.

Conclusions

In this paper advanced semi-fragile digital signature method is presented. Proposed approach enabled us to authenticate image in question – simple but effective design is capable to withstand algorithmic attacks like oracle attack. Innovative 2D analysis, that mimics 2D image structure, allows identifying tampered regions with resolution up to one pixel, using block-based scheme. Extension of ECC principles gave rise to iterative restore procedures, thus enabling restoration of damaged image after image processing operations from the digital signature.

References

1. **Chun-Shien Lu, Hong-Yuan Mark Liao**, Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme // Proc. ACM Multimedia and Security Workshop at the 8th ACM Int. Conf. on Multimedia. – 2000. – P. 115–118.
2. **Wakatani A.** Digital Watermarking for ROI Medical Images by Using Compressed Signature Image // Proc. System Sciences. – 2002. – P. 2043–2048.
3. **Boncelet C.** Image authentication and tamper proofing for noisy channels – // IEEE Image Processing. – 2006. – P. 1985–1988
4. **Xie L., Arce G.R., Graveman R.F.** Approximate Image Message Authentication Codes // IEEE Trans. Multimedia. – 2001. – P. 242–252.
5. **Norcen R., Uhl A.** Robust Visual Hashing Using JPEG 2000 // IFIP. – 2005. – P. 223–235.
6. **Sun Q**. Robust hash for detecting and localizing image tampering // ICIP07. – 2007. – P. 117–120.
7. **Schneider M., Chang S.** A robust content based digital signature for image authentication // ICIP. – 1996. – P. 227–230.
8. **Schneier B.** Applied Cryptography, New York:Wiley. – 1996. – 784 p.
9. **Johnson M., Ramachandran K.** Dither–based secure image hashing using distributed coding // Proc. IEEE Int. Conf. Image Processing. – 2003. – Vol. 2. – P. 751–754.
10. **Baušys R., Kriukovas A.** Vandens ženklų taikymas vaizdų autentiškumo užtikrinimui // Informacinės technologijos 2005: aktualijos ir perspektyvos. IV mokslinės praktinės konferencijos pranešimų medžiaga. – 2005. – P. 17–21.

Submitted for publication 2008 02 14

R. Bausys, A. Kriukovas. Digital Signature Approach for Image Authentication // Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. – No. 6(86). P. 65–68.

The paper examines watermarking and digital signature based approaches for image authentication. It is shown that digital signature has a better performance at least in semi-blind watermarking case. Digital signature based method for image authentication and pixel-wise tamper localization is proposed. The method is able to restore tampered pixels to initial value. Ill. 5, bibl. 10 (In English; summaries in English, Russian and Lithuanian).

Р. Баушис, А. Крюковас. Использование цифровой подписи для аутентификации изображениях // Электроника и электротехника. – Каунас: Технология, 2008. – № 6(86) . – С. 65–68.

Статья анализирует подходы, основаны водяными знаками и цифровой подписью для удостоверения подлинности изображений. Показано, что цифровая подпись отличается лучшимы свойствами, чем водяные знаки, как минимум в полуслепом случае. Предлагается метод, основанн на цифровой подписи, для удостоверения подлинности изображений с локализацией изменений до отдельных пикселей. Метод позволяет восстановить изменение пиксели на изначальные значения. Ил. 5, библ. 10 (на английском языке; рефераты на английском, русском и литовском яз.).

R. Baušys, A. Kriukovas. Skaitmeninio parašo naudojimas vaizdų autentiškumui užtikrinti // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2008. – Nr. 6(86). P. 65–68.

Straipsnyje analizuojami vandens ženklo įrašymu ir skaitmeninio parašo generavimu pagrįsti atvaizdų autentiškumo užtikrinimo metodai. Parodoma, kad skaitmeninio parašo savybės yra geresnės nei vandens ženklų, bent jau pusaklio ženklinimo atveju Pasiūlytas skaitmeninio parašo metodas atvaizdų autentiškumui užtikrinti, palaikantis paskirų pikselių lygmens pažeidimų lokalizavimo tikslumą. Šiuo metodu taip pat galima atkurti pažeistų pikselių pradines reikšmes. Il. 5, bibl. 10 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).

DOI: 10.5755/j02.eie.11186