IMAGE AUTHENTICATION USING CHAOTIC MIXING SYSTEMS

Anastasios Tefas and Ioannis Pitas

Department of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 540 06, GREECE, pitas@zeus.csd.auth.gr

ABSTRACT

A novel method for image authentication is proposed. A watermark signal is embedded in a grayscale or a color host image. The watermark key controls a set of parameters of a chaotic system used for the watermark generation. The use of chaotic mixing increases the security of the proposed method and provides the additional feature of imperceptible encryption of the image owner logo in the host image. The method succeeds in detecting any alteration made in a watermarked image. The proposed method is robust in high quality lossy image compression. It provides the user not only with a measure for the authenticity of the test image but also with an image map that highlights the unaltered image regions when selective tampering has been made.

1. INTRODUCTION

In the last decades massive digitization of multimedia data such as photographs, paintings, speech, music, video, documents etc., became very popular. New techniques for the representation, storage and distribution of digital multimedia information have been developed. At the same time, the amount of digital data that is distributed through international communication networks is rapidly increased. In such an environment original digital products can be easily copied, tampered and transmitted back in the network. Consequently, the design of robust techniques for copyright protection and content verification of multimedia data became necessary.

When content verification of multimedia data is the objective, research is mainly focused in the development of *fragile watermarks*. By the term fragile watermarks we mean watermarks that have the property of being distorted when the host media is tampered somehow. The design of algorithms that generate imperceptible fragile watermarks and detect any alteration of the host signal is the objective in content verification systems. In this paper the problem of image authentication is treated.

Several approaches have been recently proposed to address the issue of tamper proofing. The development of a "trustworthy digital camera" is proposed in [3]. A digital image is captured from a camera and then it is passed through a hash function. The output of the hash function is encrypted by the photographer's private key and a separate authentication signal is created. In order to ensure image authentication the encrypted signal is decrypted by the photographer's public key and the hashed version of the original image is compared to that of the received image. In the same category belong the methods that require a separate header for the image authentication [4].

This work has been funded by the LTR-ESPRIT European Project 31103 - INSPECT

A compression tolerant method for image authentication is proposed in [2]. The proposed scheme is based on the extraction of feature points that are almost unaffected by lossy image compression. The major drawbacks of this method are the need of a separate header for storing the digital signature and the low accuracy in the detection of tampered regions. An authentication method that gives a distortion measurement instead of a binary decision about the image authenticity is proposed in [9]. It does not need a separate signature file or header for image authentication but it can not detect the image regions that are authentic if selective modifications to fine image details have been made. A method for watermarking in the wavelet transform domain is proposed for authentication in [8]. The issue of detecting the tampered regions in an image is not addressed. A method for image authentication by changing the least significant bit (LSB) in an image is proposed in [7]. The method although detects alterations that are made in several image regions it is not robust to lossy image compression that does not reduce significantly the image quality.

In this paper a novel technique for image authentication is proposed. It is based on an established watermarking technique [5, 6]. The novelty of the method is based on the detection of tampered regions and alterations in fine details. It provides a measure and not a binary decision about the image authenticity. The use of chaotic mixing techniques for encryption provides high security.

2. WATERMARK GENERATION BY CHAOTIC MIXING

Let $\mathcal{R}$ and $\mathcal{Z}$ denote the set of real and integer numbers, respectively and $\mathcal{U} = \{0, 1\}$. Given an image $f(\mathbf{x}) : \mathcal{D} \subseteq \mathcal{Z}^2 \rightarrow \mathcal{Z}$ and a watermark key $k \in \mathcal{Z}$, a binary watermark $w(\mathbf{x}) : \mathcal{G} \subseteq \mathcal{Z}^2 \rightarrow \mathcal{U}$ can be produced by the watermark generation procedure. The block diagram of the watermarking procedure is depicted in Figure 1. In the watermark generation procedure either chaotic tech-

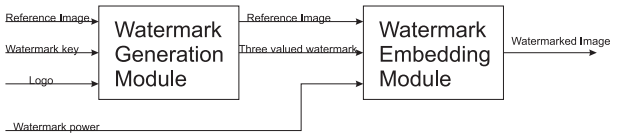


Figure 1: The watermarking procedure.

niques or pseudorandom number generators can be used for producing the watermark $w(\mathbf{x})$.

A two dimensional chaotic mixing can be considered as spatial transformation of planar regions. It is represented by a map:

$$\mathcal{A} : U^2 \rightarrow U^2, U = [0, 1) \subset \mathcal{R} \quad (1)$$

and is defined by the formula:

$$\mathbf{x}_{n+1} = (\mathbf{A}\mathbf{x}_n) \mathrm{mod} 1, \quad \mathbf{x} \in U^2 \quad (2)$$

where $\det \mathbf{A} = 1$. Iterated actions of the map $\mathcal{A}$ on a point $\mathbf{x}_0$ form a dynamical system $\mathcal{A}^{(n)} : U^2 \to U^2$, given by the iterative process:

$$\mathbf{x}_n = (\mathbf{A}^n \mathbf{x}_0) \mathrm{mod} 1 \tag{3}$$

The set of points $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2, \ldots$ is an orbit of the chaotic system. Although these systems are strongly chaotic they possess a set of periodic orbits. An orbit is periodic, if it is finite i.e., there exists a number T of iterations such that $\mathbf{x}_T = \mathbf{x}_0$. The necessary and sufficient condition for an orbit to be periodic is that the initial position $\mathbf{x}_0$ to have rational coordinates [1]. Thus, it is easy to use these maps for discrete lattices $N \times N$, $N \in \mathcal{Z}$ by modifying (2) as:

$$\mathbf{x}_{n+1} = (\mathbf{A}\mathbf{x}_n) \mathrm{mod} N, \quad \mathbf{x} \in \mathcal{F} = [0, N-1] \times [0, N-1] \subset \mathcal{Z}^2 \tag{4}$$

The least common multiple of the periods of all orbits in an image is called *recurrence time*. It is obvious that:

$$(\mathbf{A}^R \mathbf{x}) = \mathbf{x}, \quad \forall \mathbf{x} \in \mathcal{F} \tag{5}$$

where R indicates the recurrence time of the image. The recurrence time is determined by the dimension N of the square lattice and the chaotic map that is used for mixing.

Considering that in chaotic maps $\det \mathbf{A} = 1$ we derive a two parameter family of maps given by the formula:

$$\mathbf{A} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \tag{6}$$

where $a, b \in \mathcal{Z}$. The above map is used for mixing the image owner logo in order to create the watermark $w(\mathbf{x})$. The logo $l(\mathbf{x}) \in \{1, 2\}$ is a binary image of dimensions $N_1 \times N_2$. Alternatively, the logo can be produced by a pseudorandom number generator. The number of pixels to be watermarked is determined by the number of pixels in the logo. We consider the logo to be embedded in a larger area (i.e., of the image size) at the position $\mathbf{m}$ to form the unmixed watermark:

$$w'(\mathbf{x}) = \begin{cases} l(\mathbf{x} - \mathbf{m}) & \text{if } \mathbf{m} \le \mathbf{x} \le \mathbf{m} + (N_1, N_2) \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

If the number of pixels in the logo is smaller or bigger than the number of pixels that we want to sign, the logo image can be resized or repeated in different positions so as its pixels number to be approximately the desirable. After the embedding of the logo a initial watermark $w'(\mathbf{x}) \in \{0, 1, 2\}$ is formed. Afterwards, the watermark is mixed by using the chaotic mixing procedure described previously to generate the watermark $w(\mathbf{x}) \in \{0, 1, 2\}$ which is going to be used for watermarking the image.

For additional security and uncorrelated spreading of the initial logo we can apply a series of chaotic mixing procedures in $w'(\mathbf{x})$ with different parameters. In that case, the position of a pixel after $i+1$ mixing procedures is given by:

$$\mathbf{x}_{i+1} = (\mathbf{A}_i^{n_i} \mathbf{x}_i) \bmod N_i, \quad \mathbf{x}_i \in \mathcal{F} = [0, N_i - 1] \times [0, N_i - 1] \tag{8}$$

were $\mathbf{x}_i$ is the position of the pixel after i mixing procedures. Accordingly, the inverse procedure can be applied iteratively to the mixed image resulting the initial image:

$$\mathbf{x}_{i-1} = (\mathbf{A}_i^{R_i - n_i} \mathbf{x}_i) \bmod N_i \tag{9}$$

where R_i is the recurrence time for the map $\mathbf{A}_i$ and the dimension N_i. The initial unmixed watermark with the logo embedded in several positions is illustrated in Figure 2a. The result after mixing the initial watermark three times with different parameters according to (8) is shown in Figure 2. The inverse procedure for recovering the embedded logo according to (9) is illustrated in Figure 3.

3. WATERMARK EMBEDDING

The next procedure is the watermark embedding procedure of the watermark $w(\mathbf{x})$ in the image $f(\mathbf{x})$ and is given by:

$$f_w(\mathbf{x}) = f(\mathbf{x}) \oplus w(\mathbf{x}) \tag{10}$$

where $f_w(\mathbf{x})$ is the watermarked image and $\oplus$ is a generalized superposition operator which includes appropriate data truncation and quantization if needed. The watermark embedding procedure can be applied either in the spatial domain or in the DFT,DWT,DCT domains. In the watermark embedding procedure we alter all the pixels of the original image according to the following formula:

$$f_w(\mathbf{x}) = \begin{cases} f(\mathbf{x}) & \text{if } w(\mathbf{x}) = 0 \\ g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 1 \\ g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) & \text{if } w(\mathbf{x}) = 2 \end{cases} \tag{11}$$

where g_1, g_2 are suitably designed functions based on $\mathbf{x}$ and $\mathcal{N}(\mathbf{x})$ which denotes a function that depends on the neighborhood of $\mathbf{x}$. The functions g_1, g_2 are called *embedding functions* and they are selected so as to define an inverse detection function $G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x}))$. The detection function when it is applied to the watermarked image $f_w(\mathbf{x})$ gives the watermark $w(\mathbf{x})$:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = w(\mathbf{x}) \tag{12}$$

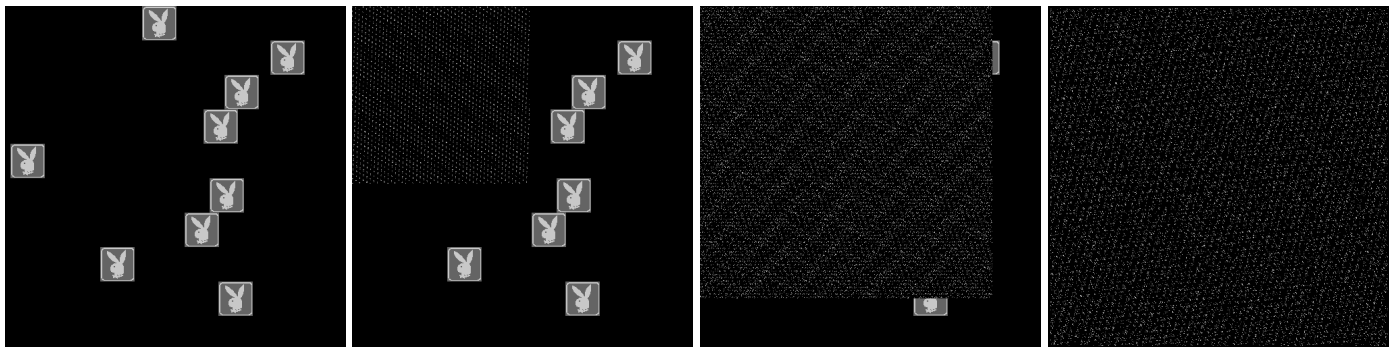
Obviously several embedding functions and the appropriate detection function can be designed giving different watermarking schemes. The function that is used in our method is based on an averaging operation and a superposition of real quantities in the pixels which are going to be signed:

$$g_1(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_1 f(\mathbf{x}) \tag{13}$$

$$g_2(f(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \mathcal{N}(\mathbf{x}) \oplus \alpha_2 f(\mathbf{x}) \tag{14}$$

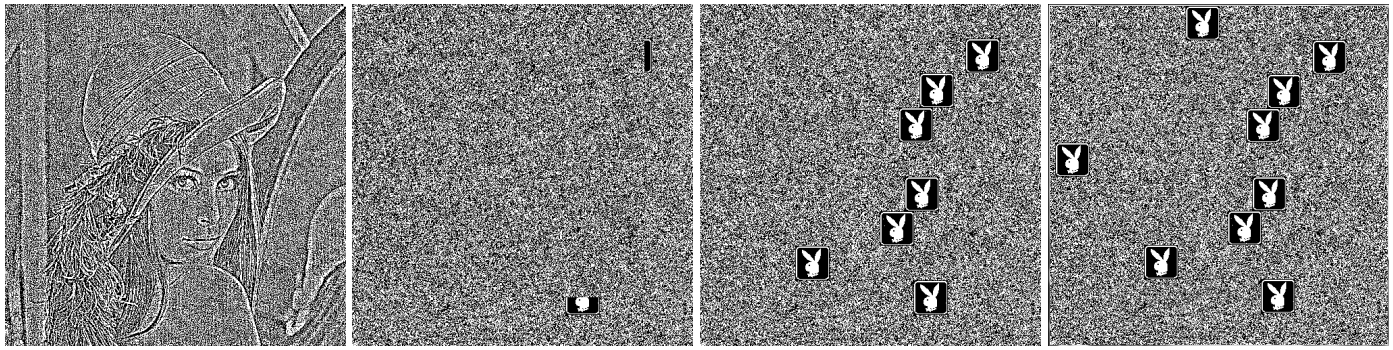
where α_1, α_2 are suitably chosen constants and $\mathcal{N}(\mathbf{x})$ is a local operator of the pixels around $\mathbf{x}$. The sign of α_1, α_2 is used for the detection function. In order to avoid perceptual distortions the values of α_1, α_2 should be small enough.

The size of the neighborhood of $\mathbf{x}$ used for the calculation of $\mathcal{N}(\mathbf{x})$ is important for the watermarking procedure. Moreover, the number of pixels used for the calculation of $\mathcal{N}(\mathbf{x})$ determines the upper bound of the number of watermarked pixels in an image. If a pixel to be signed is contained in the neighboring region of another signed pixel the detection function of the later may affected by the alteration to the former pixel resulting in a false detection. To avoid such problems we should use small blocks (i.e., 3×3). The maximum number of pixels that can be signed in an image of dimensions $N \times N$ by using blocks of $(2r+1) \times (2r+1)$ for calculating $\mathcal{N}(\mathbf{x})$ is $k = \frac{N^2}{(r+1)^2}$.



(a) (b) (c) (d)

Figure 2: The watermark generation procedure by using chaotic mixing. (a) Initial unmixed watermark. (b) First mixing. (c) Second mixing. (d) Final watermark image generated by a third mixing.



(a) (b) (c) (d)

Figure 3: The watermark detection (logo recovering) procedure by using chaotic mixing. (a) Initial detection image by applying the detection function in the image. (b) First inverse mixing. (c) Second inverse mixing. (d) Final detection image generated by a third mixing.

4. WATERMARK DETECTION

The last procedure of the watermarking framework is the watermark detection procedure which gives the detection ratio of the watermark (i.e. a authenticity measure for the image), a binary decision for the image authenticity and possibly an image denoting the unaltered (authentic) regions of the watermarked image. The block diagram of the watermark detection procedure is illustrated in Figure 4. In the detection procedure we generate first the watermark $w(\mathbf{x})$ according to the procedure described in Section 2. The detection function resulting from (13,14)is defined as:

$$G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) = \begin{cases} 1 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) > 0 \\ 2 & \text{if } f_w(\mathbf{x}) - \mathcal{N}(\mathbf{x}) < 0 \end{cases} \tag{15}$$

The detection function holds if $\alpha_1 > 0$ and $\alpha_2 < 0$ and this should be considered in the design of the embedding functions. By employing the detection function in the watermarked image a bi-valued detection image $d(\mathbf{x})$ is produced:

$$d(\mathbf{x}) = G(f_w(\mathbf{x}), \mathcal{N}(\mathbf{x})) \tag{16}$$

Based on the watermark $w(\mathbf{x})$ and the detection image $d(\mathbf{x})$ we can estimate the image authenticity. We can also detect changes made at certain image regions. The detection is based on the pixel to pixel comparison for the nonzero pixels in $w(\mathbf{x})$. By comparing the watermark $w(\mathbf{x})$ and the detection image $d(\mathbf{x})$ we form the false detection image:

$$e_w(\mathbf{x}) = \begin{cases} 1 & \text{if } w(\mathbf{x}) \neq 0 \text{ and } w(\mathbf{x}) \neq d(\mathbf{x}) \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

The false detection image has value 1 if a watermarked pixel is falsely detected and 0 otherwise. The detection ratio is given by the ratio of the correct detected pixels to the sum of the watermarked pixels in the image.

$$D_w = 1 - \frac{\text{card}\{e_w(\mathbf{x})\}}{\text{card}\{w(\mathbf{x})\}} \tag{18}$$

For an unwatermarked image the probability of a pixel to be detected as signed with g_1 or g_2 is $p = 0.5$. Thus, the detection ratio in an unwatermarked image forms a binomial distribution. The cumulative distribution function (*cdf*) of the detection ratio is given by:

$$P_n = p^k \sum_{i=0}^{n} \frac{k!}{i!(k-i)!} \tag{19}$$

where k is the total number of the watermarked pixels and n is the number of correct detected pixels. The decision about the authenticity of an image is taken by comparing the watermark detection ratio of the image with a predefined threshold T. The value of the threshold determines the minimum level of authenticity that is acceptable by the user.

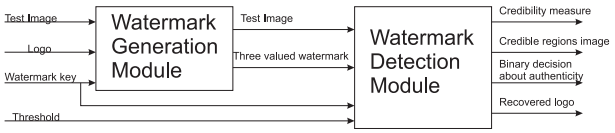


Figure 4: The watermark detection procedure.

5. EXPERIMENTAL RESULTS

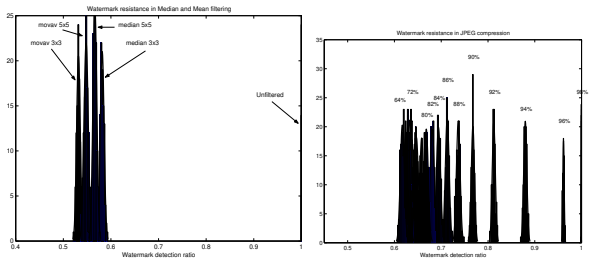
filtering: We have tested the performance of the proposed method for two types of filtering with different window size. These filters are the moving average filter of size 3×3 and 5×5 and the median filter of size 3×3 and 5×5. In order to estimate the pdf of the detection ratio the reference image was watermarked with 100 watermarks generated by random keys and it was filtered using the aforementioned filters. The estimated pdfs of the detection ratio are depicted in Figure 6a. It is obvious from the plots that the detection ratio is reduced significantly when the image is filtered and the output of the algorithm is that the image is not authentic.

Image editing: The most frequent type of attack in an image is the selective editing of certain image regions or the tampering of fine details in an image. This type of attack aims at changing the content of an image and not necessary at reducing the quality of the original image. Thus, it is very difficult to detect such alterations since these alterations are often made in fine details. They succeed to change the image content without changing the watermark detection ratio significantly. The smaller are the regions that can be detected by an image authentication algorithm the better the algorithm is. As it has been described, in the tampered regions the watermark detection ratio should follow (19). The original watermarked image is edited in several regions in such way as the alterations to be imperceptible. The edited image is illustrated in Figure 5b. The false detected watermark image is shown in Figure 5c. It is obvious that the discreditable regions are highlighted.

(a) (b) (c)

Figure 5: (a) Original watermarked image. (b) Altered image. (c) False detection image.

Image compression: Although lossy image compression is not desirable for high quality multimedia products we would like the image authentication method that we use to be robust for high quality image compression (e.g., compression ratio 1:2,1:3). Many methods that have been developed for image authentication have the major drawback that they are not robust for high quality lossy image compression. The method proposed in this paper has the advantage that the watermark embedding functions (11) are designed as to be robust in high quality image compression. In order to estimate the pdf of the detection ratio after lossy image compression with several compression ratios the reference image was watermarked with 100 watermarks generated by random keys and it was compressed with several qualities. The estimated pdfs of the watermark detection ratio for several compression ratios are depicted in Figure 6b. It is obvious from the plots that the detection ratio is significantly reduced when the image is heavily compressed. However, the drop of the detection ratio is smooth and for high quality image compression the detection ratio is more than 90%.



(a) (b)

Figure 6: The estimated pdfs of the watermark detection ratio for several filtering types (a), and compression ratios (b).

6. CONCLUSIONS

A novel method for image authentication has been proposed. It succeeds in detecting any alteration made in a watermarked image and decide for its authenticity. The use of chaotic mixing increases the security of the proposed method and provides the additional feature of imperceptible encryption the image owner logo in the host image.

7. REFERENCES

[1] D. K. Arrowsmith and C. M. Place. *An Introduction to Dynamical Systems*. Cambridge University Press, 1990.

[2] S. Bhattacharjee and M. Kutter. Compression tolerant image authentication. In *Proc. of ICIP'98*, volume I, pages 425–429, Chicago, USA, 4-7 October 1998.

[3] G.L. Friedman. The trustworthy digital camera: Restoring credibility to the photographic image. *IEEE Transactions on Consumer Electronics*, 39(4):905–910, November 1993.

[4] M. Schneider and S.F. Chang. A robust content-based digital signature for image authentication. In *Proc. of ICIP'96*, volume III, pages 227–230, Lausanne, Switzerland, September 1996.

[5] G. Voyatzis and I. Pitas. Digital image watermarking using mixing systems. *Computer & Graphics*, 22(3), 1998.

[6] G. Voyatzis and I. Pitas. The use of watermarks in the protection of digital multimedia products. *Proceedings of the IEEE*, 87(7):1197–1207, July 1999.

[7] P.W. Wong. A public key watermark for image verification and authentication. In *Proc. of ICIP'98*, volume I, pages 425–429, Chicago, USA, 4-7 October 1998.

[8] L. Xie and G.R. Arce. Joint wavelet compression and authentication watermarking. In *Proc. of ICIP'98*, volume II, pages 427–431, Chicago, Illinois, USA, 4-7 October 1998.

[9] B. Zhu, M.D. Swanson, and A.H. Tewfik. Transparent robust authentication and distortion measurement technique for images. In *Proc. of DSP'96*, pages 45–48, Loen, Norway, September 1996.