A Public-key Asymmetric Robust Watermarking Algorithm Based on Signal with Special Correlation Characteristic

Yanjun Hu[1,2], Li Gao, Xiaoping Ma
College of Communication & Electronic Engineering[1]
China University of Mining and Technology
South Suburb
221008, XuZhou, P.R.China
huyanjun@cad.zju.edu.cn

Zhigeng Pan[2,3], Li Li[2]
State Key Lab of CAD&CG[2]
Institute of VR and Multimedia[3]
Zhejiang University
310027, HangZhou, P.R.China
zgpan@cad.zju.edu.cn

ABSTRACT

A public-key asymmetric robust watermarking algorithm based on signal with special correlation characteristic is proposed in this paper. This algorithm is designed to permit pubic watermark detection while preventing the watermark from being removed without the private keys. A signal, which is pseudorandom sequence with special auto-correlation characteristic, is used as watermark, and the signal's characteristic is the foundation of this algorithm. Therefore we first construct the method of generating the pseudorandom sequence and prove its auto-correlation characteristic. Then we describe the algorithm in detail. Experiment results show that the algorithm is valid and robust to common signal distortions and malicious attacks.

Keywords

Public-key; robust watermarking; pseudorandom sequence; auto-correlation.

1. INTRODUCTION

Digital watermarking is a kind of technique that embeds the signal including owner identification and copy control information into multimedia data such as audio, video and images for copyright protection [Cox02a, Li02a, Yin01a].

Watermarking algorithms can be classified into fragile watermarking and robust watermarking [Pet99a, Vin02a].

The public-key watermarking algorithm can be more effective to face the attacks. Also it has more potential value of application. Some public-key fragile watermarking algorithms are proposed. The Wong's algorithm [Won01a], which based on public-key cryptography, is a typically one. However, there are few public-key robust watermarking algorithms proposed since they are requested to survive severe tampering. In Wong's algorithm, any subtle change in watermarked media will make the decrypt failure. Thus Wong's method can not be applied simply to the robust watermarking algorithm.

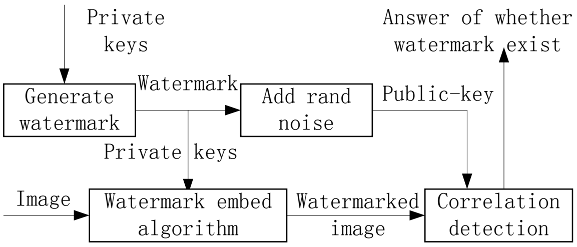

Figure 1. Watermark embedment & detection process

Based on a special signal, which is pseudorandom sequences with special auto-correlation characteristic, we propose a pubic-key asymmetric robust watermarking algorithm (see Figure 1). In this algorithm, to detect whether an image is watermarked or not, we just need to calculate the cross-correlation function between the public-key and coefficient extracted from the image. That is, except a bi-answer of whether the image is watermarked, you will not know any information of watermark else in the watermark detection process. This algorithm also answers the Cox's question [Cox02a]: whether a watermark system can be

***WSCG POSTERS** proceedings*
WSCG'2004, February 2-6, 2004, Plzen, Czech Republic.
Copyright UNION Agency – Science Press

designed that permits public detection of the watermark while preventing an adversary from removing the watermark.

The goal of this paper is to present a public-key robust watermarking scheme which is not based on cryptography. To implement the scheme, the watermark (a special signal with special auto-correlation characteristic) is designed. In Section 2, the generating method of watermark is presented, and it is proved that the watermark has the special auto-correlation characteristic. In Section 3, a pubic-key watermarking algorithm based on this kind of watermark is demonstrated. It is experimented the algorithm's robust to common signal distortions and malicious attacks in Section 4. A conclusion is given in Section 5.

2. CREATEION OF WATERMARK AND ITS CORRELATION CHARACTERISTIC

Composition of Watermark

The generating method of watermark based on the OPSS (optimal pseudorandom sine sequences) [HU00a], which is introduced as followings:

If p is a prime and b is its primitive root, then $1/p$ is full-recurrent-decimal-sequence. we can get OPSS $x=\{x[n]\}$ from this sequence. By extending the sequence with the period $p-1$, the auto-correlation function is:

$$R(x,\tau)=\frac{1}{p-1}\sum_{k=1}^{p-1} x[k]\bullet x[k+\tau]$$

$$=\begin{cases} p/(2(p-1)); & \tau=0 \\ -p/(2(p-1)); & \tau=(p-1)/2 \\ 0; & 0<\tau<p-1, \tau\neq(p-1)/2 \end{cases} \qquad (1)$$

The watermark is generated by inserting a small random real data I before the *k–th* data of OPSS, where $1\leq k\leq p, I\ll p$

Auto-correlation Characteristic Of Watermark

Extending the watermark sequence $y=\{y[n]\}$ with the period p, the auto-correlation function is:

$$R(y,\tau)=\frac{1}{p}\sum_{k=1}^{p} y[k]y[k+\tau]$$

$$\approx\begin{cases} 0.5; & \tau=0 \\ -0.25; & \tau=\frac{p}{2},\frac{p}{2}+1 \\ 0; & 0<\tau<p-1; \tau\neq\frac{p}{2},\frac{p}{2}+1 \end{cases} \qquad (2)$$

We will prove Eq. [2] as followings.

Proof. Let $x=\{x[n]\}$ be OPSS, and its auto-correlation function is $R(x,\tau)$. Sequence $y=\{y[n]\}$ is generated by inserting a random real data I into sequence x, where $I\ll p$. Here we assume I is inserted after the $x[k]$. The $R(y,\tau)$ is the auto-correlation function of the sequence y.

(1) While $\tau=0$ or $\tau=1$, it is easy to validate correctness of the equation.

(2) While $2\leq\tau\leq k+1$ and $p\gg I$, we can get:

$$R(y,\tau)=R(x,\tau)+R(x,\tau-1)+\frac{I}{P}(x[k-\tau+1]+x[k+\tau])-g(\tau)$$

Where:

$$g(\tau)=\frac{1}{p}\Big(\sum_{i=k-\tau+1}^{k} x[i]\bullet x[i+\tau]+\sum_{i=0}^{k-\tau+1} x[i]\bullet x[i+\tau-1]+\sum_{i=k+1}^{p-1} x[i]\bullet x[i+\tau-1]\Big)$$

$$=\frac{1}{2p}\sum_{i=k-\tau+1}^{k}\Big(\cos\frac{2\pi b^{i-1}(1-b^{\tau})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau})}{p}\Big)$$

$$+\frac{1}{2p}\sum_{i=0}^{k-\tau+1}\Big(\cos\frac{2\pi b^{i-1}(1-b^{\tau-1})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\Big)$$

$$+\frac{1}{2p}\sum_{i=k+1}^{P-1}\Big(\cos\frac{2\pi b^{i-1}(1-b^{\tau-1})}{p}-\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\Big)$$

Assume $i=1,2,\cdots,p-1$, then b^{i-1} goes through the group of mod p, except the value 0. For $1\leq\tau\leq p$, there must be $b^{\tau}-1\neq0(\bmod p)$ and $b^{\tau-1}-1\neq0(\bmod p)$, and $\sum_{i=k-\tau+1}^{k} b^{i-1}(1-b^{\tau})\cup\sum_{i=0}^{k-\tau+1} b^{i-1}(1-b^{\tau-1})\cup\sum_{i=k+1}^{P-1} b^{i-1}(1-b^{\tau-1})$ will take the number of $p—2$ value of mod p group one for each, except the value 0.

①If $\tau\neq(p-1)/2$ or $\tau\neq(p+1)/2$, it can be obtained that $g(\tau)=\frac{\varepsilon(I,k,\tau)}{p}\approx0$ （ where $\varepsilon(I,k,\tau)\in[-2,2]$ ） since the $\sum_{i=k-\tau+2}^{k} b^{i-1}(1+b^{\tau})\cup\sum_{i=0}^{k-\tau+1} b^{i-1}(1+b^{\tau-1})\cup\sum_{i=k+1}^{P-1} b^{i-1}(1+b^{\tau-1})$ take the number of $p—2$ value of mod p group one for each, except the value 0.

②If $\tau=(p-1)/2$, there is $\cos\frac{2\pi b^{i-1}(1+b^{\tau})}{p}=1$ and $\sum_{i=0}^{k-\tau+1}\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\cup\sum_{i=k+1}^{P-1}\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}\approx\frac{p-2}{4}$, thus $g(\tau)\approx\frac{1}{4}$

③If $\tau=(p+1)/2$, there is $\cos\frac{2\pi b^{i-1}(1+b^{\tau-1})}{p}=1$; and $\sum_{i=k-\tau+2}^{k}\cos\frac{2\pi b^{i-1}(1+b^{\tau})}{p}\approx\frac{p+1}{4}$, thus $g(\tau)\approx\frac{1}{4}$.

It is concluded that Eq. [2] are valid.

(3)While $k+1<\tau\leq p$, and $p\gg I$, it is:

$$R(y,\tau)=R(x,\tau)+R(x,\tau-1)+\frac{I}{P}(x[k-\tau+1]+x[k+\tau])-h(\tau)$$

Where:

$$h(\tau)=\frac{1}{p}(\sum_{i=k-\tau+1}^{k} x[i]\bullet x[k+\tau+1]+\sum_{i=0}^{k-\tau+1} x[i]\bullet x[i+\tau]+\sum_{i=k+1}^{p-1} x[i]\bullet x[i+\tau])$$

The proof is similar with (2), and it is omitted.

3. WATERMARKING ALGORITHM

Three notations are defined as following:

- The *benchmark sequence* is defined as following:

$$St(\tau)=\begin{cases} 0.5; & \tau=0 \\ -0.25; & \tau=\frac{p}{2},\frac{p}{2}+1 \\ 0; & 0<\tau<p-1;\tau\neq\frac{p}{2},\frac{p}{2}+1 \end{cases} \quad (3)$$

where p is the length of sequence and it is a primitive root of 10.

- For sequence $x=\{x[n]\}$ and $y=\{y[n]\}$, whose length are both p, their *cross-correlation function* is:

$$R(x,y,\tau)=\frac{1}{p}\sum_{k=0}^{p-1} x[k]\bullet y[k+\tau(\bmod p)] \quad (4)$$

their *distinguish function* is:

$$Dis(x,y)=\sum_{k=0}^{p-1}\left|\frac{x[k]}{2|x[0]|}-\frac{y[k]}{2|y[0]|}\right| \quad (5)$$

Watermark Embedment

Let $W=\{W[i]\}$ ($i\in[1\ldots p]$) denoted the watermark, which is generated through the method discussed in Section 2.2 by choosing I and k. The values of I and k are private keys. Then a random sequence whose length is the same as watermark' length, denoted by $Rndn=\{Rndn[i]\}$, is also given. The public-key is generated by Eq.[6]:

$$PubK[i]=W[i]+Rndn[i] \quad (6)$$

Then the watermark can be embedded as the algorithm described in [Cox99a]. Cox proposed three formulae. The following equation is adopted: $r_w[i]=r_o[i]+\alpha\bullet PriK[i]$ ($i\in[1\cdots p]$), where α is embedment intensity. Also it is one of private keys.

Watermark detection

The detection process does not need these private keys. It is based on auto-correlation characteristic of watermarks. First, we extract a sequence of value $v=\{v[i]\}$ from test image. Then $R(v,PubK,\tau)$, the cross-correlation function between sequence v and $PubK$, is calculated.

- If test image has been watermarked: Thus the sequence v can be considered: $v[i]=I_o[i]+\alpha\bullet W[i]+n[i]$. Here, $\{n[i]\}$ is possible noise. And the following relations hold:

$$R(v,PubK,\tau)=R(I_O+\alpha\bullet W+n,W+Rndn,\tau) \quad (7)$$

Where the sequence W is independent of I_o, $Rndn$ and n. The sequence $Rndn$ is independent of I_o and n. Thus, we can obtain Eq. [8] :

$$R(v,PubK,\tau)\approx\alpha\bullet R(W,W,\tau)\approx\alpha\bullet St(\tau) \quad (8)$$

So, the value of distinguish function will be obtained: $Dis(R(v,PubK,\tau),St(\tau))=\varepsilon$

- If test image has not been watermarked: Similarly, it can be concluded that $Dis(R(v,PubK,\tau),St(\tau))\gg\varepsilon$

Thus, a threshold d is published. Whether watermark exists is judged by comparing the value of $Dis(R(v,PubK,\tau),St(\tau))$ and the threshold d.

4. EXPERIMENTS

The cover image is the 512*512 pixels image "lena". Parameters are set to $p=313$, $b=10$, $\alpha=0.15$, $d=50$. For cover image, which is not embedded watermark, it is can be calculated that the value of the distinguish function (VDF): $Dis(R(v,PubK,\tau),St(\tau))$ =201.38

For the watermarked image, we can calculate that PSNR=44.20dB, VDF=13.42

(1) Common Signal Distortions

The experiment is shown in Figure 2, and the result is Table 1. It is clear that this algorithm can withstand the common signal distortions. It is not unexpected because this algorithm naturally inherits all of the advantage of algorithm works in frequency domain.

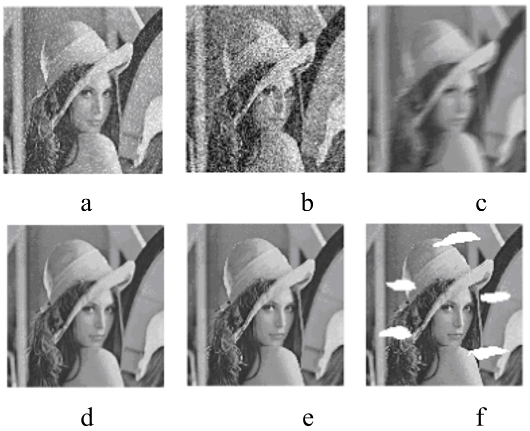

Figure 2. Results of experiment of common signal distortions to watermarked images

Here: attack of (a)adding random noise with mean 0 and maximum 0.1; (b)adding Gaussian noise with mean 0 and variance 0.02; (c)wobbling; (d)applying median filter; (e)applying Wiener filter; (f)performing random cutting out portions of image

Figure 3	a	b	c
VDF	19.33	18.28	97.45

Figure 3	d	e	f
VDF	24.12	19.82	43.95

Table 1. VDF Values of Figure 3

(2) JPEG Compression

The experiment is shown as Table 2. The result suggests that algorithm is robust to common encoding distortions again.

Quality factor	10	20	30
VDF	15.92	15.93	16.32
Quality factor	**40**	**50**	**60**
VDF	15.93	15.92	16.18

Table 2. Robustness to JPEG compress

(3) Malicious Attacks

It is confirmed that the watermark can't be calculated from the public-key because the public-key is created by Eq. [6]. Random noise will be created only just in time when it is needed and will be abandoned when the watermark has been embedded.

Suppose the attacker generate a random watermark, denoted as $GusK$, and choice a random value β as the value of embedment intensity. Then the attacker try to remove the watermark by using $GusK$ and β . From Eq.[7], we can get $R(v,PubK,\tau)\approx \alpha\bullet R(W,W,\tau)+ \beta\bullet R(GusK,W,\tau)$. The value of VDF will be still smaller than the threshold. Figure 3 shows the experiment of collision, and watermarks can be removed only when the correct private keys is used.

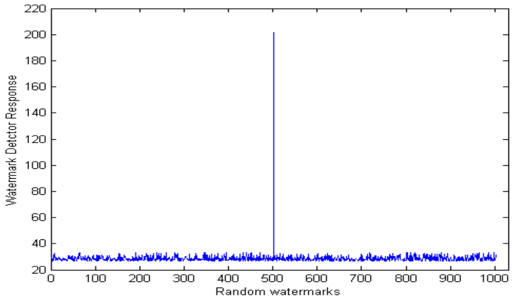

Figure 3. Watermark detector response to remove watermark by using 1,000 randomly generated watermarks and α

Therefore, to remove the watermark, adversary must know the private keys.

5. CONCLUSION

The experimental results show that this algorithm is effective and robust enough to common signal distortions and malicious attack. The time complexity of attacking depends on the length of watermarking signal and the range of embedment intensity α . We can enhance the time complexity of attacking through extending the length of watermark or generating watermarks by assemble several signals discussed in Section 2. It is needed to note that this algorithm can work in other transform domain.

This algorithm can be expanded. Such as it can be used as proof ownership based on experiment result of Figure 3. If someone claims the owner of watermarked image, it means that he/she can eliminate the watermarking "clearly".

6. ACKNOWLEDGMENTS

This research is supported by Excellent Youth NSF of Zhejiang Province (RC 40008) and TRAPOYT Program in Higher Education Institutions of MOE, P.R.C.

7. REFERENCES

[Cox99a]I.J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia, Proc. IEEE, 87(7), 1999, pp.1127-1141.

[Cox02a]Ingemar J. Cox and Matt L. Miller, The first 50 years of electronic watermarking, EURASIP JASP 2002:2, pp.126-132, 2002

[Li02a]Li Li, Zhigeng Pan, Shushen Sun, Xuelong Wu. A Private and Lossless Digital Image Watermarking System, ICIG'2002 conference. 2002,16-18 August, Hefei, pp.365-370

[HU00a]Dewen HU, A novel method for generating pseudorandom integer strings and pseudorandom sequences, Science In China (Series E), 43(4), 2000, pp. 413-420

[Pet99a]F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information Hiding – A Survey, Proc. IEEE 87(1999), pp.1062-1078

[Vin02a]Vinayak, Dangui, EE368A : Final Project Robust watermarking of digital images, Availabe:http://ise0.stanford.edu/class/ee368a_proj01/dropbox/project05/presentation.html

[Won01a]Ping Wah Wong, N. Memon, Secret and public key image watermarking schemes for image authentication and ownership verification , IEEE Transactions on Image Processing, vol:10, 2001, pp.1593 –1601

[Yin01a]K.K. Yin, Z.G. Pan, J. Y. Shi and D. Zhang. Robust mesh watermarking based on multiresolution processing. Computers & Graphics 2001;25: pp.409-420