International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.299-306
http://dx.doi.org/10.14257/ijsia.2015.9.7.27

Researching Indistinguishability of the Polymorphism Time Stamp Watermarking

Yifeng Yin*, Heyu Wen and Kunpeng Fan

School of Computer and Communication Engineering,
Zhengzhou University of Light Industry, Zhengzhou 450002, China
yinyifeng@zzuli.edu.cn

Abstract

With the rapid development of computer network, digital watermarking, which is an effective digital products copyright protection technology, was widely applied in the security forensic. Those were analyzed that are the defects of existing time stamp scheme of digital watermarking and the characteristics of the pseudo-random sequence. The new scheme based on time stamp and pseudo-random sequence was proposed. Indistinguishability and scalability of watermark were analyzed from the experimental results. And other two aspects were obviously improved in the new scheme, which were in improving protocol's security and reducing the quantity of data embedded in digital works.

Keywords: *Digital watermarking; Time stamp; Pseudo-random sequence*

1. Introduction

With the vigorous development of multimedia information, digital watermarking is widely used in as a protection of multimedia information technology. Digital watermarking is a kind of adding identification information in the audio, image and video (watermarking). The difference, which is between the original data and the subsequent watermark information, makes people very difficult to distinguish. And it does not affect the availability of original data. But through the specialized inspection, we can extract the information. The information can prove the original on the copyright of digital products [1-4].

The main purpose of digital watermarking technology is to ensure that the data can prove its owner after being illegal copied. It can guarantee the original copyright, because if there is copyright dispute, arbitration can confirm the authenticity of the watermark copyright real owner through the third party. Watermark arbitration is divided into blind arbitration and non-blind arbitration [5]. Now most digital watermarking schemes are adapted to non-blind arbitration. More relatively attacks on non-blind arbitration's study. And non-blind arbitration is the most common interpretation attack [6].

Interpretation attack is one of the main means of digital watermark attack. In the process of the watermark's arbitration, the arbitrators according to the difference, which is between the works and original works, arbitrate the watermark. The attacker of the interpretation attacks by the existent loopholes in the process. So the arbitration party cannot make correct judgment on ownership [7].

The rest of this paper is organized as follows. In Section 2, we introduced the characteristics of the timestamp protocol and pseudo-random sequence. The proposed algorithm is introduced in Section 3.The discussions of the experimental results are in Section 4. Finally, Section 5 gives the conclusion.

ISSN: 1738-9976 IJSIA

2. Related Theories

2.1 Pseudo-random Sequence

Pseudo random sequence is a certain sequence with some characteristics of random. It is generated by a shift register. And it has some random characteristics. Pseudo random sequence is close to the white noise correlational function, prior to certainty and repeatability. These features make the pseudo random sequences be widely used in cryptography and spread spectrum communication [8-10].

The main property of pseudo random sequence is unpredictable. If given a sequence of prefix, there is no algorithm to greater than 0.5 the probability that cannot be ignored guess it down a bit. That is, the sequence is unpredictable. Shown by the following formula:

$$Pr\left[B(1^{|x_n|}, X_n) = next_B(X_n) \right] < \frac{1}{2} + \frac{1}{p(n)} \tag{1}$$

The algorithm B read-only $i < |x|$ bits of x when entering $(1^{|x|}, X_n)$, then $next_B(x)$ return the i+1 bits of x; On the other hand, that returns a uniform select bits (to prevent B read the entire string x). If there is no probability polynomial time algorithm to the probability that cannot be ignored to the higher than 0.5 after the completion of a task $next_B(x)$, then the ensemble is called unpredictable in polynomial time [11].

When the object is infinite string sequence, there is no efficient algorithm can tell sequence $\{x_n\}$ and $\{y_n\}$ apart. There is no efficient algorithm D that can accept an unlimited number of x_n, and declined with the corresponding y value. So we say that they are not distinguishable.

If there is a uniform overall $U = \{U_{t(n)}\}_{n \in N}$, that makes the X and U indistinguishable in polynomial time. So the overall $X = \{X_n\}_{n \in N}$ is pseudo random. Overall X is pseudo-random if and only if it is not predictable in polynomial time [12].

These properties of pseudorandom sequences are helpful to ensure that the watermark has better robustness, suitable for the need of digital watermarking design.

2.2 Time Stamp Protocol

The time stamp is a special kind of data type. It can uniquely identify a moment of time. By the time stamp protocol, we can tie electronic documents and its generation time together. So it can prove the accurate time of the document. The document has the characteristic that is difficulty to forge [13]. Timestamp agreement must have a trusted timestamp authority (TSA) to provide time. The general process of its generation is as follows: The user will get the electronic document of the Hash code and send to TSA; TSA joins the time of receipt file abstract information and encrypts the file (signature); Then TSA sends back to the user [14].

Based on the characteristics of time stamp, we can add the timestamp in the digital watermark in embedding process. So we can easily determine that the watermark is first added. And it enhances resistance to attack watermark [15]. The specific process of time stamp scheme of digital watermarking is as follows: (1) W creates the work that is named W1; (2)W generates and registers a watermark; (3) W according to $W1$ and Wa generates the watermark works that is named $W1^*$;(4) W calculates Q,that is the Hash values of $W1^*$, $Q = H(W1^*)$ and the signature of Q is denoted as $Sign(Q)$;(5) W sends $(Q, Sign(Q))$ to TSA;(6) TSA signs $Tt = (Q, Sign(Q), T)$ as $Sign(Tt)$,and sends

$P=\left(Tt,Sign\left(Tt\right)\right)$ to the W;(7) W gets $W1^{**}$ after P is embedded in $W1^{*}$, $W1^{**}$ is transmitted in the network as the final version.

In the process of adding timestamp in the digital watermark, the overmuch information in the embedded digital works can be found. And in the so much information, just Wa and T are actually to protect the copyright of digital works and against interpretation attack effectively. If we can take appropriate means to modify the agreement, it only embeds Wa and T into digital works. We can significantly reduce the embedded information so as to improve the practicability of this design.

3. Design of the Polymorphism Time Stamp

Table 1. Notation

Notations	Meaning
W	The original person
W1	The work of W
Wa	The watermark
TSA	Time-stamp authority
Sq,Sq2	Pseudo-random sequence
G1,G2	Gauss normal distribution sequence
K	The scrambling parameter
L,L*,n	Integer

After the previous analysis, combining the characteristics of pseudo-random sequence and time stamp, this paper proposes a digital watermarking scheme design based on time stamp and pseudo random sequence, the specific process is as follows:

Step 1: W creates the work W1; the watermark signal $W0$ is generated by the gauss normal distribution sequence G1. $W0$ is composed of $(0,1)$. After encoding the watermark signal $W0$, we get m0 that is a set of block code. Finally the m0 line to the bit extension, we get m that is the spreading sequence of $(-1,1)$. We set a secret key and the gauss normal distribution sequence G2. Then a pseudo-random sequence Sq, which consists of $(-1,1)$, is generated by G2. $Wa=Sq\times m$. Wa is the watermark that is generated and registered by W. Wa is embedded into $W1$. We get $W1^{*}$. $W1^{*}=W1+Wa$

Step 2: W scrambles the binary bit sequence of $W1^{*}$, and gets $A\left(W1^{*},K\right)$. K is saved by W; W calculates L that is the bit length of A and Takes an integer n. $L^{*}=L/n$. The first nL^{*} bits of A are divided into n blocks that are $Dn=\left\{di\mid i=1\sim n\right\}$. W generates $Sq2$. The length of $Sq2$ is n; by the '0' or '1' that is corresponding to the bit j of $Sq2$, we select the dj blocks from Dn; The regulations are as follows: if j of $Sq2$ is '0', we don't select the dj; otherwise, we select dj; We get $A^{*}\left(W1^{*},K\right)^{*}$ when always select in accordance with the values of bit in $Sq2$;W encrypts $A^{*}\left(W1^{*},K\right)^{*}$ and gets $B=EpT\left(EkW\left(A^{*}\left(W1^{*},K\right)^{*}\right)\right)$. Then W sends B to TSA;

Step 3: TSA decrypts B and gets $EkW\left(A*\left(W1*,K\right)*\right)$ according to its own private key. Then TSA decrypts $EkW\left(A*\left(W1*,K\right)*\right)$ and get $A*\left(W1*,K\right)*$ according to the public key of W.TSA generates T and R based on the current time, scrambles T and R, and get $T*$. Then TSA sends $B* = EpW\left(EkT\left(A*\left(W1*,K\right)*,T*\right)\right)$ to W;

Step 4: W decrypts B* and get $EkT\left(A*\left(W1*,K\right)*,T*\right)$ according to its own private key. Then W decrypts $EkT\left(A*\left(W1*,K\right)*,T*\right)$, then gets $A*\left(W1*,K\right)*$ and $T*$. W gets $W1**$ after $T*$ is embedded in $W1*$, $W1**$ is transmitted in the network as the final version.

W		TSA
$Wa = Sq \times m$, $W1* = W1 + Wa$		Random integer R The current time T
$B = EpT\left(EkW\left(A*\left(W1*,K\right)*\right)\right)$	$\xrightarrow{B}$	$R,T \rightarrow T*$, $B \rightarrow A*\left(W1*,K\right)*$
$A*\left(W1*,K\right)*$, $T*$	$\xleftarrow{B*}$	$B* = EpW\left(EkT\left(A*\left(W1*,K\right)*,T*\right)\right)$
$T*,W1* \rightarrow W1**$		

Figure 1. Design of the New Protocol

4. Security Discussions of the Experimental Results

Experimental results are presented in this section to illustrate effects of the watermark algorithm that is proposed in this work. The simulation experiment was to be done on Matlab 13 platform. In this experiment the original image is “kids” as shown in Figure 2.The watermark that is generated by the proposed algorithm is embedded to the original image. Then we get the watermarked image as shown in Figure 3. Then we get the analysis the watermark expansion image as shown in Figure 4.

From the Figure 2 and Figure 3, our naked eye cannot see the traces of the watermark, which namely satisfy indistinguishability in the subjective visual. In the objective point, the big value of the picture’ PSNR (peak signal to noise ratio) means less distortion in the new algorithm which illustrates the good invisibility of this proposed algorithm. So we get the conclusion that the proposed algorithm has invisibility. From the Figure 4(a), we can see the result of analysis the watermark expansion before the watermarking is embedded in picture. From Figure 4(b), we can see the result of analysis watermark expansion after the watermarking is embedded in picture. After extracting the watermark from the image, we get the same analysis result as Figure 4(a). So, the conclusion can be proved that the watermark has good expansion.

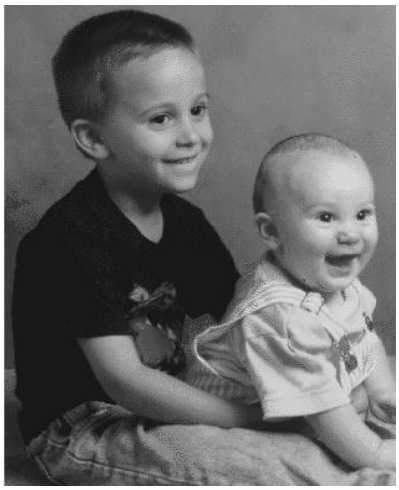

Figure 2. Original Image

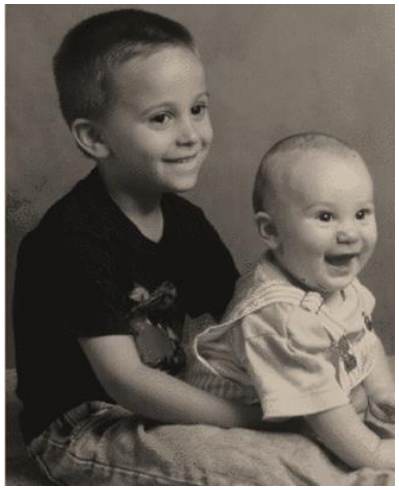

Figure 3. Watermarked Image

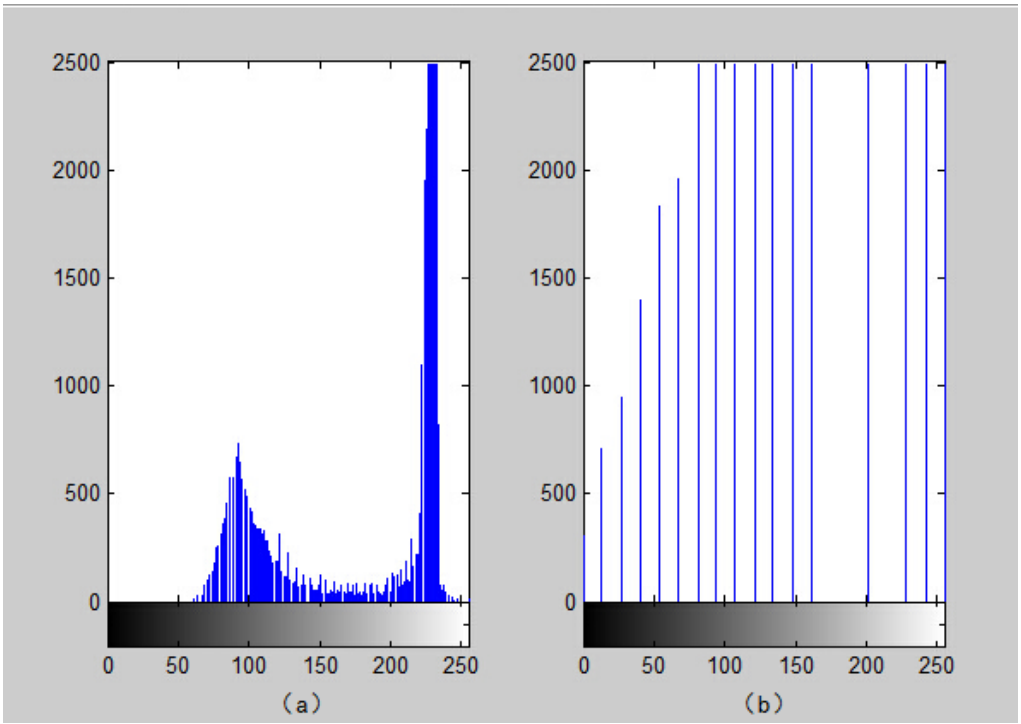

Figure 4. Analyze the Watermark Expansion

The watermark *Wa* is generated by m and pseudo random sequence *Sq* which m and *Sq* are generated by the gauss normal distribution sequence G1 and G2. Those illustrate that the watermark greatly enhances the ability to resist more copies of joint strikes. We can ensure the security of digital works when W applies to TSA for the time stamp. The reason is that W scrambles the binary bit sequence of *W1** and selects bit blocks according to the pseudo random sequence *Sq2*. TSA scrambles *T* and *R* to generate *T**.And *T** do not have dominant characteristics of *T*, which ensure the safety of the time stamp. Data transfer between W and the TSA is transmitted through their own private and other public key encryption. Due to the uniqueness of the private key characteristics, this guarantees the safety of the identification.

5. Conclusion

With the development of multimedia information, digital watermarking is widely used to protect digital products. Digital watermarking often encounter interpretation attack. In this paper, we analyze the actuality of digital watermarking, characteristics of pseudorandom sequence and time stamp protocol. We find defects of the timestamp in the existing digital watermarking protocol. Then, we put forward a new design based on pseudo random sequence and time stamp. The experimental results show that watermark, generated by the new design, is difficult to fake and indistinguishability. Therefore, this watermark can play an important role in network forensics. We will research how to further reduce the computation complexity of the watermark generation, and improve indistinguishability of watermark in the digital products.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant No.61272038 and No.61340059, Academician workstation funded projects (No.131PYSGZ202), the Education Department of Henan Province Science and Technology Research Project (12B520069) and Key Project of Science and Technology Research (13A520363), the Doctor Fund of Zhengzhou University of Light Industry (2010BSJJ005).

References

[1] L. Chia-Chen, C. Chin-Chen and C. Yi-Hui, "A novel SVD-based watermarking scheme for protecting rightful ownership of digital images", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 5, (**2014**).
[2] F. Hai, Z. Quan and L. Kaijia, "Robust watermarking scheme for multispectral images using discrete wavelet transform and tucker decomposition", Journal of Computers (Finland), vol. 11, no. 8, (**2014**).
[3] Q. Gu and T. Gao, "A novel reversible robust watermarking algorithm based on chaotic system", Digital Signal Processing: A Review Journal, vol. 1, no. 23, (**2013**).
[4] B. Abdelhamid, L. Lamri, N. Laurent and P. A. Christine, "New images watermarking scheme based on singular value decomposition", Journal of Hubei University for Nationalities (Natural Science Edition)", vol. 1, no. 4, (**2013**).
[5] D. P. Kumar and K. Jong-Myon, "Digital watermarking scheme based on fast Fourier transformation for audio copyright protection", International Journal of Security and its Applications, vol. 2, no. 5, (**2011**).
[6] Y. Chen, H. Cui, Y. Wang and L. Chen, "A semi-fragile watermarking algorithm for copyright protection and tamper localization of engineering graphics", Journal of Computer-Aided Design and Computer Graphics, vol. 8, no. 26, (**2014**).
[7] S. S. Sujatha and Mohamed Sathik M, "A novel DWT based blind watermarking for image authentication", International Journal of Network Security, vol. 4, no. 14, (**2012**).
[8] Y. Rui Research and application of pseudo-random sequence. Journal of Shenyang Engineering Institute (Natural Science), vol. 2, no. 5, (**2009**).
[9] S.-j. Luo, S.-s. Qiu and X. Chen, "A Way to Complexity Analysis of Chaotic Pseudorandom Sequence", Journal of South China University of Technology (Natural Science Edition), vol. 1, no. 38, (**2010**).
[10] C. Zhu and N. Ren, "An algorithm for digital watermark based on pseudo-random sequence and DCT for remote sensing image", Geomatics and Information Science of Wuhan University, vol. 12, no. 36, (**2011**).
[11] G. Oded, "Foundation of cryptography", Beijing: People's Posts and Telecommunications Press (**2003**).
[12] Z. Zhu, "A class of chaotic pseudorandom sequence generators based on dynamic S-box", Journal of Huazhong University of Science and Technology (Natural Science Edition), vol. 11, no. 38, (**2010**).
[13] H. Liu, Z. Zhang, J. Wen and F. Feng, "A DCT-Domain Zero-Watermark Scheme Based on Time Stamping. Computer Technology and Development", vol. 9, no. 19, (**2009**).
[14] H.-l. Pei, T. Shang and J.-w. Liu, "Secure network coding method merged with timestamp and homomorphic signature", Journal on Communications, vol. 4, no. 34, (**2013**).
[15] Q. Huang, Y.-d. Wang, J.-h. Han, Y.-d. Fan and D.-h. Li, "Timestamp Protocol Processing Based on Event Order", Computer Engineering, vol. 23, no. 36, **(2010).**

Authors

Yifeng Yin, he received his BS from ShenYang Ligong University, Shenyang, China, in 1993 and his MS and PhD from Xidian University, Xi'an, China, in 2001 and 2009, respectively. His PhD work focused on information security and cryptography. From 2006 to 2009, he worked for Key Laboratory of Computer Network and Information Security of Ministry of Education, Xidian University, China, as a researcher and developed the polymorphic cipher and researched its cryptographic properties for virtual S-box. He was a full-time professor with the School of Computer and Communication Engineering, Zhengzhou University of Light Industry since November, 2013. His current project deals with security Virtual S-box technologies for authentication service. As professional and academic activities, Dr. Yin is Chinese Association for Cryptogic Research (CACR) Member, China Computer Federation (CCF) Member and IEEE CS Member.

Heyu Wen, she received her bachelor's degree from Nanyang Institute of Technology in 2013. She is currently a Master Degree from Zhengzhou University of Light Industry. Her research interests include security Virtual S-box technologies for authentication service.

Kunpeng Fan, he received his bachelor's degree from ZHUHAI COLLEGE OF JILIN UNIVERSITY in 2012. He is currently a Master Degree from Zhengzhou University of Light Industry. His research interests include security Virtual S-box technologies for authentication service.