

Countermeasure of Public Key Attacks for Asymmetric Watermarking

JongWeon Kim*, De Li**(Corresponding author)

*Dept. of Copyright Protection at Sangmyung University, Korea

**Dept. of Computer at Yanbian University, China

jwkim@smu.ac.kr, leader1223@ybu.edu.cn

Abstract— In this paper, as a measure to respond to public key attacks that commonly occur in existing asymmetric watermarking systems, we propose a method to additionally generate and distribute public keys for the verification and detection of public key attacks. To configure an effective asymmetric watermarking system, public keys and private keys were generated based on a linear transformation method using special matrixes. The system was designed to be able to generate many public keys that can effectively detect correlations with the same private key when an attack has occurred, so that the system can effectively respond to public key attacks.

Based on the results of the experiments, the system was able to effectively detect correlations using public and private keys in images where watermarks had been inserted. In addition, it was found that the system could effectively detect correlations in images under public key attacks by using additionally issued public keys for verification.

Keywords— Private key & Public key, Correlation Detection, Asymmetric, Public key Attack

I. INTRODUCTION

With the occurrence of illegal reproduction and distribution of digital media, digital media copyright holders have become interested in technologies that can protect those copyrights. Among the technologies that can protect copyrights, watermarking technology is being actively studied and developed. This technology is a technique that inserts additional information for control and authentication into the original data subject to intellectual property rights protection, such as multimedia data and publications, which can be widely distributed and circulated on networks, in order to protect intellectual property rights over multimedia. In particular, since Steve Jobs of Apple Co. requested DRM-free service from record companies, demand for watermarking technology has been expanding further.

Most existing watermarking systems use symmetric key methods. Because these systems use the same keys for insertion and detection, verifiers can detect watermark information from detection devices and remove inserted watermark information. To respond to these attacks, asymmetric watermarking technology that uses different keys during insertion and detection of watermarks is necessary.

Similar to public key password systems, asymmetric watermarking methods are public key detection methods where the holders of copyrights over contents generate private keys and public keys, and use the private keys when inserting information and have verifiers use the public keys when detecting the information.

Various types of asymmetric watermarking methods have been proposed. Van Schyndel [1] implemented a method using the transformation of Legendre sequence, Choi [2] used a method using linear transformation, and Picard [3] proposed an asymmetric watermarking method using neural network functions. Smith [4] proposed a simple method that inserts the same watermark two times and detects the watermark by calculating the correlation between the two parts. Furon [5] implemented a method using a power density spectrum method, and Craver [6,7], Adelsbach [8,9] et al. proposed a method using cryptological protocols. In addition, safer asymmetric algorithms are being proposed, including the following: Chen [10] proposed a method that enables many watermarks to be detected by one detection key; Fu [11] and Gui [12] used a method that inserts owner and purchaser information into originals in the form of weighted sums and detects the information in asymmetric methods; and Tzeng [13] used a method to insert watermarks in certain decomposed spaces and detect watermarks with certain matrixes.

There are differences and similarities among these existing methods. However, most of them are accompanied by one drawback, in that they cannot appropriately respond to diverse attacks. In particular, they are defenselessly exposed to public key attacks. Therefore, in this paper, we propose a correlation-detection-based asymmetric watermarking method that is highly safe, has excellent public key detection performance, and can effectively respond to public key attacks.

II. PROPOSED ASYMMETRIC WATERMARKING SYSTEM

A. Configuration of private keys and public keys

Similar to public key password systems, the proposed asymmetric watermarking method is composed of private keys and public keys. S_r is a secret key, from which private and public keys are generated.

Private keys and public keys are configured as follows, using the secret key. Where U is a random generation matrix and Q is an orthogonal matrix generated by the decomposition of a random matrix,

$$S = QS_r \quad (1)$$

$$P = QU^tUS_r \quad (2)$$

The purpose of using orthogonal matrix Q is to increase the complexity of the calculation of private keys by using public keys to make attacks difficult. In calculating correlations, the characteristic that the transposed matrix of an orthogonal matrix is the same as an inverse matrix is used to enable effective correlation detection. Another reason to configure public keys and private keys is to enable the public key generator to easily generate additional public keys for verification by changing a random matrix U when a public key attack has occurred.

Watermarks are generated as shown in the following equation (3). Where m is insertion bit information that takes a value of $m \in \{-1, 1\}$, if m is -1 , it will mean that bit 1 will be inserted; and if m is 1, it will mean that bit 0 will be inserted. S is a private key generated in equation (1).

$$W = m \cdot S \quad (3)$$

$$I_i(w) = I_i + W_i \quad (4)$$

To insert a watermark, 1 bit of information is inserted into the information insertion block of $n \times n$, as shown in equation (4). I_i and $I_i(w)$ are the original block and the block where the watermark was inserted, respectively. W_i is a watermark signal to be inserted into an information insertion block.

B. Correlation detection using public keys

A process to calculate correlations with the general correlation equation using public key P and signal $I(w)$ where a watermark was inserted is as follows:

$$\begin{aligned} C &= P^t I(w) \\ &= (S_r^t U^t U Q) I + (S_r^t U^t U Q) N + m (S_r^t U^t U Q) Q S_r \\ &= (S_r^t U^t U Q) I + (S_r^t U^t U Q) N + m V^t V \end{aligned} \quad (5)$$

In the third term of equation (5), Q is offset using the characteristic that the transposed matrix of an orthogonal matrix is the same as an inverse matrix and, consequently, correlation $V = US_r$ appears. Because the original signal and the noise signal in the first and second terms, respectively, come to have very low correlations with the public key, their values are shown as relatively very small values compared to the third term, and whether a private key has been inserted can be judged only with the correlation value of V .

C. Public key attack analysis and countermeasure

When detecting the correlation of public keys, attacks using public keys will always exist. If public keys are deducted from signals where watermarks have been inserted in appropriate intensity, as shown in equation (6), negative public keys will reduce the correlation, so that watermarks will not be detected.

Where $I(w)'$ is the signal after public key attacks occurred and β is the intensity of the public key attacks,

$$C_{at} = P^t I(w)' = P^t (I(w) - \beta P) \ll P^t I(w) \quad (6)$$

If public key attacks succeed, the degree of distortion between the attacked signal and the signal before the attacks will be determined in order to assess the performance of the asymmetric method. Because the degree of deformation is not high at around 2~3dB in most methods, it can be said that these attacks are sufficiently possible.

As a countermeasure against public key attacks, there is a method to detect correlations with private keys. In this case, however, by the nature of asymmetric systems, private keys may not be delivered to verifiers for detection, but certifiers should receive the contents that have been attacked from verifiers, detect watermarks with private keys, and notify the results to verifiers. However, if the verification that must be performed by verifiers is performed by certifiers on behalf of verifiers, reliability problems may occur and, more importantly, the meaning of the asymmetric systems will be lost, and detection by the asymmetric systems will become little different from detection by symmetric systems.

Therefore, we propose a method for certifiers to additionally reissue public keys. When public key attacks have occurred, certifiers will additionally issue public key P_{VD} for verification and detection to verifiers, using equation (7), as follows:

$$P_{VD} = QU_{VD}^t U_{VD} S_r \quad (7)$$

In this equation, U_{VD} is a random matrix orthogonal to U that was used when public key P used in existing attacks was being generated, and Q and S_r are the orthogonal matrix and secret key used in generating secret key P , as they were. By doing this, P_{VD} is made to correlate with the existing private key so that the correlation can be easily detected. Equation (8) shows a process to detect correlations from the signal of the attack on P_{VD} by public key P . Where β is the attack intensity of P ,

$$C_V = (P_{VD})^t (I(w) - \beta P) = P_{VD}^t I(w) - \beta P_{VD}^t P \quad (8)$$

Because P_{VD} becomes correlated with both the private key and public key P , both the first term and second term of this equation generate correlation values. However, because the correlation between P_{VD} and P in the second term has a value smaller than the value of auto-correlations, and β is the attack intensity of P , these cannot reduce the entire correlation value generated in the first term. Therefore, C_V will still appear as some size of correlation value.

However, verifiers can attack again using the newly issued public key P_{VD} , similar to equation (8). In this case, the watermark can be detected again with the original public key P , as shown in equation (9).

$$C = (P)^t (I(w) - \beta_{VD} P_{VD}) = P^t I(w) - \beta_{VD} P^t P_{VD} \quad (9)$$

As such, the asymmetric watermarking key generation system proposed in this paper generates public key P_{VD} for

verification and sends it to verifiers so that the verifiers can effectively detect the watermark using P_{VD} or P .

III. EVALUATIONS

In the process of implementing this algorithm, a 512×512 standard image was used. In addition, in order to configure a method that is robust against compression, certain 8×8 DCT areas were selected in implementing the algorithm. A 128×128 size matrix was used as the information insertion block ($n \times n$), and 128×128 matrixes were also used for all keys used in this study, and matrix Q was generated through the decomposition of QR. Experiments were conducted on Lena images and, in the results, the PSNR of images where a watermark was inserted was shown to be 40.8dB. When no compression attack was made, high detection performance with clear peak values was shown.

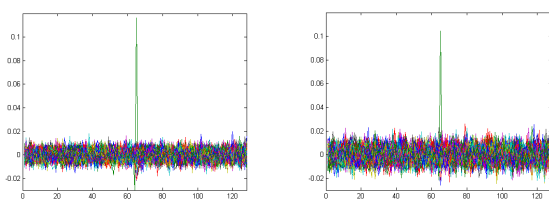


Figure 1. Correlation of Private and Public Keys in JPEG

Figure 1 shows the results of detection where the correlation values of private keys and public keys were normalized after JPEG compression. The left side shows the results of private key detection ($C_{\max}=0.1161$, $C_{\text{snd}}=0.0198$), and the right side shows the results of public key detection ($C_{\max}=0.1044$, $C_{\text{snd}}=0.0260$). $C_{\max}$ and C_{snd} are the largest value, that is, correlation Peak value, and a value that is next largest to the Peak value among correlation values, respectively. From these, it can be identified that the public key detection was accomplished effectively.

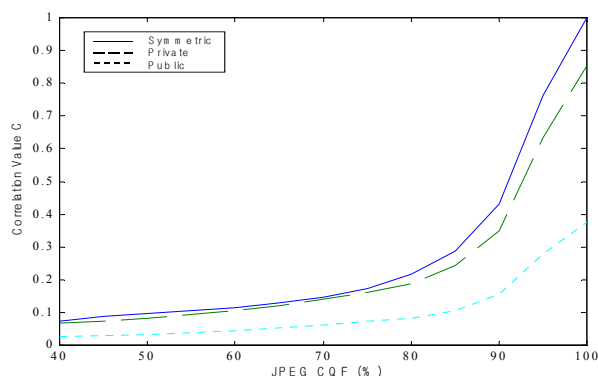


Figure 2. Detection Performance Comparison of Symmetric and Asymmetric system according to QF

Figure 2 shows the $C_{\max}$ of the secret key, private key, and public key in relation to the QF (Quality Factor) of JPEG compression to compare the detection performances of

symmetric and asymmetric watermarking systems in relation to the QF of JPEG compression. As can be seen here, the private key detection in the asymmetric method is close to the secret key detection in the symmetric method, while the public key detection shows a slightly lower value than the values shown by the secret key and private key detections.

TABLE 1. PUBLIC KEY DETECTION PERFORMANCE FOR COMPRESSIONS

Format	CV	Lena	Baboon	Peppers
BMP	C _{max}	0.983	0.997	0.989
	C _{snd}	0.044	0.075	0.061
JPG	C _{max}	0.049	0.178	0.062
	C _{snd}	0.019	0.065	0.038
J2K	C _{max}	0.298	0.419	0.372
	C _{snd}	0.035	0.057	0.044

Table 1 shows the detection performance of the public key by image in relation to image formats, including bmp, jpg, and jpeg2000. When comparing, using the values of differences between $C_{\max}$ and C_{snd} as detection performances, first, by image, in bmp formats, Lena images showed a slightly higher performance and, in jpg and j2k formats, Baboon images with a high ratio of high frequency content showed the highest detection performance. When comparing performances in relation to compression, it can be identified that bmp showed the highest detection performance, followed by j2k and jpg, in order. The jpg used QF=65% and CF (Compression Factor)=65%.

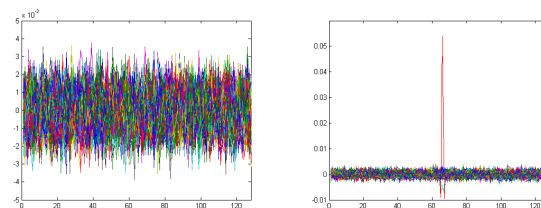


Figure 3. Correlation after Public Key Attack(BMP)

Figure 3 shows the results of attack experiments conducted on a BMP, where attacks were made with public key P and detection was conducted with additionally issued public key P_{VD} for verification. The left side shows that after being attacked with public key P , correlations could not be detected with P , and the β value used in the attack was $2.5e-4$. The right side shows the results of the detection ($C_{\max}=0.0539$, $C_{\text{snd}}=0.004$), where correlations were accurately detected with public key P_{VD} .

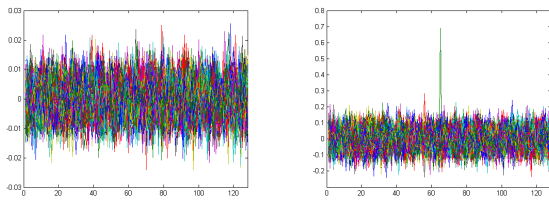


Figure 4. Correlation after Public Key Attack (JPG)

Figure 4 shows the results of attack experiments conducted on a JPG, where attacks were made with public key P and detection was conducted with additionally issued public key P_{VD} . The left side shows that after being attacked with public key P , correlations could not be detected with P , and the β value used in the attack was $2.8e-4$. The right side shows the results of the detection ($C_{max}=0.6899$, $C_{smd}=0.2836$), where correlations were accurately detected with public key P_{VD} . This proves that even when public key attacks were made in a state of JPEG compression, correlations could still be detected. QF=65% was used when the experiment was being conducted.

IV. CONCLUSIONS

In this paper, we proposed a correlation-detection-based asymmetric watermarking system that is highly stable and has excellent detection performance. Public keys and private keys were generated based on a linear transformation method using special matrixes so that private keys cannot be inferred from public keys, and the system was configured to be able to effectively detect correlations. In order to effectively respond to public key attacks that commonly occur in most existing asymmetric watermarking techniques, we proposed a system to additionally generate and distribute public keys for public key attack verification and detection, in order to enable effective responses to some public key attacks.

Based on the results of the experiments, it was identified that correlations could be effectively detected from images where watermarks had been inserted, and that the correlations could be effectively detected even after compression. It was also identified that correlations could be effectively detected from images that had been attacked with public keys by using additionally issued public keys for verification.

ACKNOWLEDGMENT

The Project Sponsored by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry.

REFERENCES

- [1] R. G. Van Schyndel, A. z. Tirkel, and I. D. Svalbe, "Key independent watermark detection," in Proc. of the IEEE Intl. Conf. on Multimedia Computing and Systems, vol. 1, pp. 580-584, Florence, Italy, June 1999.
- [2] H. Choi, K. Lee, and T. Kim, "Transformed-key asymmetric watermarking system," in Proc. of SPIE: Security and Watermarking of Multimedia Contents, vol. 4314, pp. 280-289, San Jose, USA, Jan. 2001.

- [3] J. Picard and A. Robert, "Neural Networks functions for public key watermarking," in Workshop on Information Hiding, pp. 142-156, Pittsburgh, PA, USA, Apr, 2001.
- [4] J. Smith and C. Dodge, "Development in steganography," in Workshop on Information Hiding, pp. 77-87, Dresden, Germany, Oct, 1999.
- [5] T. Furon and P. Duhamel, "An asymmetric public detection watermarking technique," in Workshop on Information Hiding, pp. 88-100, Dresden, Germany, Oct, 1999.
- [6] Craver S, Katzenbeisser S, "Copyright protection protocols based on asymmetric watermark: The ticket concept," in Proceedings of the 6th Conference on Communication and Multimedia Security (CMS'01), pp. 159-170, 2001.
- [7] Craver S, "Zero knowledge watermark detection," in International Workshop on Information Hiding (IHW'99), Lecture Notes in Computer Science 1768, pp. 101-116, 1999.
- [8] Adelsbach A, Sadeghi AR, "Zero-Knowledge watermark detection and proof of ownership," in International Workshop on Information Hiding (IHW'2001) Lecture Notes in Computer Science 2137, pp. 273-288, 2001.
- [9] Adelsbach A, Katzenbeisser S, Sadeghi AR, "Cryptography meets watermarking detecting watermarks with minimal or zero knowledge disclosure," in Proceedings of the European Signal Processing Conference (EUSIPCO'2002), Toulouse, France, September 3-6, 2002.
- [10] Kim T Y, Choi H, Lee K and Kim T. An asymmetric watermarking system with many embedding watermarks corresponding to one detection watermark [A]. IEEE Signal Process Lett, 11(3): 375-377, 2004.
- [11] Fu Y, Shen R, Shen L. A novel asymmetric watermarking scheme, Proceedings of the Third International Conference on Machine Learning and Cybernetics, Shanghai, August, 26-29, 2004.
- [12] Guo-fu Gui, Ling-ge Jiang and Chen He. General construction of asymmetric watermarking based on permutation. IEEE Int. Workshop VLSI Design & Video Tech. Suzhou, China, May 28-30, 260-263, 2005.
- [13] Tzeng J, Hwang W L, and Chen I L., An asymmetric subspace watermarking method for copyright protection, IEEE Trans. Signal Process, 53(2): 784-792, 2005.