A Transformation Scheme for Deriving Symmetric Watermarking Technique into Asymmetric Version

Rinaldi Munir[1] Bambang Riyanto[2] Sarwono Sutikno[3]

Wiseto P. Agung[4]

GJCST Computing Classification
I.4.5, G.0

***Abstract*-This paper proposes a transformation scheme for rendering the asymmetric watermarking technique into its asymmetric version. The asymmetric technique uses secret watermark as private key and public watermark as public key. The public watermark has a normal distribution and the private watermark is a linear combination of the public watermark and a secret sequence. The detection process is implemented by correlation test between the public watermark and the received image. The scheme is used to transform Barni Algorithm, a symmetric watermarking technique, into a asymmetric version. Experiments showed that the asymmetric technique was proved as robust as its symmetric version against some typical image processing schemes.**

Keywords- asymmetric watermarking, Barni Algorithm, transformation, correlation.

I. Introduction

Digital watermarking has been used widely as a tool for protecting copyright of digital multimedia data (e.g images) [1, 2]. Many digital watermarking techniques for still images have been proposed [1-3]. The particular problem with the state-of-the-art watermarking techniques is that the majority of these schemes are symmetric: watermark embedding and detection use the same key. The symmetric watermarking scheme has a security problem: once attacker knows the secret key, the watermark not only can be detected, but it can be easily estimated and removed from the multimedia data completely and thereby defeat the goal of copyright protection.

A solution to solve the problem is the asymmetric watermarking scheme, in which different key(s) are used for watermark embedding and detection. An asymmetric watermarking system uses the private key to embed a watermark and the public key to verify the watermark. Anybody who knows the public key could detect the watermark, but the private key cannot be deduced from the public key. Also, knowing the public key does not enable an attacker to remove the watermark [3].

Review of several existing asymmetric watermarking techniques can be found in [3]. The asymmetric techniques proposed until now can be classified into two categories [8]. The first category is watermark-characteristics-based-method where the watermark is the signals which have special characteristics such as periodicity. The other is transform-based-method to make a public key from a given private key by a proper transform. Legendre-sequence-key et al. [5] belong to the first category, whereas Hartung and Girod's [6] and Gui [7] techniques belong to the second category.

Many symmetric watermarking techniques have been proposed and some of them have good results in robustness and imperceptibility. Thus we have an idea to derive a symmetric watermarking technique into its asymmetric version, because designing a new asymmetric watermarking technique may need intensive effort and time. In this paper, we contribute to propose a transformation scheme which can be used to derive the symmetric technique into its asymmetric version. We choose a classical symmetric watermarking technique which has good robustness and imperceptibility, i.e. Barni Algorithm [9]. We use the scheme to derive an asymmetric version of Barni Algorithm

II. Proposed Scheme

In several symmetric techniques, the secret key is the watermarks itself where they have the normal distribution. In asymmetric version of the symmetric technique, the private key and the public key is referred as the private watermark (Ws) and the public watermark (Wp) respectively. The public watermark should have a correlation with the private watermark, because the detection is implemented by using correlation test between the public watermark and the received image.

In our scheme we map the symmetry method into the asymmetry version. Based on the compatibility between symmetric and asymmetric watermarking method, then in the mapping no change in the watermark embedding algorithm. Watermark embedding on the asymmetric version is same as the original method (symmetric), but watermark detection algorithm is a slight change. The change is in the reference watermark used in correlation test. In the symmetric method correlation test performed between the received image and original watermark, then in the asymmetry version correlation test is performed by the received image and the public watermark

A new process added to the mapping is a transformation of a private watermark to produce a public watermark. The public watermark W_p is generated by the transformation f to the private watermark W_s,

$$W_p = f(W_s) \qquad (1)$$

Fig.1 shows the transformation diagrams. The transformation f is a one-way function, so that

About-[1,2,3] Rinaldi Munir, Bambang Riyanto, Sarwono Sutikno (School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia).(e-mail;rinaldi-m@stei.itb.ac.id[1],briyanto@lskk.ee.itb.ac.id[2] ssarwono@gmail.com[3]

About-[4] PT.Telekomunikasi,Indonesia(e-mail; wiseto@telkom.co.id)

computationally almost impossible to derive private watermark from the corresponding public watermark. One-

process of transformation the symmetric watermarking method into its asymmetric version.

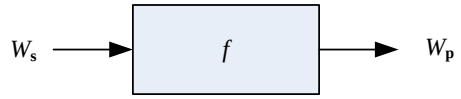


Fig. 1. Transformation of the private watermark to the public watermark

We design both of watermarks to have normal distribution, as the choice of this distribution gives resilient performance against collusion attack [1]. We use a concept in statistics to design a function *f*.

In statistics, if we add two or more random variables as a linear combination where each of them has normal distribution, then the result has normal distribution too. Let X be a sequence with mean μ_1 and variance σ_1^2 and Y be sequence that independent from X with mean μ_2 and variance σ_2^2. A combination linear of X and Y is defined as $Z = aX + bY$ where a and b is parameters. Sequence Z has the mean $\mu_3 = a\mu_1 + b\mu_2$ and variance $\sigma_3^2 = a^2\sigma_1^2 + b^2\sigma_2^2$ [10].

In generating the watermarks we have to ensure that the combination linear is secure. It means that the private watermark cannot be deduced from the public watermark. Furthermore, knowing the public watermark does not enable a user to remove the embedded watermark from the watermarked image. This characteristic is realized by adding the public watermark with a secret sequence. Security of this asymmetric version depend on the secret sequence. Let W_p be the public watermark and R be the secret sequence, the private watermark can be obtained by adding W_p and R as

$$W_s = f(W_p, R) = \beta_0 W_p + \beta_1 R \qquad (2)$$

where β_i is a parameter in [0, 1] to control the trade off between the two sequences and $\beta_0 + \beta_1 = 1$. In order to make the sequence R is more secure, we encrypt R by a random permutation before adding with W_p. Thus, eq. (2) can be written as

$$W_s = f(W_p, R) = \beta_0 W_p + \beta_1 \tilde{R} \qquad (3)$$

where $\tilde{R}$ is encrypted version of R. Fig. 2 shows the process of generating the public and the private watermark.

The private watermark W_s is embedded into the image according to the equation used by its symmetric technique. In the detector side, using the public watermark, W_p, the test correlation is computed to accomplish the watermark detection.

way nature of this property is important to provide security on asymmetric watermarking method. The Function f is core

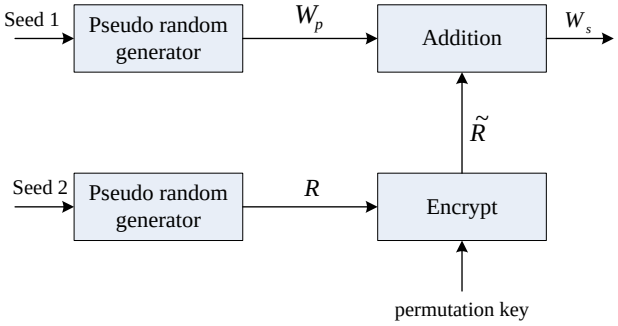


Fig. 2. Generating of the public and the private watermark

III. Security Analysis

Because of the public watermark, detector, and watermarked image are publicly available (not secret), the attacker uses the public information to deduce the private watermark W_s. Such attacks are called public attack. Once W_s can be calculated, then W_s is removed from the watermarked image by performing a subtraction operation on watermark embedding formula (depending on methods).

Security of this transformation scheme is based on two factors as follows:

A. One-way function

One-way functions are commonly used in cryptography to enhance system security. In the one-way function, computing to evaluate function value of the variables is relatively easy, but to discover variables value of the function value is relatively computationally difficult and even impossible. In Eq. (3) parameter R can be viewed as trapdoor, it is impossible to find Ws without knowing the trapdoor, because the attackers must do the inversion of the one-way function. The attacker knows Wp but he (or she) does not know R. Because of $\tilde{R}$ is an encrypted version of R, the attacker must know the R before getting $\tilde{R}$.

B. Permutation

Let the attacker knows R, next he (or she) needs to know a random permutation used to encrypt R. Because cardinality of R is n, the attacker must try $n!$ permutation to find the right one. Remember that n is large enough, it is about 25% of original image size, so that finding the right permutation needs $O(n!)$ computation. For n = 10000 as example, there are 10000! computation. We conclude that it is impossible for attackers to deduce the private watermark from these public information.

IV. Case Study: Transformation of Barni Algorithm

In this section we present derivation of a symmetric watermarking method into the asymmetric version based on transformation scheme which has been described in Section

II. The symmetric watermarking method is a classic method, i.e Barni Algorithm.

In Barni Algorithm, the watermark consists of a pseudo random sequence of M real number, $W = \{w(1), w(2), ..., w(n)\}$, that has a normal distribution with *mean* = 0 and *variance* = 1. The watermark W is inserted into selected DCT coefficients, $V = \{v(1), v(2), ..., v(n)\}$. The watermark detection is done by computing correlation between the selected DCT coefficients from a possibly corrupted image I^*, i.e. $V^* = \{v^*(1), v^*(2), ..., v^*(n)\}$.

In the asymmetric version of Barni Algorithm, we use two watermarks, the first is a private watermark, $W_s = \{w_s(1), w_s(2), ..., w_s(M)\}$, that embedded into the host image and the second is a public watermark $W_p = \{w_p(1), w_p(2), ..., w_p(n)\}$, for detection phase. Both of the watermarks are generated by the procedure explained in Section 2. The private watermark is embedded into the image according to formula:

$$v_w(i) = v(i) + \alpha \left| v(i) \right| w_s(i) \qquad (3)$$

In the detector side, using the public watermark, W_p, the following correlation is computed:

$$c = \frac{1}{n}\sum_{i=i}^{n} v^*(i) \cdot w_p(i) \qquad (4)$$

After we set the threshold T, the watermark detection is finished by comparing c and a threshold. The threshold is depend on the received image and calculated with following formula:

$$T = \frac{\alpha}{3n}\sum_{i=1}^{n}\left|v^*(i)\right| \qquad (5)$$

V. Simulation and Results

We apply our method to image watermarking by using MATLAB as programming tool. The test image is a 512 × 512 color image 'train'. Size of the private watermark is n = 16000. The watermark and the secret sequence R have a normal distribution with *mean* = 0 and *variance* = 1. The public watermark is generated by function f which has been explained in Section II with β_0 is equal to 0.8 and β_1 = 0.2. The embedding strength α is equal to 0.25. Histogram of the public watermark and the private watermark is shown in Fig. 3. From Fig. 2(b) we observe that shape of distribution graphics of the private watermark is like a bell as common standard normal distributions.

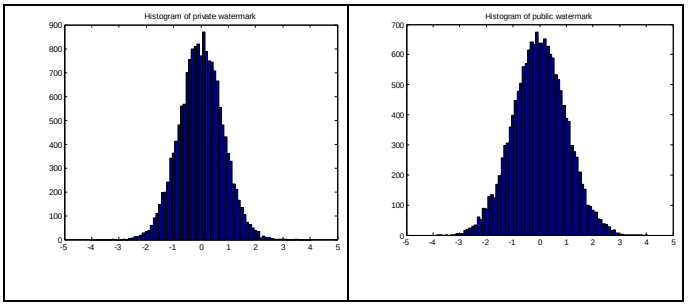
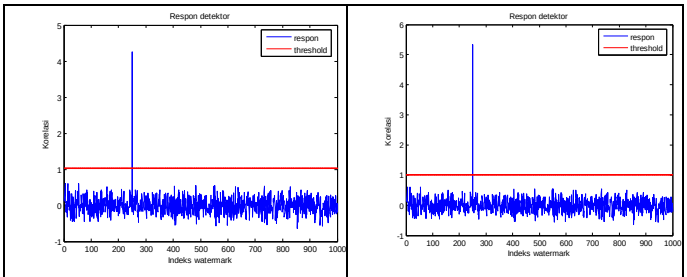


Fig.3. Histogram of the private and public watermark

Before embedding the private watermark, the original image is transformed from *RGB* to *YcbCr*. The watermark is embedded to luminance component (*Y*) only, and the final result is retransformed from *YcbCr* to *RGB*.

Figure 4(a) shows the original image and Figure 4(b) shows the watermarked image (PSNR = 36.9833). Visually the watermarked image quality was almost identical with the original image. Figure 4(c) shows response of a public detector to 1000 random watermarks, one of them (index 250) is a public watermark that have a correlation with the private watermark. Such images provide two interpretations [9]. The first interpretation, the response to the public watermark is compared with the T to decide the existence of the (private) watermark within the image. The second interpretation, if people do not know which watermark is embedded in the image, then response from all the public watermark is compared and the highest response is selected. Response from the public watermark is should be the highest compared with the others and this suggests the existence of a corresponding private watermark in the image.

(a) Original image (b) Watermarked image



(c) Response of public detection (c) Response of private detection

Fig. 4. Output of watermark embedding and detection on 'train' image .

Figure 4(c) shows that the correlation test with the correct public watermark correlation value is significantly higher than the other. The threshold T is calculated analytically from equation (5) is 1.0188. In case there is no attack on the watermarked image, the detector gives the value c = 4.2512. Because c > T, it can be concluded that the image contains the (private) watermark. For comparison, in private

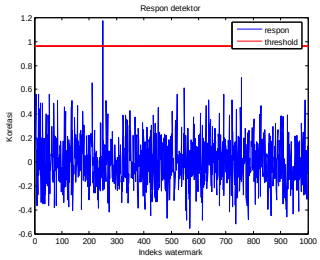
detection (using the private watermark on correlation test) gives c = 5.3251 (Fig. 4(d)).

The next experiment was done to see robustness of the watermark against some non-malicious attacks, which is the general operations performed on image processing (cropping, compression, low-pass filtering, etc.). We use Jasc Paint Shop version 6.01 as image processing software. The experiments and results are explained as follows.

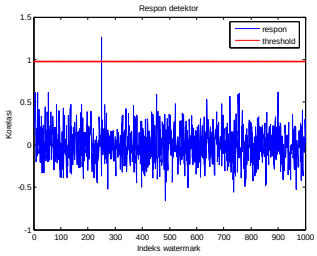
V.1. Experiment 1: JPEG Compression

We tested the robustness against JPEG compression with extreme compression qualitie. For compression quality 6%, the watermark can be detected succesfully (c = 1.1727, T = 0.9602). For comparison, in private detection (using the private watermark) gives c = 1.4632). See Fig. 5

(a) JPEG image with low compression quality



(b) Response of public detection

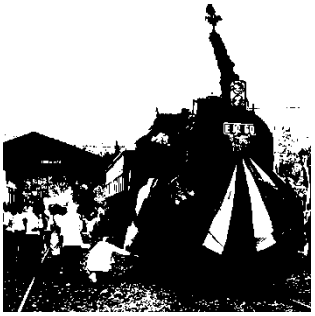


(c) Response of private detection

Fig 5. JPEG compression with compression quality 6%. The watermark can be detected

V.2 Experiment 2: Dithering

We convert the watermarked image to a binary image by dithering operation. It means plenty of gray-level information lost. It is shown in Fig. 6 that the watermark still can be detected. The response to the right watermark is largest among the response to all the watermarks (c = 3.4352, T = 2.4982).



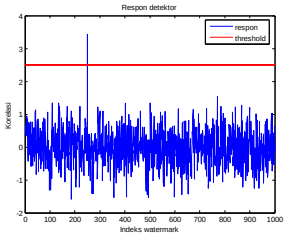


Fig. 6. (a) Dithering. (b) Response of public detector

V.3. Experiment 2: Image Cropping

Image cropping will remove some watermark information. In our simulation, we cut unimportant part from the watermarked image (about 50%), the missing part of the image is replaced with black pixels (see Figure 7a). In fact, we can always correctly detect the watermark because the correlation value (c = 2.1752, T = 0.8579) is still greater significantly than the others. For comparison, in private detection gives c = 2.7349.

(a) Cropped image

(b) Image after histogram equalization

Fig. 7. Image cropping and histogram equalization

V.4. Experiment 4: Histogram Equalization

The watermarked image is adjusted so that distribution of gray-level is uniform by using histogram equalization operation (a typical low-pass filtering operation, see Fig. 7(b)). Experiment shows that the watermark can be detected where c = 6.4877, T = 1.2269. For comparison, in in private detection gives c = 8.1186.

V.5. Experiment 5: Resizing

The watermarked image is resized until 50% of the original size. Experiment shows that the watermark still can be detected. For resizing up to 200% of the original image, the watermark still can be detected well (we found that c = 1.8030, T = 0.4520). For comparison, in in private detection gives c = 2.2571

VI. Discussion

Based on a series of experiments that have been done for asymmetric version of Barni algorithm, it has achieved some results which are analyzed as follows.

A series of experimental results show that the asymmetric

version remains robust to typical image processing operations like JPEG compression, histogram equalization, dithering, cropping, and resizeng. Detector response of asymmetric method is not much different to original symmetric version, and correlation values yielded by detector not differ significantly

VII. Conclusion

In this paper a scheme for deriving a symmetric watermarking technique into its asymmetric technique has been proposed. For test case, Barni algorithm, a classical image watermarking, is successfully transformed into an asymmetric watermarking technique. This technique uses two watermarks: the first watermark is a public watermark used for public detection, and the second watermark is a private watermark that has a correlation to the public watermark. The private watermark is a linear combination of the public watermark and an encrypted version of a secret sequence. Security of this asymmetric technique is based on one-way function with trapdoor and the difficulty of finding the secret sequence where it needs O(n!) computation. Simulations against various attacks confirmed that this asymmetric technique is as robust as its symmetric version

VIII. References

1) Ingemar J. Cox, et al, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. On Image Processing, Vol. 6, No. 12, Dec 1997, pp.1673-1687.
2) Mauro Barni, Franco Bartolini, Watermarking Systems Engineering, Marcel Dekker Publishing, 2004.
3) Joachim J. Eggers, Jonathan K. Su, and Bernd Girod, Asymmetric Watermarking Schemes, GMD Jahrestagung, Proceedings, Springer-Verlag, 2000.
4) R.G. Schyndel, A.Z.,Tirkel, I.B. Svalbe, (1999): "Key Independent Watermark Detection", in Proceeding of the IEEE Intl. Conference on Multimedia Computing and Systems, volume 1, Florence, Italy.
5) J.J. Eggers, J.J., J.K. Su, B. Girod (2000): "Public Key Watermarking by Eigenvectors of Linear Transform", EUSIPCO 2000.
6) F. Hartung, F. and B. Girod (1997): "Fast Public-Key Watermarking of Compressed Video", Proceedings of the 1997 International. Conference on Image Processing (ICIP).
7) Guo-fu Gui, Ling-ge Jiang, and Chen He, "A New Asymmetric Watermarking Scheme for Copyright Protection" IECE Trans, Fundamentals Vol. E89-A, No 2 February 2006.
8) Geun-Sil Song, Mi-Ae-Kim, and Won-Hyung Lee, "Asymmetric Watermarking Scheme Using Permutation Braids", Springer-Verlag, 2004.
9) Mauro Barni, F. Bartolini, V. Cappellini, A.Piva, "A DCT-Domain System for Robust Image Watermarking", Signal Processing 66, pp 357-372, 1998.
10) Walpole, Ronald E., Myers, Raymond H., (1995), Probability and Statistics for Engineers and Scientists, Mc. Graw-Hill, 1995