A New Copyright- and Privacy-Protected Image Trading System Using a Novel Steganography-Based Visual Encryption Scheme

Wannida Sae-Tang[*†], **Masaaki Fujiyoshi**[**1], and **Hitoshi Kiya**[**2], Non-members

ABSTRACT

In copyright- and privacy-protected image trading systems, the image sent to the trusted third party (TTP) is visually encrypted, and the image is traditionally unrecognizable. The image, however, is suspicious and has a possibility to be attacked. Image steganography then becomes more interesting than image encryption for this application; however, applying image steganography instead of image encryption degrades the fingerprint extraction performance. In addition, the content provider (CP) is allowed to directly contact with the consumer in the conventional systems. Thus, the consumer's privacy is not protected completely. This paper proposes a new copyright- and privacy-protected image trading system with a novel steganography-based visual encryption scheme, where the scheme protects a commercial image much more securely by generating a recognizable image instead of a suspicious encrypted image. By replacing amplitude components of a dummy image by those of a commercial image, the output image looks like a degraded dummy image instead of the commercial image, while it contains some details of the commercial image, i.e., the amplitude components of the commercial image are hidden in a dummy cover image. A discrete cosine transform-based fingerprinting method, which is compatible with the proposed amplitude component replacing scheme, is also proposed in this paper to solve the problem of applying image steganography. As another contribution of this paper, the CP is not allowed to directly send the image reconstruction key to the consumer, to increase consumer's privacy protection. The second TTP is then introduced to the proposed system, and in addition, the image reconstruction key is encrypted by the CP before being sent to the consumer via the second TTP for more security. Experimental results show that the proposed scheme generates recognizable images and perfectly visually encrypts the commercial images. It also achieves much higher reconstructed image qualities than those of the conventional scheme, and the proposed system simultaneously enhances the fingerprinting performance using the proposed compatible fingerprinting method.

Keywords: Image Encryption, Image Steganography, Data Hiding, Privacy Protection, Image Copyright Protection.

1. INTRODUCTION

Nowadays, online trading is very popular. Almost everything could be sold via the Internet including digital media. Copyright protection and privacy protection are very important for such kinds of goods. In image trading systems, a commercial image is always copyright-protected before being sold [1–3]. Moreover, consumers also need privacy protection. In the systems [4–13], a commercial image is copyright-protected by a trusted third party (TTP) instead of a content provider (CP). The purpose of introducing the TTP to the system is for consumer's privacy protection against the CP. As well, for consumer's privacy protection, the TTP does not need to recognize the commercial image. The CP, therefore, encrypts the commercial image before sending it to the TTP. The copyright protected image is then transmitted from the TTP to the consumer simultaneously with sending the decryption key from the CP to the consumer for image reconstruction. As a result, the commercial image which is reconstructed by the consumer is copyright protected, and the consumer's privacy is protected against both the CP and the TTP. In addition, besides considering the CP and the TTP, there is possibility that malicious third parties attack/steal the image from the TTP. In this case, encryption also protects the image from the malicious third parties.

Though the images sent to the TTP are perfectly visually encrypted in the conventional systems, from another point of view, the encrypted images are suspicious, and there is possibility to be attacked. It is better if the image treated by the TTP seems to be recognizable. The malicious third party may believe that it is just a general image and does not try to attack the image. From the above reason, an image steganography technique [14, 15] becomes more interesting than image encryption for this application. In image steganography, the hidden message can be an image, text, voice, or other media, while the cover

Manuscript received on January 4, 2019 ; revised on February 27, 2019.

*The author is with The Sirindhorn International Thai-German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, E-mail : wannida.s@tggs.kmutnb.ac.th

**The authors are with Tokyo Metropolitan University, Japan, E-mail : fujiyoshi-masaaki@tmu.ac.jp[1], kiya@tmu.ac.jp[2]

†Corresponding author.

image is modified in some way to embed that information. The cover image after hiding the information is called as "stego-image." In the focused application, the hidden message is desired to be an image (a commercial image). Hiding a high quality image, not just a binary message or a smaller image, into another image of the same size is not an easy task. The cover image quality might be degraded by the steganography process. B. Shumeet [16] proposed an image steganography method which applies deep learning to hide a color image into another image of the same size. In a similar application, a secret message is often firstly encrypted by some traditional encryption methods, and then a cover image is modified in some way to contain the encrypted message. However, in the focused copyright- and privacy-protected image trading system application, it is not expected that the commercial image is encrypted in the steganography process, because the consumer ID must be subsequently embedded to the stego-image for copyright protection, and the fingerprint should still exist in the image reconstructed by the consumer. It should not be destroyed by the decryption process. Moreover, applying image steganography instead of image encryption degrades the fingerprint extraction performance, because when the image is reconstructed by the consumer, the cover image which contains the embedded fingerprint is separated from the hidden image and then discarded. Thus, the challenging problem is how to hide a high quality commercial image into a dummy image of the same size while keeping/enhancing the fingerprinting performance.

This paper, therefore, proposes a novel steganography-based visual encryption scheme for copyright- and privacy-protected image trading systems. In the scheme, the amplitude components of a dummy image are replaced by those of a commercial image. To support the idea, there is evidence which explains that discrete cosine transformed (DCTed) signs/discrete Fourier transformed (DFTed) phases generally contain important information of images [17], and they were used for image recognition [18–21], delay estimation [22], image registration [23, 24], inpainting [25], and image matching [26, 27]. Without DCTed sign/DFTed phase components, the amplitude components do not contain any comprehensive information of the original image. In contrast, after losing the amplitude information, the image is still recognizable with a lower quality (degraded), and when the phase/sign components are combined with the amplitude components of another image, the image is also recognizable with a lower quality. For this reason, the image generated by the proposed scheme looks like a degraded dummy image and is considered as a "stego-image." From the steganography perspective, the dummy image is considered as the cover image, and the amplitude components of the commercial image are considered as a secret message. This image is sent to the TTP for image copyright protection. Thus, the consumer's privacy is stronger protected against malicious third parties, because the malicious third parties recognize the image as the dummy image instead of the commercial image. It should be noted that even though the amplitudes of the dummy image are discarded, the DCTed signs of the commercial image are important for image reconstruction at the consumer side, and it is referred to as the image reconstruction key. As another contribution of this paper, a new copyright- and privacy-protected image trading system is proposed to further increase consumer's privacy protection. In the proposed system, the CP is not allowed to send the image reconstruction key to the consumer directly, whereas the conventional systems allow the CP to identify the consumer for sending the image reconstruction key to the consumer. The second TTP is then introduced to the proposed system, and simultaneously, the image reconstruction key is encrypted by the CP before being sent to the consumer via the second TTP. This encryption process protects the consumer's privacy against the malicious third parties, in a manner similar to the encryption process in the conventional systems. Though the encrypted image has a possibility to be attacked as in the conventional systems, the decrypted image in the proposed system is different from that in the conventional systems, i.e., it is just a DCTed signs and even if the inverse discrete cosine transform (IDCT) is performed, the output image is just a degraded version of the commercial image, which is at least valueless in business, while the decrypted image in the conventional systems is the original commercial image itself. In conclusion, the proposed system with the second TTP and the encryption of an image reconstruction key offers better security, because: 1) the consumer is completely anonymous for the CP; and 2) it provides encryption for the image reconstruction key for more security. Moreover, in the proposed system, after the DCTed signs of the dummy image are discarded in the image reconstruction process, the fingerprint can be kept perfectly and is easy to be extracted by combining the proposed DCTed amplitude component replacing scheme with a proposed compatible discrete cosine transform (DCT)-based fingerprinting method which does not modify the DCTed signs. Only the amplitude components are modified by the fingerprinting method as described in Section 3.3.

The rest of this paper is organized as follows. Section 2 describes conventional copyright- and privacy-protected image trading systems and provides requirements for the systems. Section 3 describes the proposed amplitude component replacing scheme, the proposed system, and the proposed fingerprinting method. Experimental results and discussions are given in Section 4. Finally, Section 5 concludes this paper.

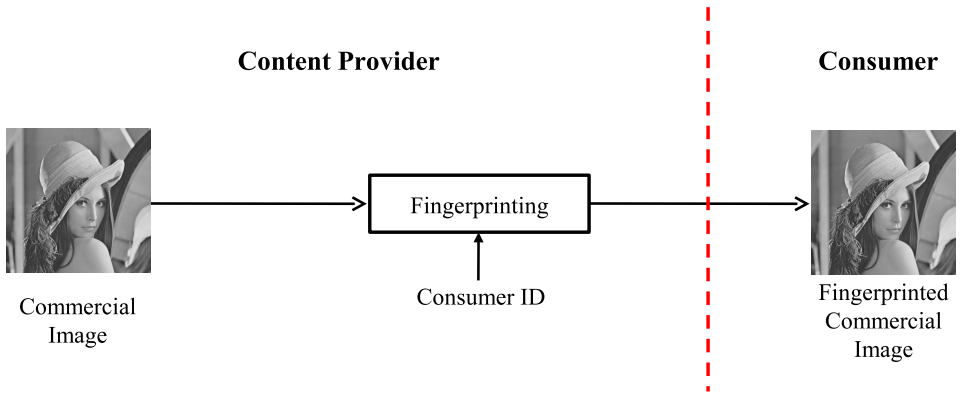


Fig. 1: *Copyright-protected image trading systems [1–3].*

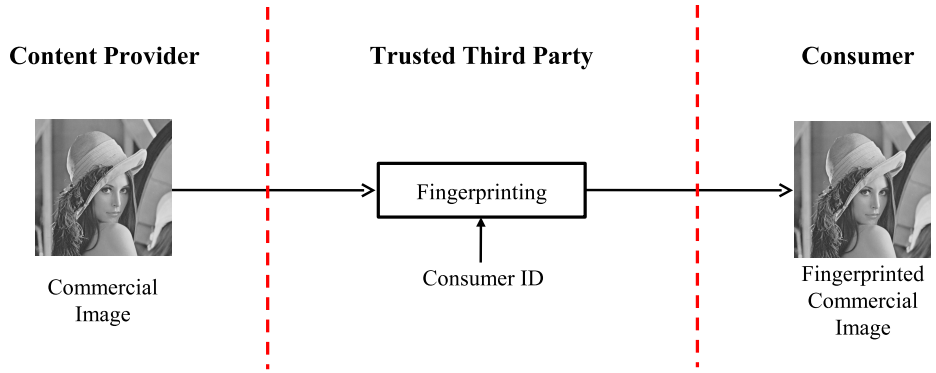


Fig. 2: *Copyright- and privacy-protected image trading systems with trusted third parties [4–13].*

2. CONVENTIONAL COPYRIGHT- AND PRIVACY-PROTECTED IMAGE TRADING SYSTEMS AND REQUIREMENTS

This section describes conventional copyright- and privacy-protected image trading systems and requirements for the systems.

2.1 Conventional Copyright- and Privacy-Protected Image Trading Systems

In copyright-protected image trading systems [1–3], the consumer ID is embedded into the original commercial image by the CP using a fingerprinting technique as shown in Fig. 1. This kind of system is simple, but the consumer's privacy is not protected. The CP knows the consumer's information and also knows the image which he/she buys. To solve the problem, a TTP was introduced to the image trading systems [4–13]. In such systems, the TTP is responsible for image copyright protection instead of the CP as shown in Fig. 2. The original commercial image is sent from the CP to the TTP. Then, the TTP embeds the consumer ID to the image using a digital fingerprinting technique before sending the image to the consumer. In this kind of image trading system, the CP does not get the consumer's information, therefore, the consumer's privacy is protected against the CP. However, the consumer's information could be unintentionally leaked at the TTP instead. To solve the problem, the CP should visually protect the commercial image before sending it to the TTP. To protect the visual of the image, the original image is divided into two parts in [7]. One part is sent directly from the CP to the consumer, while the other is sent to the TTP for fingerprinting before being sent to the consumer. Both images are unrecognizable. The consumer then composes the images to obtain the fingerprinted commercial image with privacy protection. However, the image sent to the TTP reveals some details of the commercial image. It is not perfectly visually protected and looks suspicious. Moreover, the amount of the fingerprint which can be embedded into the image is about only one half of that for the original image.

The scheme called "amplitude-only image (AOI)" was proposed to solve the problem [8]. Firstly, the original image is transformed using discrete Fourier transform (DFT). Then, the amplitude components and phase components are extracted. Inverse DFT (IDFT) is applied to amplitude components and phase components independently to obtain the AOI and phase-only image (POI), respectively. The AOI is naturally visually protected, while the POI reveals the original image. The AOI, therefore, plays a key role in consumer's privacy protection and copyright protection.

Anyway, there is much research on the image trading systems using AOIs [8–12]. DCT-based AOI [10] and Hadamard transform-based AOI [12] were also proposed. Moreover, one dimensional (1D) transformation of each transform was evaluated [10]. Finally, it was concluded that the 1D DCTed AOI method [10, 11] is the best among various types of the AOIs in several aspects, i.e., reconstructed image quality, fingerprinting performance, and memory cost and complexity. This paper, therefore, considers the 1D DCTed AOI [10] as a conventional method to be compared. To generate the 1D DCTed AOI, the $X \times Y$-pixel commercial image, $f(x, y)$, is transformed using 1D DCT as described by Eq. (1).

$$F_c(x, v) = \alpha(v) \sum_{y=0}^{Y-1} f(x, y) \cos\left(\frac{\pi}{Y}\left(y + \frac{1}{2}\right) v\right) \tag{1}$$

Here, $F_c(x, v)$ be the $X \times Y$-sized column-wise 1D DCTed coefficients of the commercial image $f(x, y)$, where $x = 0,\ 1,\ 2,\ \ldots,\ X-1,\ y = 0,\ 1,\ 2,\ \ldots,\ Y-1,\ v = 0,\ 1,\ 2,\ \ldots,\ Y-1$, and

$$\alpha(v) = \begin{cases} \sqrt{\frac{1}{Y}}, v = 0 \\ \sqrt{\frac{2}{Y}}, v = 1, 2, \ldots, Y-1 \end{cases} \tag{2}$$

The coefficients, $F_c(x, v)$, can also be expressed in the polar form as

$$F_c(x, v) = |F_c(x, v)|\, S_c(x, v) \tag{3}$$

where $|F_c(x, v)|$ and $S_c(x, v)$ denote the amplitude and the sign components of $F_c(x, v)$, respectively. To generate the AOI, the amplitude components, $|F_c(x, v)|$, is inversely transformed as

$$\mathrm{AOI}(x, y) = \sum_{v=0}^{Y-1} \alpha(v)\, |F_c(x, v)| \cos\left(\frac{\pi}{Y}\left(y + \frac{1}{2}\right) v\right) \tag{4}$$

where $\mathrm{AOI}(x, y)$ denotes the AOI. The AOI generated by the CP is sent to the TTP for fingerprinting. Then, the fingerprinted AOI, $\mathrm{AOI}_{fp}(x, y)$, is sent to the consumer. The consumer performs the 1D DCT to the fingerprinted AOI to obtain amplitude components including fingerprints, $|F_{fp}(x, v)|$. Finally, the consumer combines $|F_{fp}(x, v)|$ with the DCTed sign components, $S_c(x, v)$, received from the CP, and applies the 1D IDCT to the combined components to obtain the fingerprinted commercial image, $f_{fp}(x, y)$.

Besides the AOI schemes, other image encryption schemes [13] could be applied to the copyright- and privacy-protected image trading system. However, those schemes generate encrypted images which are unrecognizable and suspicious. In this paper, the image sent to the TTP is desired to be recognizable, and it becomes the most important requirement for copyright- and privacy-protected image trading systems as described in Section 2.2.

2.2 Requirements for Copyright- and Privacy-Protected Image Trading Systems

As mentioned above, another requirement for the copyright- and privacy-protected image trading systems is added. The requirements for the systems are then concluded as follows.

1. Visual encryption: The image sent to the TTP should not reveal the commercial image. The TTP and the malicious third parties should not be able to recognize the commercial image even some details of the image.
2. Recognizability: The image sent to the TTP should be meaningful or recognizable for protecting the image from suspicion.
3. Reconstructed image quality: The quality of the reconstructed commercial image at the consumer side is desired to be as high as that of the original commercial image.
4. Fingerprinting performance: The fingerprinting performance which is evaluated by the correct fingerprint extracting rate is desired to be high to protect the copyright of the commercial image.

3. PROPOSED SCHEME AND SYSTEM

Since the conventional schemes mentioned in Section 2.1 do not meet the second requirement, this section proposes an amplitude component replacing scheme to generate a meaningful image simultaneously with protecting the visual of the commercial image. In addition, a compatible fingerprinting method is proposed to solve the problem of applying image steganography to the focused application. Moreover, this section also proposes a new system with a second TTP.

3.1 Proposed Amplitude Component Replacing Scheme

Similar to the conventional schemes, a commercial image is divided into two parts by the proposed scheme using the DCT; the amplitude components and the sign components. Differently from the conventional schemes, a dummy image is needed in the proposed scheme. The DCTed amplitude components of the dummy image are subsequently replaced by those of the commercial image. Firstly, the $X \times Y$-sized commercial image, $f(x, y)$, is transformed by using two dimensional (2D) DCT as described by Eq. (5).

$$F(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{X-1} \sum_{y=0}^{Y-1} \left[f(x,y) \cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right) \cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right) \right] \quad (5)$$

where $F(u,v)$ denotes the 2D DCTed coefficients of the image, $f(x,y)$,

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{X}}, u = 0 \\ \sqrt{\frac{2}{X}}, u = 1,2,\ldots,X-1 \end{cases} \quad (6)$$

and

$$\alpha(v) = \begin{cases} \sqrt{\frac{1}{Y}}, v = 0 \\ \sqrt{\frac{2}{Y}}, v = 1,2,\ldots,Y-1 \end{cases} \quad (7)$$

$F(u,v)$ can also be expressed in the polar form as

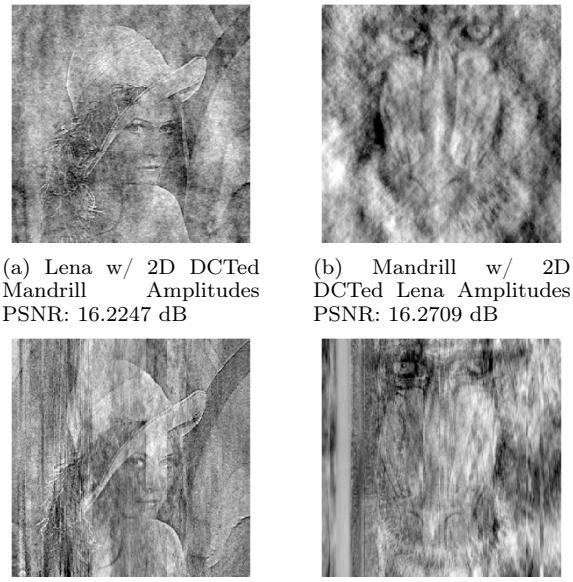
$$F(u,v) = |F(x,v)|\, S(x,v) \quad (8)$$

where $|F(x,v)|$ and $S(x,v)$ denote the amplitude components and the sign components, respectively. In the same way, the dummy image, $f_d(x,y)$, is also transformed by using the 2D DCT to extract the DCTed signs, $|F(x,v)|$, are then combined with the DCTed signs of the dummy image, $S_d(u,v)$. Finally, the 2D IDCT is applied to obtain the stego-image, $f'_d(x,y)$, as described by Eq. (9).

$$f'_d(x,y) = \alpha(u)\alpha(v) \sum_{u=0}^{X-1} \sum_{v=0}^{Y-1} \left[|F(u,v)|\, |S_d(u,v) \cos\left(\frac{\pi}{X}\left(x+\frac{1}{2}\right)u\right) \cos\left(\frac{\pi}{Y}\left(y+\frac{1}{2}\right)v\right) \right] \quad (9)$$

Figs. 3(a) and (b) show the images with replaced 2D DCTed amplitude components for "Lena" and "Mandrill," respectively. The images show that interchanging amplitude components just degrades the qualities of the images, and they are still recognizable with about 16 dB PSNR. From this characteristic, we can utilize it for the copyright- and privacy-protected image trading system application. Besides the 2D DCT, the 1D DCT can also be applied in the proposed scheme. Figs. 3(c) and (d) show the images with replaced 1D DCTed amplitude components. The images are also recognizable with about 16 dB PSNR. In addition, applying 1D DCT instead of 2D DCT reduces the complexity of the system.

It is noted that, the DCT is applied to images in the proposed scheme instead of the DFT, because the DCTed signs consisting of +1 and -1 are integers and can be stored perfectly as a binary image without quantization. On the other hand, though the DFT has a good characteristic for the scheme which is complete decomposition of an image to amplitude and phase components, the DFTed phase components consist of real numbers and therefore the quantization of the DFTed phase components is required to store them as a low depth/standard depth image. As a result, the reconstructed image quality is much degraded due to those quantization errors, similar to other transformations which generate phase components as real numbers, for examples, fractional Fourier transform, Hadamard transform, ..., etc. In addition to image quality degradation, the quantized phase components, which are even stored as a standard depth image (for example 8-bpp image), require more storage memory and transmission bandwidth than those required by the DCTed signs.



(a) Lena w/ 2D DCTed Mandrill Amplitudes PSNR: 16.2247 dB

(b) Mandrill w/ 2D DCTed Lena Amplitudes PSNR: 16.2709 dB

(c) Lena w/ 1D DCTed Mandrill Amplitudes PSNR: 15.8864 dB

(d) Mandrill w/ 1D DCTed Lena Amplitudes PSNR: 15.8797 dB

Fig.3: *Images with replaced amplitude components by using 2D DCT and 1D DCT, respectively.*

3.2 Proposed Copyright- and Privacy-Protected Image Trading System with A Second TTP

From the characteristic of the image with replaced amplitude components described in Section 3.1, the stego-image consisting of the DCTed amplitude components of the commercial image and the DCTed signs of the dummy image is sent to the TTP for future fingerprinting in the proposed system as shown in Fig. 4. The TTP/malicious third party then recognizes the dummy image instead of the commercial image, but actually the amplitude components of the commercial image is secretly conveyed to the first TTP. The image is then fingerprinted by the first TTP; therefore, if the used fingerprinting method does not modify the DCTed signs, the fingerprint is

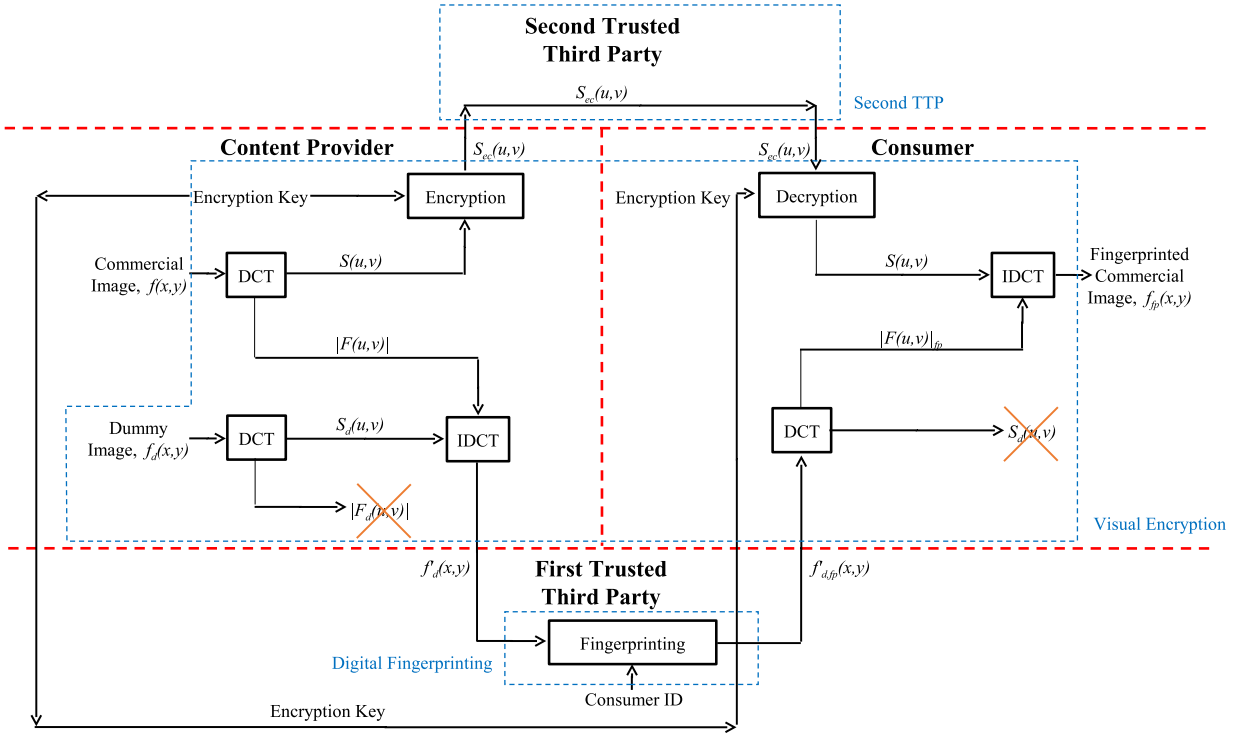


Fig.4: *Proposed copyright- and privacy-protected image trading system using DCTed amplitude component replacing. Three dotted blocks (visual encryption, second TTP, and digital fingerprinting) are different from conventional systems, c.f., Table 1.*

perfectly embedded to the amplitude components of the commercial image. Thus, this paper also proposes a compatible fingerprinting method as described in Section 3.3. After the fingerprinting process, the first TTP sends the image to the consumer. In addition, the amplitude components of the dummy image are discarded as marked by a cross symbol in Fig. 4.

The DCTed signs of the commercial image are simultaneously conveyed to the consumer as a key for image reconstruction. However, differently from the conventional systems, the image reconstruction key is not sent directly from the CP to the consumer in the proposed system. It is sent from the CP to the introduced second TTP, and then it is conveyed from the second TTP to the consumer. This makes sure that, the CP does not contact with the consumer directly, for complete consumer's privacy protection. In addition, the image reconstruction key is encrypted by the CP before sending it to the second TTP for consumer's privacy protection against the second TTP/malicious third parties. The encryption key is conveyed to the consumer via the first TTP as shown in Fig. 4. Though the encrypted image reconstruction key has a possibility to be attacked, the decrypted image is just the DCTed signs of the commercial image. By performing the IDCT, the output image is just a much degraded version of the commercial image. In this case, a part of the consumer's privacy might be lost, but at least the stolen image does not have enough quality for any businesses. This is another difference between the proposed system and the conventional systems.

For the encryption process, general binary encryption techniques can be applied, because the DCTed signs are stored as a general binary image. Therefore, the description and the experiment of the encryption process is omitted. In addition, in practical terms, the image can be easily losslessly compressed using general standard compressions with the same reason that the image is a general binary image.

For image reconstruction, the fingerprinted stego-image is transformed by the consumer using the 2D DCT. After that, the amplitude components of the commercial image containing the fingerprint are extracted, and are then combined with the decrypted DCTed signs of the commercial image. Finally, the 2D IDCT is applied to reconstruct the commercial image containing the fingerprint called the "fingerprinted commercial image," while the DCTed signs of the dummy image are finally discarded as marked by a cross symbol in Fig. 4.

For the fingerprint extraction process, it is simple, because the fingerprint can be extracted directly and efficiently from the reconstructed fingerprinted commercial image, $f_{fp}(x, y)$. However, this is true if and only if the fingerprinting method does not modify the DCTed signs of the image at all. In other words, the fingerprint should be embedded only into the ampli-

Table 1: *Comparison of the conventional and the proposed methods and systems.*

	Conventional	**Proposed**
1) Visual encryption scheme	1D DCTed AOI	DCTed amplitude component replacing
2) Second TTP for consumer's privacy	Not exist	Exist
3) Digital fingerprinting method	Mainly amplitudes and some phases	Amplitude-only fingerprinting

tude components of the commercial image, similar to embedding the fingerprint to the AOI in the conventional system. If not, the fingerprint would not be perfectly extracted due to the discarding of the DCTed sign components of the dummy image in the image reconstruction process. To meet this requirement, a new fingerprinting method is proposed in Section 3.3.

3.3 Proposed Compatible Fingerprinting Method

Since any arbitrary amplitude-based fingerprinting method should be used in the proposed system as well as in the conventional systems, the visually protected images are fingerprinted by a new frame DCT-based amplitude-only fingerprinting method developed here based on the block DCT-based image quality-guaranteeing fingerprinting method [28]. The proposed method guarantees fingerprinted image quality in terms of the signal-to-watermark ratio (SWR) by controlling the energy of the fingerprint sequence, and the SWR is defined as

$$\mathrm{SWR} = 10\log_{10}\frac{255^2}{\sum_{x=0}^{X-1}\sum_{y=0}^{Y-1}\left\{A\left(x,y\right)-\widehat{A}(x,y)\right\}^2} \tag{10}$$

where $A(x,y)$ denotes the visually protected image to be fingerprinted, and $\widehat{A}(x,y)$ denotes the fingerprinted image. The lower the number of desired SWR becomes, the stronger the fingerprint signal becomes. That is, the fingerprint is easier to be extracted when the SWR is lower. It is noted that this tradeoff between the correct fingerprint extracting rate and the image quality of the fingerprinted image is typical for digital fingerprinting [3]. The method quantizes the DCTed coefficients to hide a fingerprint in an image. The quantization step size Q for hiding a binary fingerprint sequence into $A(x,y)$ is derived as

$$Q = 10^{-0.05R}\sqrt{\frac{D}{L}\sum_{x=0}^{X-1}\sum_{y=0}^{Y-1}255^2} \tag{11}$$

where R denotes the user-given desired SWR to be guaranteed. D is defined as

$$D = \frac{12N_\sigma^2}{N_\sigma^2+3M_\sigma^2} \tag{12}$$

where N_σ and M_σ are set to 1 and 0.5, respectively. L is the length of the fingerprint bit sequence. The l-th fingerprint bit w_l is hidden in an AC coefficient c_l in the image as

$$\widehat{c}_l = \begin{cases}\mathrm{sgn}\left(c_l\right) * \left(Q * \mathrm{round}\left(\frac{|c_l|}{Q}\right) + w_l'\right), & \mathrm{round}\left(\frac{|c_l|}{Q}\right) \neq 0 \\ w_l', & \text{otherwise}\end{cases} \tag{13}$$

where $\widehat{c}_l$ denotes the fingerprinted coefficient, and w_l' denotes the l-th energy controlled fingerprint bit given by

$$w_l' = \frac{M_\sigma Q}{N_\sigma}(w_l - 0.5) \tag{14}$$

where $l = 0,\ 1,\ \ldots,\ L-1$.

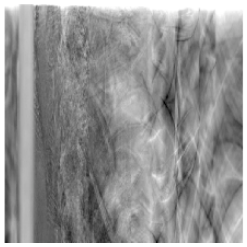
In conclusion, this paper proposes three things: 1) amplitude component replacing-based visual encryption scheme to generate a meaningful image simultaneously with protecting the visual of the commercial image, 2) a new system with a second TTP, and 3) a compatible fingerprinting method to solve the problem of applying image steganography to the focused application. Table 1 compares the conventional and the proposed methods and systems.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

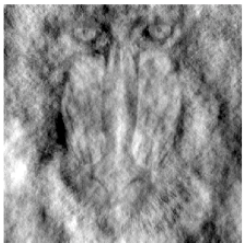
The proposed 2D DCTed amplitude component replacing scheme is compared with the conventional 1D DCTed AOI scheme. In addition, the proposed scheme is extended to the 1D DCT. The experiment is divided into three parts: 1) visual protection and recognizability, 2) reconstructed image quality, and 3) fingerprinting performance. Five test images are used in the experiments.

4.1 Visual Protection and Recognizability

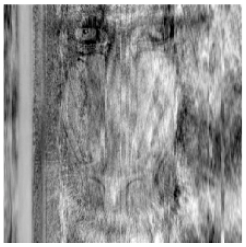
From the results shown in Fig. 5, both the proposed and conventional schemes perfectly visually protect the commercial images. But for recognizability, of course, the conventional AOI-based schemes do not meet this requirement, because the schemes generate unrecognizable images for all five test images, c.f., 1st column. In contrast, for the proposed scheme, almost all stego-image shown in the second and the



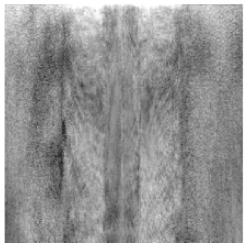
(a) Lena 1D DCTed AOI



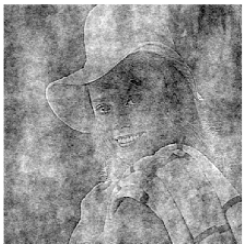
(b) Mandrill w/ 2D DCTed Lena Amplitudes PSNR: 16.2709 dB



(c) Mandrill w/ 1D DCTed Lena Amplitudes PSNR: 15.8797 dB

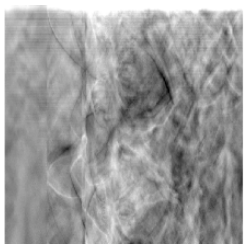


(d) Mandrill 1D DCTed AOI

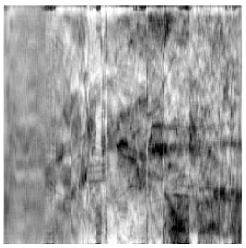


(e) Elaine w/ 2D DCTed Mandrill Amplitudes PSNR: 15.8143 dB

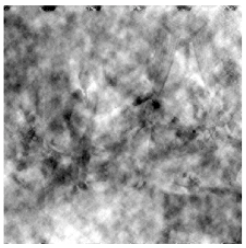
(f) Elaine w/ 1D DCTed Mandrill Amplitudes PSNR: 15.7741 dB



(g) Elaine 1D DCTed AOI

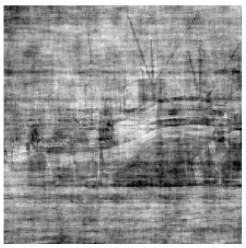


(h) Couple w/ 2D DCTed Elaine Amplitudes PSNR: 15.4611 dB



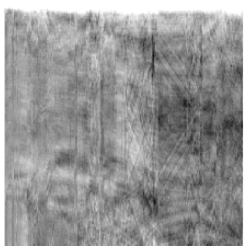
(i) Couple w/ 1D DCTed Elaine Amplitudes PSNR: 15.8831 dB

(j) Couple 1D DCTed AOI



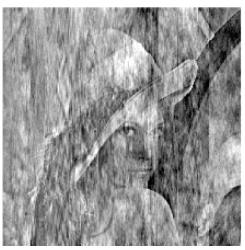
(k) Boat w/ 2D DCTed Couple Amplitudes PSNR: 16.8406 dB

(l) Boat w/ 1D DCTed Couple Amplitudes PSNR: 16.2865 dB



(m) Boat 1D DCTed AOI

(n) Lena w/ 2D DCTed Boat Amplitudes PSNR: 15.1895 dB



(o) Lena w/ 1D DCTed Boat Amplitudes PSNR: 15.1332 dB

Fig.5: *AOIs generated by the conventional scheme and stego-images generated by the proposed scheme. The first column shows images generated by the conventional scheme. The second and third columns show images generated by the proposed scheme.*

Table 2: *Intensity ranges of visually protected images.*

(a) 1D DCTed AOIs by the conventional system [10].

Commercial	Min	Max
Lena	-16.9223	631.7171
Mandrill	1.0373	784.1869
Elaine	-22.2700	678.0037
Couple	-47.2701	857.1235
Boat	0.7186	784.8557

(b) Stego-image by the proposed system.

Commercial-Dummy	2D DCT		1D DCT	
	Min	Max	Min	Max
Lena-Mandrill	-76.7299	318.9002	-50.0828	290.3091
Mandrill-Elaine	-41.7917	341.9038	-115.7553	312.3400
Elaine-Couple	-98.9023	345.8351	-71.5995	364.3037
Couple-Boat	-47.8507	282.8358	-53.7514	304.8017
Boat-Lena	-63.6608	307.5326	-95.9416	328.6461

Table 3: *PSNRs of reconstructed images [dB].*

(a) Conventional system [10].

Commercial	PSNR of reconstructed image
Lena	26.6039
Mandrill	25.0147
Elaine	24.5905
Couple	24.1129
Boat	23.3659

(b) Proposed system.

Commercial-Dummy	PSNR of reconstructed image	
	2D DCT	1D DCT
Lena-Mandrill	41.4480	49.9945
Mandrill-Elaine	50.3528	47.8904
Elaine-Couple	42.2731	40.6125
Couple-Boat	50.7559	49.1417
Boat-Lena	47.1215	42.6796

third columns have enough quality to be recognized with about 16 dB PSNR comparing to the dummy images.

4.2 Reconstructed Image Quality

For the proposed scheme, the stego-image should be able to convey the secret messages effectively. To do so, the stego-image should not have a high intensity range so that some information of the image is lost by quantization/rounding in the storing process. For the conventional scheme [10], the AOI should have a low intensity range to avoid quantization/rounding effect in the storing process as well. However, the intensity range of the AOIs generated by the conventional scheme are much wider than 256 as shown in Table 2(a). This is a general problem of the AOI-based schemes. However, in the proposed scheme, replacing the amplitude components of a dummy image with the amplitude components of a commercial image generates an image with much lower intensity ranges as shown in Table 2(b), and this fact improves the qualities of the reconstructed commercial images as described below.

Storing an image with a wide intensity range as an 8-bpp image needs quantization or rounding, As a result, the qualities of the reconstructed commercial images are degraded. Though linear quantization [8] could achieve better results than rounding, it requires memorizing the quantization step size image by image to reconstruct the commercial image. Instead of the costed inverse quantization, in this paper, the images are rounded with no need for side information. Table 3 shows the qualities of the reconstructed images, when the fingerprinting process is omitted. The con-

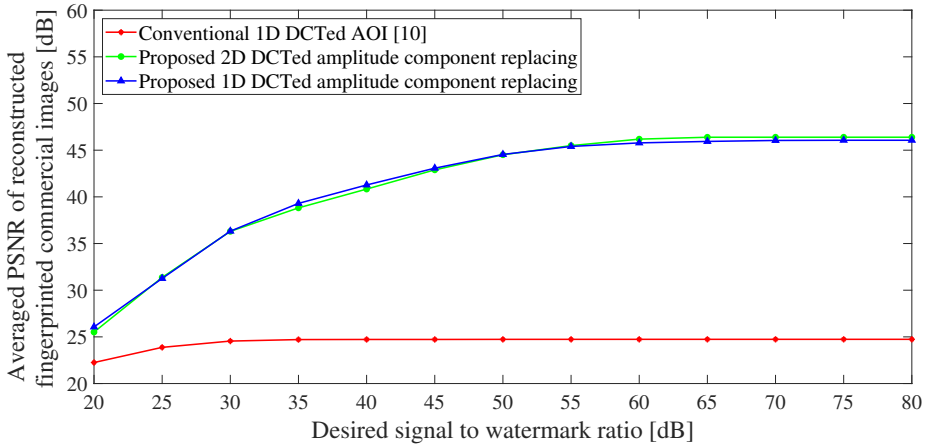


Fig. 6: *Reconstructed fingerprinted image qualities.*

ventional scheme achieves <30 dB PSNRs, while the proposed schemes achieve >40 dB PSNRs for all five test images. This could be described by the intensity ranges of the images shown in Table 2. The intensity ranges of the 1D DCTed AOIs are much wider (about double) than those of the stego-images generated by the proposed scheme for both 2D DCT and 1D DCT.

4.3 Fingerprinting Performance

The proposed fingerprinting method described in section 3.3 is used in the experiment. R is varied from 20 dB to 80 dB with stepping by 5 dB. 4096 random binary fingerprint bits ($L = 4096$) are embedded into 512×512-pixel stego-images. In cases of the proposed 2D DCTed amplitude component replacing system, the 2D frame DCT is used for embedding the fingerprint, and in cases of the proposed 1D DCTed amplitude component replacing system and the conventional 1D DCTed AOI system, the 1D frame DCT is used for embedding the fingerprint. For the fingerprint extraction process, as well as in the conventional system, the fingerprint can be extracted directly from the reconstructed fingerprinted commercial image, since the fingerprint is embedded to the amplitudes only.

As described in Section 4.2, the proposed system achieves much higher reconstructed image qualities when the fingerprinting is not embedded. In this section, the fingerprint is embedded, and the reconstructed image qualities are investigated again. Figure 6 shows the reconstructed fingerprinted image qualities of the proposed and conventional systems. The results are averaged by five test images. For every system, by more strongly embedding the fingerprint, the image qualities are more degraded as can be controlled by the desired SWR, R. With varying the SWR, the proposed 2D DCT and 1D DCT amplitude component replacing methods achieve much higher reconstructed image qualities in terms of averaged PSNRs than those of the conventional system regardless of the SWR.

Fig. 7 shows the fingerprint extraction performances of the proposed system and the conventional system. It is shown that the higher correct fingerprint extracting rate is achieved when the SWR of the fingerprinted image is lower, i.e., the fingerprint is embedded more strongly. However, when the fingerprint is embedded too strongly, the modified image after fingerprinting is very different from the image before fingerprinting, and it exceeds the [0, 255] range so that it is rounded to [0, 255] to be stored as an 8-bpp image. Therefore, the fingerprint is degraded by the rounding operation, and it results in a lower fingerprint extracting rate. Therefore, the results show that the proposed system enhances the correct fingerprint extracting rate compared to that of the conventional system.

Due to the fact that the fingerprinting performance depends on the fingerprinting method, other fingerprinting methods such as [29–34] could also be applied to evaluate the performance of the proposed system and the conventional system.

5. CONCLUSION

This paper has proposed a novel steganography-based visual encryption scheme for a copyright- and privacy-protected image trading system. The proposed scheme, as with conventional schemes, visually protects the image to be traded, but the visually protected image is still meaningful unlike the encrypted image in the conventional schemes. Thus, the malicious third parties neither suspect nor attack the image. Since the recognized image content is a dummy image, the consumer's privacy is protected against the TTP and malicious third parties. As another contribution of this paper, a new system is proposed where the CP is not allowed to directly send the image reconstruction key to the consumer for fur-

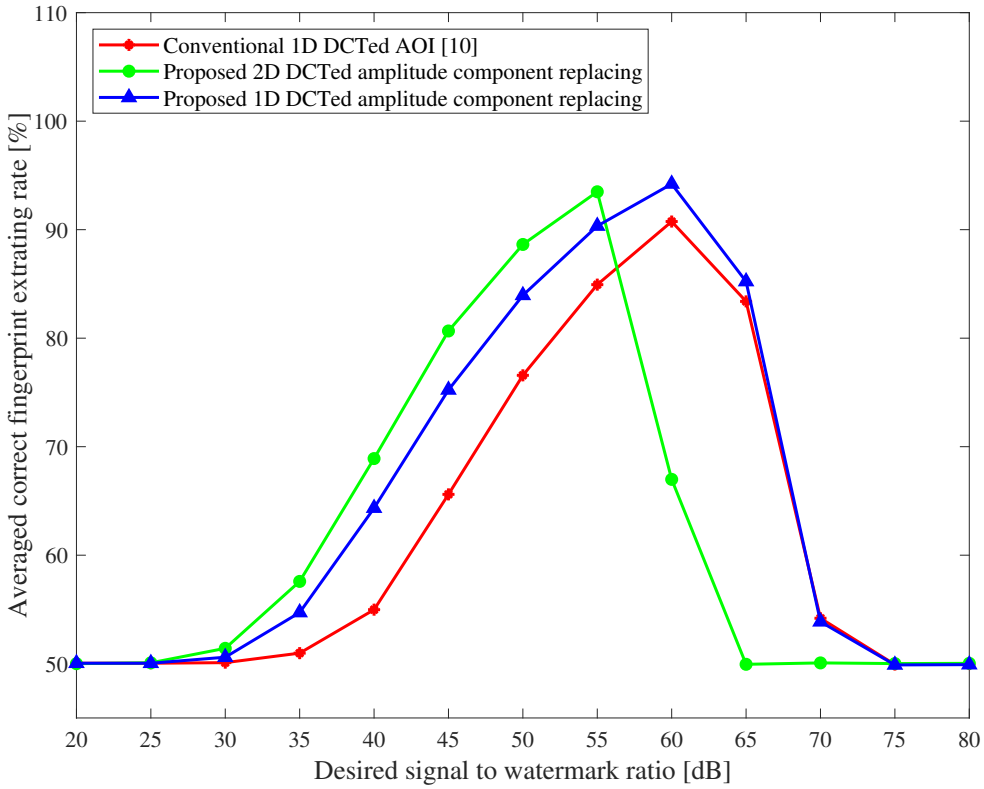


Fig. 7: *Fingerprint extraction performances.*

ther consumer's privacy protection, whereas the CP identifies the consumer to send the key to the consumer in the conventional systems. The second TTP is then introduced to the proposed system, and in addition, the image reconstruction key is encrypted by the CP before being sent to the consumer via the second TTP. This encryption process is proposed to protect the consumer's privacy against the malicious third parties. The third contribution is that a frame DCT-based amplitude fingerprinting method, which is compatible with the proposed amplitude component replacing scheme; this is proposed in this paper to solve the problem of applying image steganography to the focused application. Experimental results show that the proposed system generates recognizable images and perfectly visually encrypts the commercial images. It also achieves much higher reconstructed image qualities than those of the conventional system and simultaneously enhances the fingerprinting performance using the proposed compatible fingerprinting method.

ACKNOWLEDGMENTS

This research was funded by King Mongkut's University of Technology North Bangkok. Contract no. KMUTNB-61-DRIVE-046.

References

[1] R.L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Process. Mag., vol. 30, no. 1, pp. 82–105, Jan. 2013.

[2] M. Kuribayashi, "Recent fingerprinting techniques with cryptographic protocol," Signal Processing, S. Miron, ed., InTech, 2010.

[3] I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography," 2nd ed., Morgan Kaufmann Publishers, 2008.

[4] B. Schneier, "Applied cryptography: protocols, algorithms, and source code in C," 2nd ed., John Wiley & Sons, 1996.

[5] Y. Sengoku and H. Hioki, "A model of privacy and copyright-aware image trading system based on adaptive image segmentation and digital watermarking," in ITC-CSCC, Sapporo, Japan, pp. D-W1-02, Jul. 15-18, 2012.

[6] Y. Sengoku and H. Hioki, "An image segmentation method for privacy and copyright-aware image trading system," IEICE Tech. Rep., vol. 111, no. 496, EMM2011-67, pp.19–24, Mar. 2012.

[7] M. Okada, Y. Okabe, and T. Uehara, "A web-based privacy-secure content trading system for

small content providers using semi-blind digital watermarking," in Proc. IEEE CCNC, 2010.

[8] S. Liu, M. Fujiyoshi, and H. Kiya, "An image trading system using amplitude-only images for privacy- and copyright-protection," IEICE Trans. Fundamentals, vol. E96-A, pp. 1245–1252, Jun. 2013.

[9] W. Sae-Tang, M. Fujiyoshi, and H. Kiya, "A Generation Method of Amplitude-Only Images with Low Intensity Ranges," IEICE Trans. Fundamentals, vol. E96-A, no. 6, pp. 1323–1330, Jun. 2013.

[10] W. Sae-Tang, S. Liu, M. Fujiyoshi, and H. Kiya, "1D Frequency Transformation-Based Amplitude-Only Images for Copyright- and Privacy-Protection in Image Trading Systems," ECTI-CIT, vol. 8, no. 2, Nov. 2014.

[11] W. Sae-Tang, M. Fujiyoshi, and H. Kiya, "Evaluation of Amplitude-Only Images for Copyright- and Privacy-Protected Image Trading Systems," in ITC-CSCC, Phuket, Thailand, no. 1069, pp. 113–116, Jul. 1-4, 2014.

[12] W. Sae-Tang and H. Kiya, "Hadamard Transform-Based Amplitude-Only Images for Image Trading Systems," in IWAIT, Busan, Korea, no. 3C.5, Jan. 6-8, 2016.

[13] W. Sae-Tang, M. Fujiyoshi, and H. Kiya, "Encryption-then-Compression-Based Copyright- and Privacy-Protected Image Trading System," in ICAIP, Bangkok, Thailand, pp. 66–71, Aug. 25–27, 2017.

[14] K. Stefan and F. Petitcolas, "Information hiding techniques for steganography and digital watermarking," Artech house, 2000.

[15] J. Neil F. and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer 31.2, 1998.

[16] B. Shumeet, "Hiding images in plain sight: Deep steganography," Advances in Neural Information Processing Systems, pp. 2069–2079, 2017.

[17] A.V. Oppenheim and J.S. Lim, "The importance of phase in signals," IEEE, vol. 69, pp. 529–541, May. 1981.

[18] K. Ito, A. Nikaido, T. Aoki, E. Kosuge, R. Kawamata, and I. Kashima, "A dental radiograph recognition system using phase-only correlation for human identification," IEICE Trans. Fundamentals, vol. E91-A, no. 1, pp. 298–305, Jan. 2008.

[19] K. Ito, T. Aoki, H. Nakajima, K. Kobayashi, and T. Higuchi, "A palmprint recognition algorithm using phase-only correlation," IEICE Trans. Fundamentals, vol. E91-A, no. 4, pp. 1023–1030, Apr. 2008.

[20] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An effective approach for iris recognition using phase-based image matching," IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 10, pp. 1741–1756, Oct. 2008.

[21] Q.-S. Chen, M. Defrise, and F. Deconinck, "Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 16, no. 12, pp. 1156–1168, Dec. 1994.

[22] C.H. Knapp and G.C. Carter, "The generalized correlation method for estimation of time delay," IEEE Trans. Acoustics, Speech, and Signal Process., vol. ASSP-24, no. 4, pp. 320–327, Aug. 1976.

[23] C.D. Kuglin and D.C. Hines, "The phase correlation image alignment method," Proc. IEEE Int. Conf. Cybernetics and Society, pp. 163–165, 1975.

[24] K. Takita, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, "High accuracy subpixel image registration based on phase-only correlation," IEICE Trans. Fundamentals, vol. E86-A, no. 8, pp. 1925–1934, Aug. 2003.

[25] H. Amirshahi, S. Kondo, K. Ito, and T. Aoki, "An image completion algorithm using occlusion-free images from Internet photo sharing sites," IEICE Trans. Fundamentals, vol. E91-A, no. 10, pp. 2918–2927, Oct. 2008.

[26] I. Ito and H. Kiya, "One-time key based phase scrambling for phaseonly correlation between visually protected images," EURASIP J. Inf. Security, vol. 2009, no. 841045, Jan. 2010.

[27] I. Ito and H. Kiya, "Phase-only correlation based matching in scrambled domain for preventing illegal matching," LNCS Transactions on Data Hiding and Multimedia Security V, vol. 6010/2010, pp. 51–69, Jun. 2010.

[28] T. Tachibana, M. Fujiyoshi, and H. Kiya, "A watermarking scheme retaining the desired image quality in order to be applicable to watermarks with various distributions," IEICE Trans. Inf. & Sys. (Japanese Edition), vol. J87-D-II, no. 3, pp. 850–859, Mar. 2004.

[29] H. Inoue, A. Miyazaki, and T. katsura, "An image watermarking method based on the wavelet transform," in Proc. IEEE ICIP, pp. 296–300, 1999.

[30] Z. Zhang, Q. Sun, and W. Wong, "A novel lossy-to-lossless watermarking scheme for JPEG2000 images," in Proc. IEEE ICIP, pp. 573–576, 2004.

[31] Y. Chen and H. Huang, "A progressive image watermarking scheme for JPEG2000," in Proc. IEEE IIH-MSP, pp. 230–233, 2012.

[32] L. Sun, JC. Xu, XX. Zhang, and Y. Tian, "An image watermarking scheme using Arnold transform and fuzzy smooth support vector machine," Math. Probl. Eng., vol. 2015, Article ID 931672.

[33] FL. Liu and LL. Liu, "A new watermarking approach based on BP network in wavelet domain," in Proc. IEEE CISP, pp. 1142–1145, Oct. 16-18, 2010.

[34] S.D. Lin, S.C. Shie, and J.Y. Guo, "Improving

the robustness of DCT-based image watermarking against JPEG compression," Comput. Stand. Interfaces, vol. 32, no. 1-2, pp. 54–60, Jan. 2010.

Wannida Sae-Tang received her B.Eng. Degree in Electronic and Telecommunication Engineering with the first class honors and her M.Eng. Degree in Electrical Engineering from King Mongkut's University of Technology Thonburi, Thailand in 2007 and 2011, respectively, and her Ph.D. degree in Information and Communication Systems from Tokyo Metropolitan University, Japan in 2014 with Tokyo metropolitan governmental Asian human resources fund. From 2007 to 2009, she was an IC packaging design engineer of New product design and research and development team at United Test and Assembly Center Thai Ltd. She is currently a lecturer of The Sirindhorn International Thai-German Graduate School of Engineering, King Mongkut's University of Technology North Bangkok, Thailand. Her research interests include image processing and multimedia communications. She received the Best Paper Award of the IEICE/ITE/KSBE IWAIT in 2014.

Masaaki Fujiyoshi received his B. Arts, M. Eng., and Ph.D. degrees from Saitama University, Japan, in 1995, 1997, and 2001, respectively. In 2001, he joined Tokyo Metropolitan University where he became an Associate Professor in 2014. His research interests include image processing, media-aware security, and multimedia communications. He is a senior member of the IEICE and a member of the IEEE, EURASIP, APSIPA, ITE, and JSET. He received the IEICE Young Researchers Award in 2001.

Hitoshi Kiya received his B.E and M.E. degrees from Nagaoka University of Technology, in 1980 and 1982 respectively, and his Dr. Eng. degree from Tokyo Metropolitan University in 1987. In 1982, he joined Tokyo Metropolitan University, where he became a Full Professor in 2000. From 1995 to 1996, he attended the University of Sydney, Australia as a Visiting Fellow. He is a Fellow of IEEE, IEICE and ITE. He currently serves as President of APSIPA, and he served as Inaugural Vice President (Technical Activities) of APSIPA from 2009 to 2013, and as Regional Director-at-Large for Region 10 of the IEEE Signal Processing Society from 2016 to 2017. He was also President of the IEICE Engineering Sciences Society from 2011 to 2012, and he served there as a Vice President and Editor-in-Chief for IEICE Society Magazine and Society Publications. He was Editorial Board Member of eight journals, including IEEE Trans. on Signal Processing, Image Processing, and Information Forensics and Security, Chair of two technical committees and Member of nine technical committees including APSIPA Image, Video, and Multimedia Technical Committee (TC), and IEEE Information Forensics and Security TC. He has organized a lot of international conferences, in such roles as TPC Chair of IEEE ICASSP 2012 and as General Co-Chair of IEEE ISCAS 2019. He has received numerous awards, including six best paper awards.