J Inf Process Syst, Vol.15, No.1, pp.169~180, February 2019
https://doi.org/10.3745/JIPS.03.0109

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Wavelet-Based Digital Image Watermarking by Using Lorenz Chaotic Signal Localization

Jantana Panyavaraporn* and Paramate Horkaew**

Abstract

Transmitting visual information over a broadcasting network is not only prone to a copyright violation but also is a forgery. Authenticating such information and protecting its authorship rights call for more advanced data encoding. To this end, electronic watermarking is often adopted to embed inscriptive signature in imaging data. Most existing watermarking methods while focusing on robustness against degradation remain lacking of measurement against security loophole in which the encrypting scheme once discovered may be recreated by an unauthorized party. This could reveal the underlying signature which may potentially be replaced or forged. This paper therefore proposes a novel digital watermarking scheme in temporal-frequency domain. Unlike other typical wavelet based watermarking, the proposed scheme employed the Lorenz chaotic map to specify embedding positions. Effectively making this is not only a formidable method to decrypt but also a stronger will against deterministic attacks. Simulation report herein highlights its strength to withstand spatial and frequent adulterations, e.g., lossy compression, filtering, zooming and noise.

Keywords

Binary Image, Chaotic Signal, QR Code, Watermarking, Wavelet Analysis

1. Introduction

Electronic watermarking [1] is a process of hiding multimedia information, such as voice, image and video, etc., within the carrier signal. This information was normally embedded onto user message for ownership identification and copyright protection purposes. Digital watermarking techniques can be categorized, depending on its operational domain, into two approaches. Firstly, spatial domain watermarking is an approach where the embedding process is carried out by directly modifying the pixel values [2]. The other one is frequency domain watermarking whose embedding was done on the transformed space by altering, for instance, some frequency components of the underlying signals.

Over recent decades, there have been several watermarking schemes applied to digital images in the literatures [3-10]. It was shown in these early attempts that watermark could be inserted into the spatial domain of an image. In [3], for example, the watermark was embedded into a pair of pixels using least significant bit (LSB) substitution. Similarly, Walia and Suneja [4] applied Weber's law and embedded watermark by selectively altering the intensities of dark pixels. The major concerns shared by these spatial

Manuscript received March 2, 2016; first revision December 14, 2016; accepted January 1, 2017.
Corresponding Author: Jantana Panyavaraporn (jantanap@eng.buu.ac.th)
* Dept. of Electrical Engineering, Faculty of Engineering, Burapha University, Chonburi, Thailand (jantanap@eng.buu.ac.th)
**School of Computer Engineering, Suranaree University of Technology, Nakhon Ratchasima, Thailand (phorkaew@sut.ac.th)

domain techniques are that the watermark can easily be extracted and too fragile to withstand severe types of attacks. To circumvent these issues, much watermarking research had focused instead on the frequency domain [5-10]. In [5,6], for instances, watermarks were blindly embedded in a frequency sub-band of the most principal images obtained by using the Principle Component Analysis (PCA). Barni et al. [7] proposed the new concept of near-lossless watermarking, whereby an assumption was made that disparities resulted from the discrete Fourier transform (DFT) or discrete wavelet transform (DWT) embedding process were bounded by predefined measurement noise level. To improve the robustness criterion, Kunhu and Al-Ahmad [8] and Rosiyadi et al. [9] performed their embedding on the discrete cosine transform (DCT) domain. The former also embedded hash authentication in the spatial domain to tighten the security, while the latter applied optimally scaled singular value decomposition (SVD) to stabilize the process. Based on the similar paradigm, a combination of DCT, SVD and DWT was considered by Divecha and Jani [10], where the embedding was applied for copyright protection. In this work, the technical aspects and its performance were analyzed. Taking into account of pros and cons of spatial and spectral operations, more recent works in this area had considered robust watermarking on a spatio-spectral domain.

Other watermarking literatures put more emphasis on applications. In [11-16], watermarks were found applied to medical images for various security oriented purposes. Watermarking based on SVD and wavelet analysis, for example, was suggested in [11] and their results were shown superior to the traditional schemes in biometric (iris) images. Ding et al. [12], proposed a DCT based technique for concealing biometrics, where watermark bits were used both for integrity check and as a hidden channel. In [13], the authors proposed a dual-layer image watermarking scheme that is a reversible watermark used for verification followed by that defined by a logo image for providing confidentiality. Therein, the embedding was performed on the DCT domain, where DWT and SVD were used for transforming gray scale medical images. Another example based on wavelet analysis was proposed by Benyoussef et al. [14], where a robust ROI watermarking was created based on visual cryptography concept and the dominant blocks of wavelet coefficients and then applied to mammogram images. In [15,16], watermarking was used for securing medical images. Within the context of Picture Archiving and Communication Systems (PACS), the former scheme [15] first compressed a watermark by using the LZW algorithm and then embedded it in ultrasound images for tempering detection. While in the latter scheme [16], a watermark was integrated with encryption for verification proposed. Sharing the principle of imaging security, Jang et al. [17] presented a new watermarking system designed for the integrated copyright protection system that dealt with incremental video codec. The method based on quantization, DCT/DWT kernel or ME/MC in the encoding process. Jassim et al. [18] combined both spatial (RGB) and frequency (DWT) domain watermarking for two-layer authentication of a mobile phone image. As modern digital economy has presently gained vast popularity, commercial activities on the internet have a pressing need to protect the involving parties against security breach. Research in e-commerce has pursued this goal and proposed embedding of, for example, two-dimensional barcode or QR code in the transmitted images by using DCT [19] and wavelet transform [20].

Despite the robustness against general attacks, these schemes share a common pitfall. Specifically, once been disclosed, the embedding process can be recreated to reveal the encrypted watermark which can later be altered or forged. To strengthening the security measure, this paper proposes a novel blind digital watermark scheme based on wavelet transform and chaotic signal. With this scheme, a wavelet sub-band

served as the domain for hiding the watermark with minimally message losses. While the chaotic signal principal was employed to determine the embedding sites, this maked it harder to decipher.

However, there is an existence in literatures that some digital image watermarking schemes based on chaotic signal [21-27]. Their comparative characteristics, i.e., type of chaotic signal, imaging domain and watermark were listed in Table 1. Specifically, in [21,22], the watermarks were embedded in the DCT domain while in [24] it was done on the spatial one. Keyvanpour and Merrikh-Bayat [23] presented an embedding method using chaos-fractal coding but did not focus on the watermark types. The remaining works [25-27] presented embedding process on a wavelet domain. They are primarily different in terms of how the chaotic signals were processed. In [25], a chaotic key was generated by XOR operation with a binary sequence of a watermark logo. The chaotic encrypted image was then used for embedding the wavelet coefficients. Esgandari and Khalili [26] proposed a watermark with two-dimensional chaotic function and embedded in the middle frequency band of the wavelet image. In the last one [27], a watermark was generated on a basic of a chaotic sequence known as tent map. According to that study, the third LSB of each wavelet coefficient was accordingly modified.

Table 1. Summarize of closely related watermarking schemes using chaotic signal

Reference	Type of chaotic signal	Spatial/Transform domain	Watermark
[21]	Logistic map	Discrete cosine transform	Binary logo
[22]	Toral automorphism (two-dimensional)	Discrete cosine transform	Random sequence
[23]	Arnold's cat map	Chaos-fractal coding	-
[24]	Logistic map	Spatial domain	Gray logo
[25]	Logistic map	Discrete wavelet transform	Binary logo
[26]	Two-dimensional chaotic	Haar wavelet transform	Binary logo
[27]	Tent map	Discrete wavelet transform	Binary sequence

The presented work is most similar to that proposed by Jamal et al. [24] in that the logistic was employed to identify the watermark position in the original image. Since in their work the watermark was embedded in the spatial domain by altering the LSBs of the host image so as not to degrade its visual appearance, the resultant image could thus be easily affected by noise. To resolve this issue, we therefore adopted the Lorenz equation operating on the DWT domain as a means of localizing embedding site. This is our main contribution to differentiate the proposed scheme from the existing works [21-27]. Furthermore, to enhance the visual appearance of the extracted watermark, an average kernel was also used as imaging filter.

This paper is organized as follows: Section 2 describes the proposed watermark embedding and extracting schemes. The simulation results are presented and discussed in Sections 3 and 4, respectively.

2. Proposed Method

In order to address the above mentioned issues found in existing watermarking literatures, we therefore propose a novel watermarking scheme with the following characteristics (as shown in Table 2):

Table 2. Characteristics of our watermarking scheme

Characteristic	Description
Blind	It does not require the original image in order to recover the embedded watermark.
Noise robustness	It is robust against noise attacks such as that of Gaussian and Salt and Pepper types.
Tampering robustness	It is robust against some mild geometrical attacks such as cropping, changing of aspect ratio, resizing and rotation.
Applicability	Digital Image
Feature	There is no noticeable visual degradation in the embedding image

Without the loss of generalization ability, the proposed scheme was described and assessed based on the following data. The base image chosen as an original message was a QR code image (Fig. 1(a)). Since this binary code is quite susceptible to various degradations in practices and was often assessed by applicability in subsequent visual processing, it was accordingly chosen to illustrate the merit of our scheme. Likewise, a binary image of a university logo containing detailed features was opted as the embedded watermark (Fig. 1(b)).

(a) (b)

Fig. 1. A QR code as the original message (a) and a logo image as embedded watermark (b).

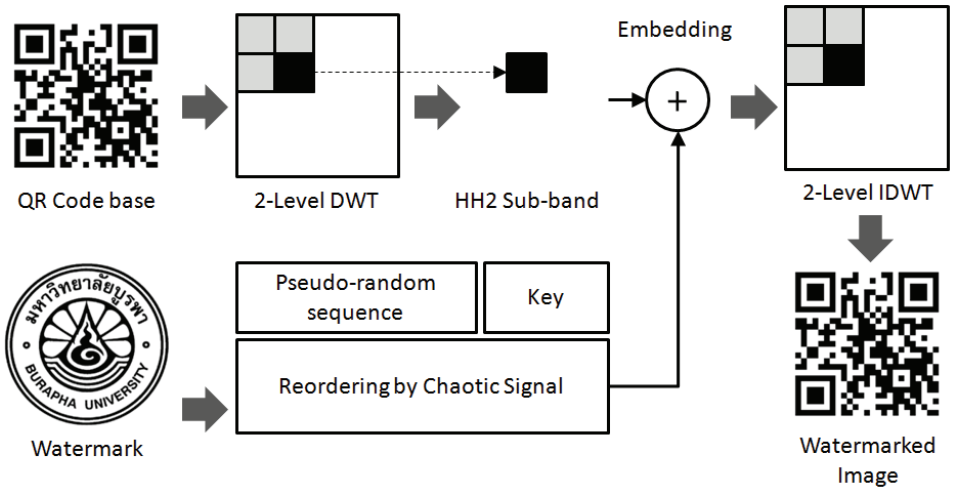


Fig. 2. A diagram outlining the proposed embedding process.

2.1 Watermark Embedding

The steps involving in the embedding are outlined in Fig. 2 and described as follows:

(i) The watermark image (Fig. 1(b)) was represented as a binary sequence (**S**) of *N* pixels, in which the foreground and background pixels were prescribed as 1 and –1, respectively.

$$\mathbf{S} = \left\{ s_i, 1 \le i \le N \right\}, s_i \in \left\{ -1, 1 \right\} \tag{1}$$

(ii) A pseudo-random sequence (**P**) of size *N* whose values were either 1 or –1 was later generated with a predefined secret key used in the embedding and extracting processes.

$$\mathbf{P} = \left\{ p_i, 1 \le i \le N \right\}, p_i \in \left\{ -1, 1 \right\} \tag{2}$$

(iii) A chaotic signal was subsequently generated according to Lorenz equation [28], with $\rho = 28$, $\sigma = 10$ and $\beta = 8/3$.

(iv) The resultant signal was then sorted (in ascending order) and then used to determine the embedding positions. The product of watermark and pseudo-random sequences $\left(s_i \cdot p_i \right)$ at a given position was then reordered with respect to the sorted Lorenz index (Fig. 3). It is worth emphasizing here that typically $\left(s_i \cdot p_i \right)$ would be directly embedded in the specified domain. In this step, however, its locations were first shuffled based on their respective Lorenz values. This made it harder to decipher the sequence.

(v) The two-level two-dimensional DWT of size *M*×*M* was computed for the QR image $\left(I_i \right)$.

(vi) The watermark obtained from step (iv) was then embedded onto HH_2 sub-band of the QR DWT according to the rule given by Eq. (3)

$$I_i' = I_i + \alpha \left(s_i \cdot p_i \right); i = 1, 2, ..., N \tag{3}$$

where I_i and I_i' is the input and output (watermarked) images, respectively; α is a constant magnitude factor, determining the watermark blending strength.

(vii) An inverse DWT (IDWT) was subsequently applied to the blended signal, resulting in the final watermarked image.

Index 1	Lorenz
1	-13.4006
2	-12.9049
3	13.4055
4	11.6934
5	9.9640
6	8.5908
7	7.2619
8	5.9932
9	16.5154
10	15.0371

→

Index 2	Lorenz
1	-13.4006
2	-12.9049
8	5.9932
7	7.2619
6	8.5908
5	9.9640
4	11.6934
3	13.4055
10	15.0371
9	16.5154

→

$\left(s_i \cdot p_i \right)$	
Original	Reordered
1	1
-1	-1
-1	1
1	-1
-1	-1
-1	-1
-1	1
1	-1
1	1
1	1

Fig. 3. An example of Lorenz calculation (left), sorted index (middle) and re-ordered watermark and pseudo-random sequences (right).

2.2 Watermark Extraction

The process of watermark extraction was blinded in a sense that it did not require the original QR code image in order to recover the embedded watermark. The prediction of its original pixels was however needed. In our scheme, this prediction was performed by using a noise elimination method with a 3×3 averaging filter. The steps involving in watermark extraction were outlined in Fig. 4 and described as follows:

(i) The predicted image $\left(\hat{I}_i\right)$ was obtained by convoluting the input watermarked image $\left(I_i'\right)$ with a spatial averaging kernel. Specifically, the value of a predicted pixel is defined as

$$\hat{I}_i = \frac{1}{c \times c} \sum_{i}^{c \times c} I_i' \tag{4}$$

where c is the kernel size.

(ii) The watermarked and predicted images were then transformed using a two-level two-dimensional DWT independently, where their HH_2 sub-bands were passed to the next step.

(iii) $\left(\hat{s}_i \cdot p_i\right)$ was computed as the difference between the HH_2 sub-bands of $\hat{I}_i$ and I_i' according to the expression:

$$\delta = I_i' - \hat{I}_i = \alpha \cdot \hat{s}_i \cdot p_i \tag{5}$$

(iv) The actual embedded bit $\left(\hat{s}_i \cdot p_i\right)$ was then given by the signed of this difference:

$$sgn(\delta_i) = \hat{s}_i \cdot p_i \tag{6}$$

(v) The watermark $\left(\hat{s}_i\right)$ was then estimated by multiplying these embedded bits with the pseudo-random sequence. Unless the sequence was generated with the exactly identical key as that at the message source, the extraction would not possibly yield the correct watermark.

(vi) The extracted bits were subsequently reordered according to the embedding positions (obtained from factored chaotic signal) and then non-linearly filtered, whereby a pixel of –1 was replaced with that of 1 only if its neighbors are all equaled to 1.

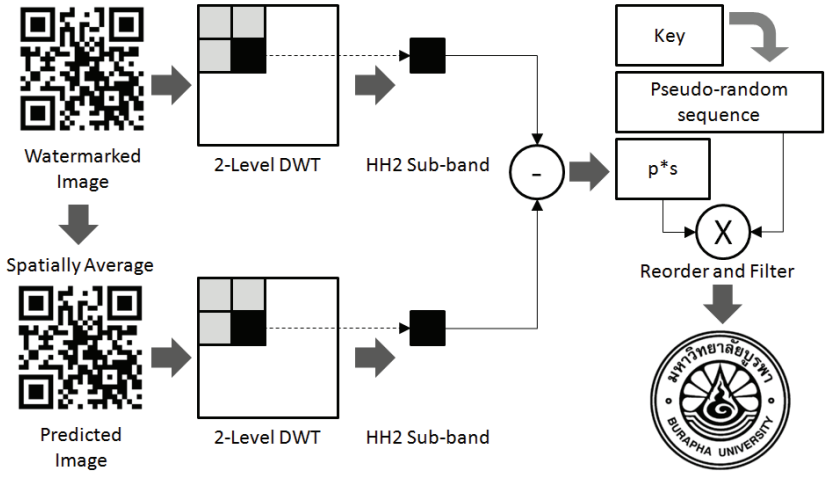


Fig. 4. A diagram outlining the proposed extraction process.

3. Experimental Settings

3.1 Performance Evaluation

To evaluate the performance of the proposed scheme, a similarity measure was computed between the original ($\mathbf{S}$) and extracted (predicted) ($\hat{\mathbf{S}}$) watermarks. The results reported as follow were based upon normalized correlation (NC), as given in Eq. (7).

$$NC = \frac{\sum_{i=1}^{M} \mathbf{S}_i \mathbf{S}'_i}{\sum_{i=1}^{M} \mathbf{S}^2{}_i} \tag{7}$$

In addition, the quality of the watermarked image $\left(I'\right)$ compared with the original one $\left(I\right)$ was also measured using the peak signal-to-noise ratio (PSNR), as given in Eq. (8).

$$PSNR = 10\log \frac{\left(2^b - 1\right)}{\left(\frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(I\left(i,j\right) - I'\left(i,j\right)\right)^2\right)} \tag{8}$$

where b is the number of bits specifying pixel depth and $m \times n$ is the image dimension.

3.2 Simulation Setups

In the following experiment a QR code image of size 400×400 pixels and a university logo as depicted in Fig. 1 were used as the source and watermark images, respectively. The watermarking process was evaluated with the strength magnitudes (α) ranging from 5 to 45, at an interval of 5. The encoding and decoding key were set to 200.

Table 3. PSNR and NC values at different strengths

α	PSNR	NC	
		Without filter	With filter
5	51.2137	0.82	0.8454
10	43.4484	0.843	0.8682
15	39.804	0.8564	0.8787
20	37.6518	0.8823	0.8979
25	35.7863	0.903	0.9128
30	34.1389	0.9106	0.9178
35	32.6409	0.9139	0.9195
40	31.5692	0.9156	0.9212
45	30.6379	0.9177	0.9228

4. Results and Discussions

Table 3 shows the PSNR and NC computed at different magnitudes. In all cases, the QR codes were reconstructed correctly. It can be noticed that a high value of magnitude would yield a relatively low PSNR; hence, it distorted the QR image. However, as the magnitudes increased, the extracted watermark became less polluted with noise and thus had increased NC values as shown in Table 4. This tradeoff between PSNR and NC suggested an empirical choice of optimal magnitude factor of 25. It is also worth noting here that as the process was blinded, i.e., the original QR code was not assumed during the extraction, various extents of noises were thus apparent. This contamination could be effectively reduced by simply applying an average or other assorted filters.

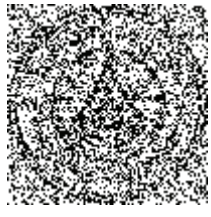
Table 4. Comparison of extracted watermarks at different strengths

α	Without filter	With filter	α	Without filter	With filter
5			10		
15			20		
25			30		
35			40		

Table 5. Effects of various attacks on PSNR and NC, at the optimal value of $\alpha = 25$

Attack type	PSNR	NC	
		Without filter	With filter
No attack	35.7863	0.903	0.9128
Salt and Pepper noise (0.01)	22.9449	0.7681	0.7985
Gaussian noise (0.01)	22.0505	0.2728	0.2783
JPEG (Q=50)	34.3687	0.5646	0.5905
Blurring (Disk)	23.6781	0.3048	0.3165
Resize (200%)	-	0.8846	0.9014

Table 6. Extracted watermark after different attacks

Attack type	Image with watermark	Watermark extraction	Watermark extraction (with filter)
Salt and Pepper noise (0.01)			
Gaussian noise (0.01)			
JPEG (Q=50)			
Blurring (disk filter)			
Resize (200%)			

Indeed, an image can generally be corrupted by unpredictable noise while being transmitted via the network or distorted by lossy compression. We therefore assessed the robustness of the proposed scheme against some typical attacks. They included salt and pepper noise, Gaussian noise, JPEG compression, blurring and resizing. Table 5 lists the effect of various attacks on image PSNR and NC of the embedded watermark. It can be noted from the table that all the attacks gave similar degrees of PSNR. When comparing the NC values, only salt and pepper noise and resizing had little effects on the extracted watermark while the others (e.g., Gaussian and blurring filter) may result in severely degraded extraction. This remark was confirmed in Table 6 that despite such attacks the extracted watermark remained clear while in other cases they were barely recognizable. As for the authentication purpose, the extracted watermarks were nonetheless functional.

5. Conclusion

In this paper, a novel digital watermarking scheme that incorporated the chaotic signal was proposed. The watermarking process was carried out on a two-dimensional wavelet domain of the binary images. The watermark was then embedded in a high frequency sub-band (HH2). In order to tighten the security measure, the Lorenz chaotic signal processing was adopted to determine the embedding position of the watermark. The experiments reported herein indicated that the proposed scheme could reconstruct the watermarked image with an acceptable visual quality and the proposed watermarking could withstand various attacks during transmission. In fact, should the proposed scheme were applied to a video sequence, a trivial temporal averaging filter could significantly help improving the visual appearance of the reconstructed images.

References

[1] C. I. Podilchuk and E. J. Delp, "Digital watermarking algorithms and applications," *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, 2001.

[2] W. N. Cheung, "Digital image watermarking in spatial and transform domains," in *Proceeding of TENCON*, Kuala Lumpur, Malaysia, 2000, pp. 374-378.

[3] N. V. Dharwadkar and B. B. Amberker, "An adaptive gray-scale image watermarking scheme using smooth and edge areas of an image," in *Proceeding of International Conference on Intelligent Systems and Signal Processing*, Gujarat, India 2013, pp. 66-71.

[4] E. Walia and A. Suneja, "Fragile and blind watermarking technique based on Weber's law for medical image authentication," *IET Computer Vision*, vol. 7, no. 1, pp. 9-19, 2013.

[5] Y. Rangsanseri, J. Panyavaraporn, P. Thitimajshima, "PCA/wavelet based watermarking of multispectral images," *Proceeding of International Symposium on Remote Sensing*, Jeju, Korea, 2005.

[6] A. Kaarna and P. Toivanen, "Digital watermarking of spectral images in PCA/wavelet transform domain," in *Proceeding of IEEE International Geoscience and Remote Sensing Symposium*, Toulouse, France, 2003, pp. 3564-3567.

[7] M. Barni, F. Bartolini, V. Capellini, E. Magli, and G. Olmo, "Near-lossless digital watermarking for copyright protection of remote sensing Images," in *Proceeding of IEEE International Geoscience and Remote Sensing Symposium*, Toronto, Canada, 2002, pp. 1447-1449.

[8] A. Kunhu and H. Al-Ahmad, "Multi watermarking algorithm based on DCT and hash functions for color satellite images," in *Proceedings of the 9th International Conference on Innovations in Information Technology*, Abu Dhabi, United Arab Emirates, 2013, pp. 30-35.

[9] D. Rosiyadi, S. J. Horng, P. Fan, X. Wang, M. K. Khan, and Y. Pan, "Copyright protection for e-government document images," *IEEE Multimedia,* vol. 19, no. 3, pp. 62-73, 2012.

[10] N. Divecha and N. N. Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images," in *Proceeding of International Conference on Intelligent Systems and Signal Processing*, Gujarat, India, 2013, pp. 204-208.

[11] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *IET Biometrics*, vol. 2, no. 1, pp. 21-27, 2013.

[12] S. Ding, C. Li, and Z. Liu, "Protecting hidden transmission of biometrics using authentication watermarking," in *Proceedings of 2010 WASE International Conference on Information Engineering*, Beidaihe, China, 2010, pp. 105-108.

[13] S. Bekkouch and K. M. Faraoun, "Robust and reversible image watermarking scheme using combined DCT-DWT-SVD transforms**,"** *Journal of Information Processing Systems*, vol. 11, no. 3**,** pp. 406-420, 2015.

[14] M. Benyoussef, S. Mabtoul, M. E. Marraki, and D. Aboutajdine, "Robust ROI watermarking scheme based on visual cryptography: application on mammograms," *Journal of Information Processing Systems*, vol. 11, no. 4**,** pp. 495-508, 2015.

[15] G. Badshah, S. C. Liew, J. M. Zain, and M. Ali, "Secured telemedicine using whole image as watermark with tamper localization and recovery capabilities**,"** *Journal of Information Processing Systems*, vol. 11, no. 4**,** pp. 601-615, 2015.

[16] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Transactions on Information Technology in Biomedicine,* vol. 16, no. 5, pp. 891-899, 2012.

[17] B. J. Jang, S. H. Lee, S. Lim, and K. R. Kwon, "Biological infectious watermarking model for video copyright protection," *Journal of Information Processing Systems*, vol. 11, no. 2**,** pp. 280-294, 2015.

[18] T. Jassim, R. Abd-Alhameed, and H. Al-Ahmad, "New robust and fragile watermarking scheme for colour images captured by mobile phone cameras," in *Proceedings of the 15th International Conference on Computer Modelling and Simulation*, Cambridge, UK, 2013, pp. 465-469.

[19] S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain," in *Proceedings of the 9th International Conference on ICT and Knowledge Engineering*, Bangkok, Thailand, 2011, pp 47-52.

[20] J. Panyavaraporn, P. Horkaew, and W. Wongtrairat, "QR code watermarking algorithm based on wavelet transform," in *Proceedings of the 13th International Symposium on Communications and Information Technologies*, Surat Thani, Thailand, 2013, pp. 791-796.

[21] M. Saikia and S. Majumder, "A joint SVD based watermarking and encryption scheme using chaotic logistic map," *ECTI Transactions on Computer and Information Technology*, vol. 9, no. 2, pp. 101-106, 2015.

[22] E. Chrysochos, V. Fotopoulos, and A. N. Skodras, "Robust watermarking of digital images based on chaotic mapping and DCT," in *Proceedings of the 16th European Signal Processing Conference*, Lausanne, Switzerland, 2008, pp. 1-5.

[23] M. Keyvanpour and F. Merrikh-Bayat, "An effective chaos-based image watermarking scheme using fractal coding," *Procedia Computer Science*, vol. 3, pp. 89-95, 2011.

[24] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dynamics*, vol. 73, no. 3, pp 1469-1474, 2013.

[25] P. Khare, A. K. Verma, and V. K. Srivastava, "Digital image watermarking scheme in wavelet domain using chaotic encryption," in *Proceedings of 2014 Students Conference on Engineering and Systems*, Allahabad, India, 2014, pp. 1-4.

[26] R. Esgandari, M. S. Student, and M. Khalili, "A robust image watermarking scheme based on discrete wavelet transforms," in *Proceedings of the 2nd International Conference on Knowledge-Based Engineering and Innovation*, Tehran, Iran, 2015, pp. 988-992.

[27] S. Mohammadi and S. Talebi, "An image watermarking algorithm based on chaotic maps and wavelet transform," in *Proceedings of the 9th International ISC Conference on Information Security and Cryptology*, Tabriz, Iran, 2012, pp. 135-140.

[28] Wikipedia, "Lorenz equations," [Online]. Available: https://en.wikipedia.org/wiki/Lorenz_system.

Jantana Panyavaraporn https://orcid.org/0000-0003-2554-0276

She is an assistant professor of Electrical Engineering, Burapha University, Thailand. She received her B.Eng. in Electrical Engineering from Burapha University (2002), M.Eng. in Telecommunication Engineering from King Mongkut's Institute of Technology Ladkrabang (2005), and Ph.D. in Electrical Engineering from Chulalongkorn University (2010). Her research interests include image processing, video processing and video coding.

Paramate Horkaew https://orcid.org/0000-0003-0879-7125

He received his B.Eng. (First Class Honors) in Telecommunication Engineering (1999) from King Mongkut's Institute of Technology Ladkrabang, Thailand and Ph.D. in Computer Science from Imperial College London, University of London, London, UK (2004). He is an assistant professor at the School of Computer Engineering, Suranaree University of Technology, Thailand. His main research interests include computational anatomy, digital geometry processing, computer vision and graphics.