

Improvement of Secret Image Invisibility in Circulation Image with Dyadic Wavelet Based Data Hiding with Run-Length Coded Secret Images of Which Location of Codes are Determined with Random Number

Kohei Arai

Dept. of Information Science,
Saga University
Saga, Japan

Yuji Yamada

Dept. of Information Science
Saga University
Saga, Japan

Abstract— An attempt is made for improvement of secret image invisibility in circulation images with dyadic wavelet based data hiding with run-length coded secret images of which location of codes are determined by random number. Through experiments, it is confirmed that secret images are almost invisible in circulation images. Also robustness of the proposed data hiding method against data compression of circulation images is discussed. Data hiding performance in terms of invisibility of secret images which are embedded in circulation images is evaluated with the Root Mean Square difference between the original secret image and extracted one from the circulation images. Meanwhile the conventional Multi-Resolution Analysis (MRA) based data hiding is attempted with a variety of parameters, level of MRA and the frequency component location of which secret image is replaced to it and is compared to the proposed method. It is found that the proposed data hiding method is superior to the conventional method. Also the conventional data hiding method is not robust against circulation image processing.

Keywords- *Dyadic wavelet; Lifting wavelet; Data hiding; Data compression.*

I. INTRODUCTION

Wavelet analysis applications are getting more popular in time series analysis, image analysis, information security area, etc.[1],[2]. Data hiding is important for information contents security, in particular, for protection of copy right. Using data hiding methods, some important information such as copyright, signature, etc. can be embedded. Data hiding based on wavelet analysis, in particular, Multi-Resolution Analysis: MRA is widely used. One of the problems on data hiding methods is visibility of the embedded information on the available circulation images [3]-[7]. The other problem is robustness against image processing which is applied to the circulation images including data compressions. It sometime occurs that small amount of information on the embedded image appears on the circulation images slightly due to the embedding mechanism of the data hiding.

In order to improve invisibility of the secret images in the circulation images, run-length coded binarized secret images are used. The locations of the codes after the data compression in one of the frequency component images after the dyadic wavelet transformation [8] are determined with random numbers generated by Mersenne Twister of random number generator. After all, reconstructed image (inverse dyadic wavelet transformation) is used for circulation. The original secret images are almost invisible in the circulation images. This paper deals with the current problems on the widely used MRA based data hiding method (Conventional data hiding method). One of the problems is visibility of secret image in the circulation images followed by robustness against circulation image manipulations including image deformation, geometric conversion, data compression, etc. In order to overcome the aforementioned problems, a method for data hiding based on lifting dyadic wavelet transformation with run-length coding of data compression which is applied to secret image together with pixel order exchange is proposed. First, the aforementioned problems of the conventional MRA based data hiding method are discussed followed by the proposed method. Then robustness against JPEG and JPEG 2000 of data compression is discussed in the paper.

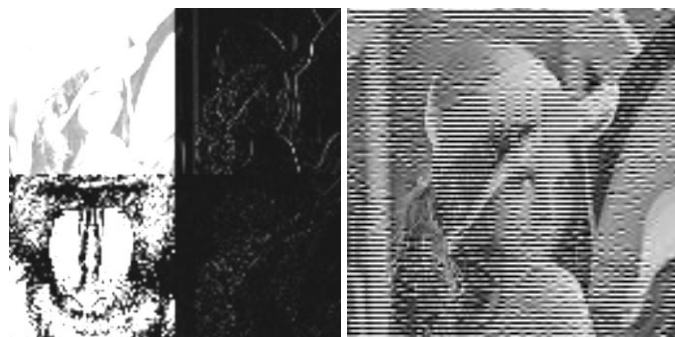
II. PROPOSED METHOD

A. Conventional wavelet based data hiding methods

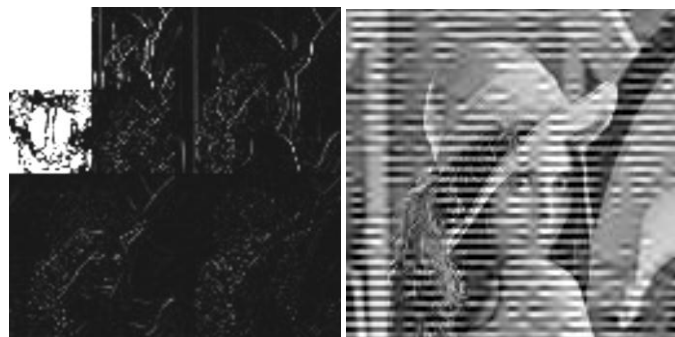
Wavelet utilized MRA allows decompose the image with wavelet coefficients (high and low frequency components) and also the original image can be reconstructed with the decomposed wavelet coefficients perfectly. If the high frequency component is replaced with secret image to be hidden, and if the reconstructed image is circulated to public, then secret image can be extracted from the circulated image if receiver knows which component is replaced with secret image. In this case, secret image has to be invisible in the circulated image. Also even if image processing including geometric conversion (linear transformation) and data compression (non-linear transformation) is applied to the circulated image, secret

image has to be extracted. The aforementioned “invisibility” and “robustness against image processing” are very important for data hiding.

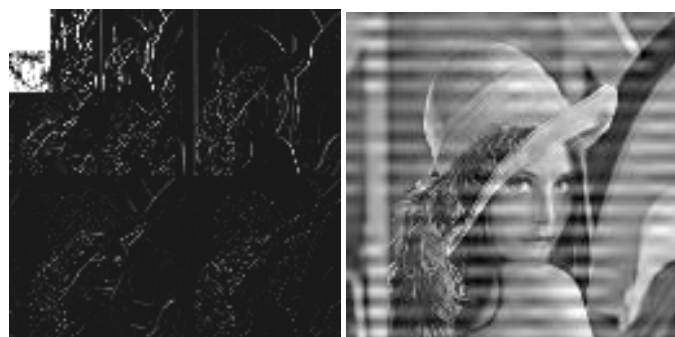
One of the examples of conventional MRA based data hiding is shown in Figure 1. The original image size is 128 by 128 pixels while the secret image size (binary) is 64 by 64 pixels for Figure 1 (a) and 32 by 32 pixels for Figure 1 (c) as well as 16 by 16 for Figure 1 (e), respectively. If the secret image is inserted at the HL (High and Low frequency components in horizontal and vertical directions) component of MRA image, and if reconstructed with the secret image, then secret image is somewhat visible in the reconstructed image which is circulation image to public.



(a) MRA image with secret image (b) Reconstructed image (Level 1)



(c) MRA image with secret image (d) Reconstructed image (Level 2)



(e) MRA image with secret image (f) Reconstructed image (Level 3)

Figure 1: Resultant images of wavelet based MRA which contains the secret image of Mandrill (left bottom), LL (left top), LH (right top), and HH (right bottom) as well as reconstructed image (circulation image) which contains embedded secret image

Invisibility of the secret image depends on base function of wavelet, level of the MRA stages. In general, secret image is

getting much invisible in the reconstructed image in accordance with increasing of level of MRA. Furthermore, secret image is much invisible in the reconstructed image when the secret is replaced to HL, LH, or HH frequency components, rather than LL components. In other word, secret image would better to hide at higher frequency components rather than low frequency component because human eyes has low pass filter of frequency response.

Root Mean Square (RMS) difference between the original image and reconstructed image which contains secret image in LH, or HL, or HH with the level of MRA, i based on Daubechies base function with support length of j which is denoted as Db_j is shown in Table 1. In this case, i is 1, 2, and 3 while j is 2, 4, and 8, respectively.

It is obvious that RMS difference is decreased in accordance with increasing of level. It is unclear that relation between RMS difference and support length. The replaced component of HH seems to be better RMS difference in comparison to the other HL, LH components. Some examples of reconstructed images with MRA based data hiding are shown in Figure 2. By comparing these, it is found that the location of frequency component of which the secret image is replaced is the most influencing factor (the best location for replacing secret image is HH) followed by the level of which the secret image is replaced. Meanwhile, support length of Daubechies base function is not so influencing in comparison to the other factors.

TABLE 1 Root Mean Square: RMS difference between the original image and reconstructed image containing secret image (Lv_i : Level of MRA, Db_j : Daubechies base function with support length of j).

RMS Difference			
Lv_1	Db_2	Db_4	Db_8
LH	78.25	77.17	77.26
HH	78.27	77.26	77.41
HL	78.91	77.64	77.61
Lv_2	Db_2	Db_4	Db_8
LH	43.57	42.75	43.68
HH	43.8	41.04	43.93
HL	45.2	43.71	44.44
Lv_3	Db_2	Db_4	Db_8
LH	21.27	21.51	20.78
HH	20.94	20.97	20.86
HL	24.84	25.05	23.77





Figure 2 Some examples of reconstructed images of MRA based data hiding (lv_i db_j denotes i level and Daubechies base function with support length of j, respectively)

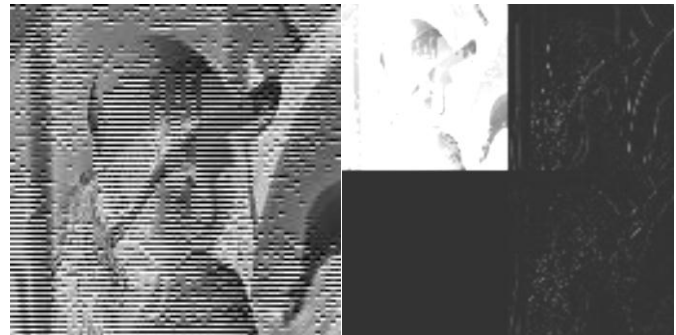
B. Robustness against image processing, intensity inversion, up-side-down of geometric conversion, magnification

Even if someone applies image manipulation to the circulation images, the secret image has to be extracted.

In order to confirm such robustness of data hiding against image manipulation or processing, intensity inversion, up-side-down of geometric conversion as well as magnification (twice large size) are applied to the circulation image and then extraction of the secret image is attempted. Resultant images with the different level of MRA (1 and 3) are shown in Figure 3. In these cases, Daubechies base function with support length of 8 is utilized for MRA. Although the extracted secret image of Mandrill in the case of magnification is poorly and is better than the other cases. Conventional MRA based data hiding is not robust against image processing applied to circulation images except magnification. Poor quality of the secret image of Mandrill can be seen in the extracted image of Figure 3 (n).



(c)Reconstructed:LH_Lv1_Db8 (d)Extracted:without image process



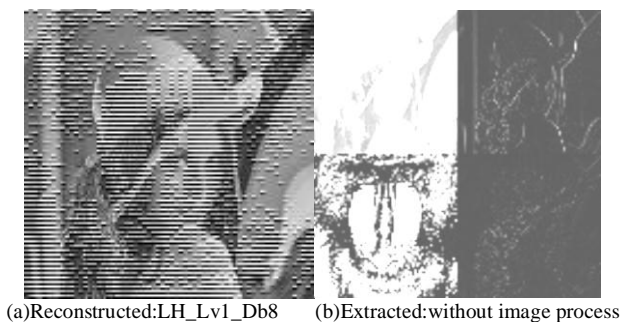
(e)Reconstructed:LH_Lv1_Db8 (f)Extracted image:Intensity inversion



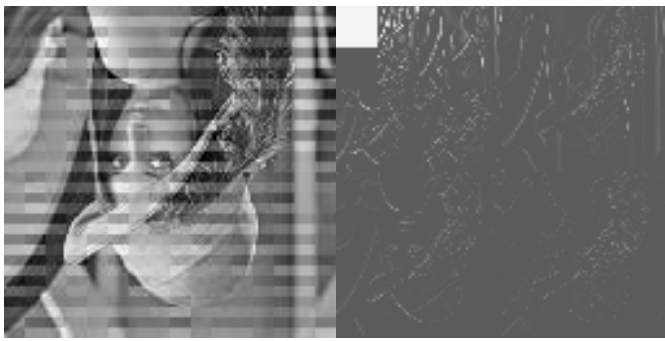
(g)Reconstructed:LH_Lv3_Db8 (h)Extracted image: Intensity inversion



(i)Reconstructed:LH_Lv1_Db8 (j)Extracted image:up-side -down conversion



(a)Reconstructed:LH_Lv1_Db8 (b)Extracted:without image process



(k)Reconstructed:LH_Lv3_Db8 (l)Extracted image:up-side -down conversion



(m)Reconstructed:LH_Lv1_Db8 (n)Extracted image:Magnification



(o)Reconstructed:LH_Lv3_Db8 (p)Extracted image:Magnification

Figure 3 Robustness of the proposed data hiding against image processing, intensity inversion, up-side-down of geometric conversion, magnification with the different level of MRA of which the secret image is replaced to it.

C. Proposed data hiding method based on lifting dyadic wavelet transformation with secret image manipulations with run-length coding and pixel order exchanges of permutation using random number

The proposed method for data hiding is based on dyadic wavelet transformation. Dyadic wavelet allows to separate frequency components keeping image size with that of original image. Dyadic wavelet is called as a binary wavelet and has high pass and low pass filter components, $\{h[k], g[k]\}$ and reconstruction filter $\{\underline{h}[k], \underline{g}[k]\}$. Low and high frequency components, C_n and d_n are expressed as follows,

$$C_n [i]=\sum_k h[k] C_{n-1} [i + k2^{n-1}] \quad (1)$$

$$d_n [i]=\sum_k g [k] C_{n-1} [i + k2^{n-1}] \quad (2)$$

Then original image is also reconstructed with the low and high frequency components as follows,

$$C_{n-1} [i]=1/2\sum_k \underline{h}[k] C_n [i-k2^{n-1}]+\sum_k \underline{g}[k] d_n [i-k2^{n-1}] \quad (3)$$

If a new parameter $s[m]$ is employed, then lifting dyadic wavelet is defined as follows,

$$h^{new}[k]=h^{old}[k] \quad (4)$$

$$\underline{h}^{new}[k]=\underline{h}^{old}[k] + \sum_m s[-m] \underline{g}^{old}[k-m] \quad (5)$$

$$g^{new}[k]=g^{old}[k] - \sum_m s[m] h^{old}[k-m] \quad (6)$$

$$\underline{g}^{new}[k]=\underline{g}^{old}[k] \quad (7)$$

Figure 4 shows a schematic process flow of the proposed data hiding based on lifting dyadic wavelet transformation. It is possible to hide the embedded image at the certain location of wavelet transformation images then circulation images containing the embedded image can be reconstructed through inverse wavelet transformation. In this case, although binary secret images are assumed, half tone, colored images are also available for secret images.

First, secret image is binarized. Before binarized secret images are replaced to one of the high frequency component images, run-length coding is applied to secret images in order to improve an invisibility of the secret images in the circulation images. Figure 5 shows schematic process flow of the run-length coding method. The number of pixels in the original binary image is 27 while the number of pixels in the compressed image is just 6 (quantization level is variable).

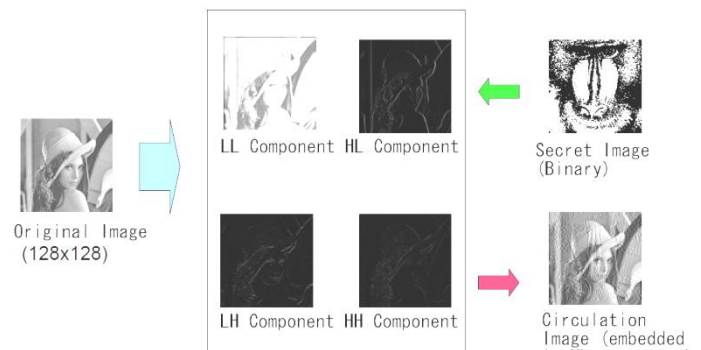


Figure 4 Schematic process flow of the proposed data hiding

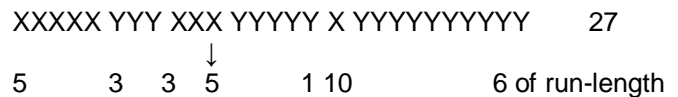


Figure 5 Schematic process flow of run-length coding.

Then run-length coded data are replaced to one of the high frequency components with the pixel order exchanges based on generated random numbers which are generated by Mersenne Twister. Only if the receiver who knows the initial value of random number of Mersenne Twister and how to decode run-length coding, then such the receiver can extract the secret images. Thus the copy right holders can assert their copy right through extraction of secret images. Figure 6 shows the process flow of the proposed data hiding (hide the secret image into the original image and create circulation image embedded the secret image then extract the secret image from the circulation image)

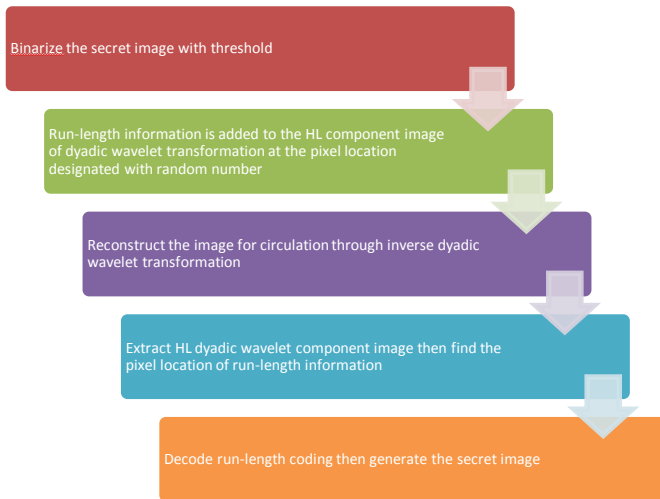


Figure 6 Process flows of the proposed data hiding method

III. EXPERIMENTS

A. Dyadic wavelet based data hiding methods

In Figure 7, the secret binary image of Mandrill [9] with a certain threshold is embedded in the HL component of the dyadic wavelet transformed images derived from the original image of Lena [9] with dyadic wavelet transformation. At the left bottom corner of Figure 7, a reconstructed image (image for circulation) is shown. The secret image can be recognizable in the circulation image, unfortunately. In these cases, Daubechies wavelet base function (support length=2) [10] is used. On the other hand, Figure 7 (b),(c),(d) shows reconstructed images of Mandrill of secret image (a) embedded Lena of original images of which the secret image is embedded at the LH, HH, and HL of frequency components, respectively. Image size is not changed for original and dyadic wavelet transformed images.

Table 2 shows RMS difference between original and reconstructed images for dyadic wavelet based data hiding. In this case, RMS difference of Daubechies base function utilized dyadic wavelet is compared to that of Haar base function. The difference is quite obvious that Daubechies base function utilized dyadic wavelet is superior to that of Haar base function.

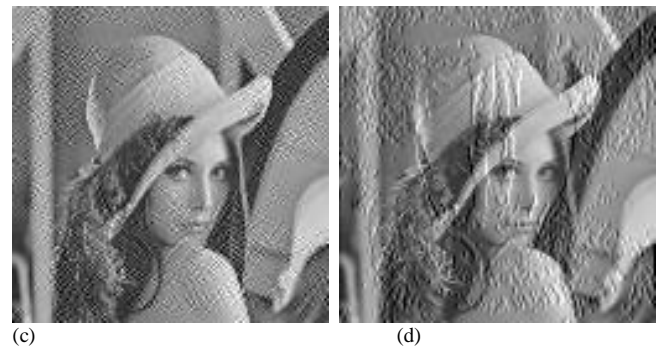
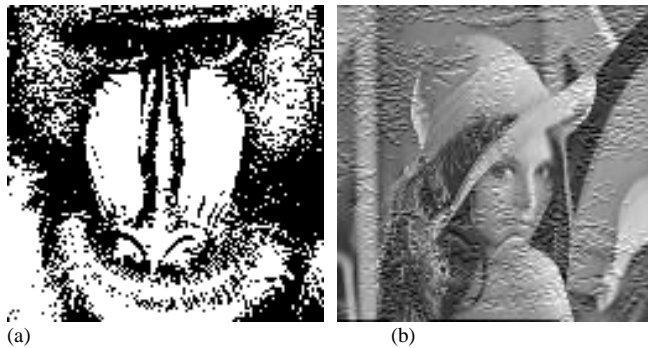


Figure 7 (a) The secret image of Mandrill, (b) Reconstructed image of Mandrill image embedded (LH) Lena image for circulation, (c) Reconstructed image of Mandrill image embedded (HH) Lena image for circulation, (d) Reconstructed image of Mandrill image embedded (HL) Lena image for circulation.

TABLE 2: RMS difference between original and reconstructed images for dyadic wavelet based data hiding.

Lv_1	Haar	Db_2
LH	43.65	24.15
HH	38.90	20.58
HL	42.67	23.42

B. Data hiding method with run-length coding and pixel order exchange based on random number (permutation matrix operation)

As shown in Figure 7, the binarized secret image of Mandrill is recognizable in the reconstructed image (circulation image). The propose data hiding method is to apply run-length coding to the binarized secret image in concern before replacing the secret image to one of high frequency components, HL, LH and HH. Also bit stream order exchange is applied to the run-length coded compressed data.

As is aforementioned in the reference [6] and [7], invisibility of the secret image is improved remarkably by scanning scheme (permutation of pixel order of the secret image in accordance with random number). Mersenne Twister [11] of random number generator is used for the permutation.

Figure 8 (a) shows LH frequency component image embedded with the binarized secret binary image of Shuttle cock with the threshold of 15 and with permutation by Mersenne Twister of random number generator while Figure 8 (b) shows the reconstructed image for circulation for the case of (a). Meanwhile, Figure 8 (c) shows LH frequency component image embedded with the binarized secret binary image of Shuttle cock with the threshold of 255 and with permutation by Mersenne Twister of random number generator while Figure 8 (d) shows the reconstructed image for circulation for the case of (c). Figure 8 (e) shows the secret image of Shuttle cock. Also Figure 8 (f) is the binarized Shuttle cock. As are shown in Figure 8 (g) and (h), Gray scale image and Binarized Mandrill has too many black pixels so that the Shuttle cock of secret image is used in the experiments.

Table 3 shows the relations between threshold and total data amount of compressed data as well as RMS difference. In accordance with increasing of threshold, the number of black pixels is decreased so that total data amount after the run-length coding is also decreased.

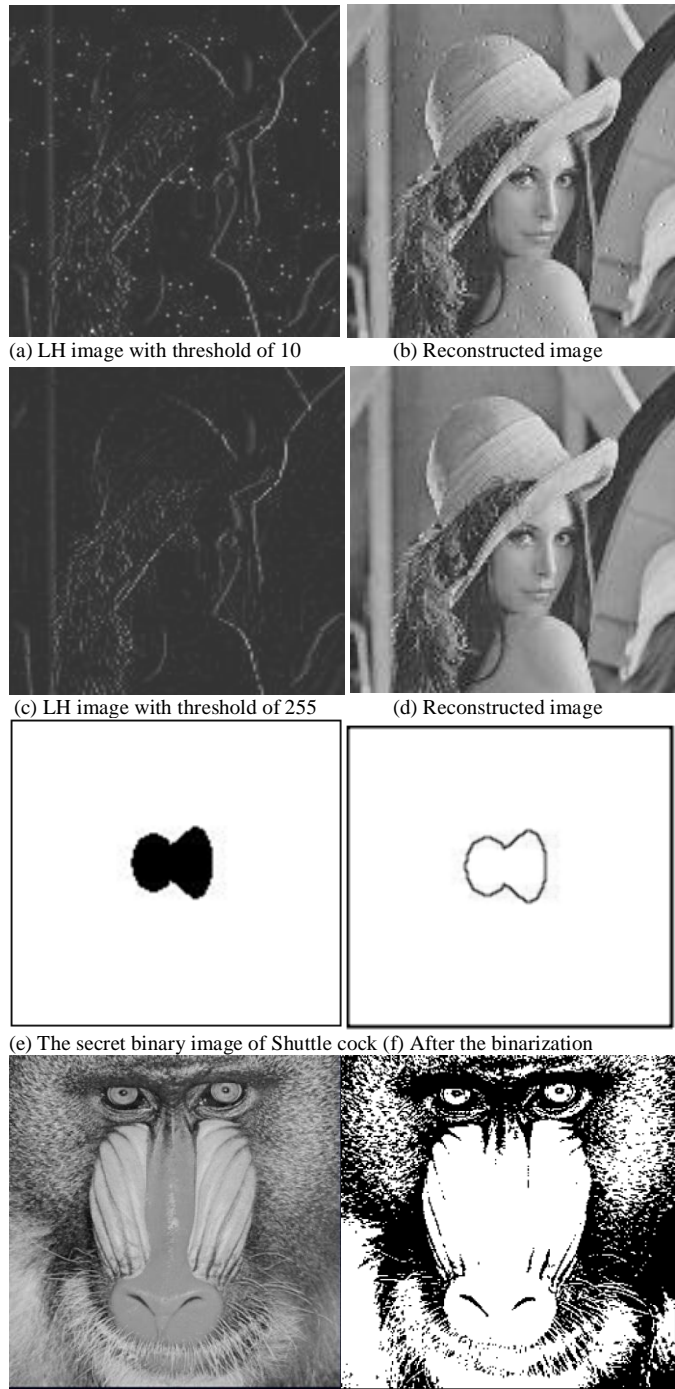


Figure 8 (a) LH frequency component image embedded with the binarized secret binary image of Shuttle cock with the threshold of 15 and with permutation by Mersenne Twister of random number generator, (b) the reconstructed image for circulation for the case of (a), (c) LH frequency component image embedded with the binarized secret binary image of Shuttle cock with the threshold of 255 and with permutation by Mersenne Twister of random number generator, (d) the reconstructed image for circulation for the

case of (c), (e) the secret image of Shuttle cock, (f) the binarized Shuttle cock, (g) Gray scale image of Mandrill and (h) Binarized Mandrill.

TABLE 3: Relations between threshold and total amount of compressed data as well as RMS difference.

Secret image	Threshold	Total data amount	RMS difference
Shuttle Cock	255	133	3.65
	15	1140	1.71

Bit stream order of the compressed data is exchanged based on random number. After that the exchanged bit stream is embedded into LH image. Then image for circulation is reconstructed with HL, HH and LL images together with secret image embedded LH image. The reconstructed image with threshold 15 and 255 which are shown in Figure 8 (b) and (d) are better quality image in comparison to the images which are shown in Figure 6. RMS difference between reconstructed image and the original image is shown in Table 3. RMS difference of 1.71 is negligible comparing to that of 24.15 of dyadic wavelet based data hiding method.

Figure 9 shows the relation between the number of pixels and RMS difference as well as total data amount. The number of pixels implies that the number of black pixels after the binarisation with the designated threshold so that it depends on the threshold.

The number of pixels is increased with decreasing of threshold. As is shown in Figure 9, the minimum of RMS difference is situated at 15 of the number of pixels. The total amount of data in unit of bit means the compressed data amount with run-length coding. The shuttle cock of secret image is binarized and replaced to LH component of dyadic wavelet transformed image results in circulation image. After that, the circulation image is compressed with run-length coding. The compressed data amount depends on the number of pixels of the binarized secret image which depends on threshold. In these cases, the location of frequency component for replacing secret image of HH and LH shows almost same RMS difference and these are better than the RMS difference of HL component. This implies that the location of HH or HL is more appropriate rather than LH component.

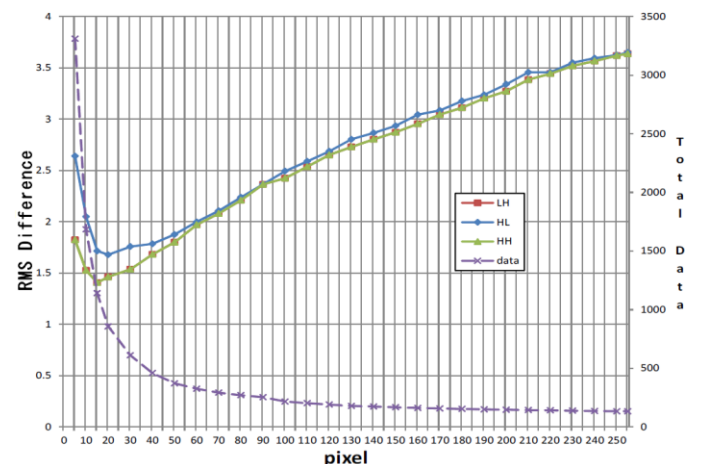


Figure 9 Relation between the number of pixels and RMS difference as well as total data amount.

C. Robustness of the proposed data hiding method against the data compressions, JPEG and JPEG 2000

The proposed method is also applied to the other data compression methods of JPEG and JPEG 2000. Figure 10 shows a small portion of decompressed images of JPEG and JPEG 2000 with data compression ratio of 100.

It is obvious that decompressed image of JPEG has block distortions while that of JPEG 2000 has not such distortion. Also much larger mosquito noise is found in the decompressed image of JPEG rather than JPEG 2000 as well. Peak signal-to-noise ratio PSNR of JPEG 2000 as a function of bit rate is greater than that of JPEG for the "Lena" image as is shown in Figure 11.



Figure 10 Enlarged portions of images of decompressed images of JPEG and JPEG 2000 with data compression ratio of 100.

After dyadic wavelet transformation is applied to the original image and HH component of the transformed image is replaced with the permuted Mandrill of secret image with random number, reconstruction image (circulation image) is generated with inverse dyadic wavelet transformation. After that JPEG and JPEG 2000 of data compression is applied to the circulation image. Using the compressed images, secret image can be extracted with decompression and inverse dyadic wavelet transformation together with inversely permutation by the same random number which is generated by Mersenne Twister.

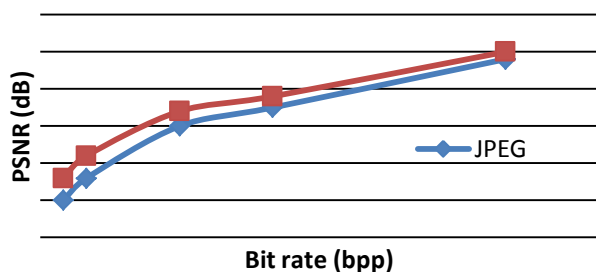


Figure 11 PSNR of JPEG and JPEG 2000 as a function of bot rate.

Figure 12 shows the circulation images with embedded secret image of Mandrill with the data compression by JPEG and JPEG 2000 with the same permutation by the same random number which is generated by Mersenne Twister. In the images, defect due to secret image with permuted by random number is visible because the binalization of parameter of threshold is

set at 255. Although both images are quite similar, details are different as is mentioned before.

After the extraction of secret image, RMS difference between the original secret image and the extracted secret image is calculated. The results show that RMS difference for JPEG data compression is 6.38 while that for JPEG 2000 is totally equal to zero because JPEG 2000 is information loss less coding while JPEG is information lossy coding.



Figure 12 Circulation images with embedded secret image of Mandrill with the data compression by JPEG and JPEG 2000 with the same permutation by the same random number which is generated by Mersenne Twister

IV. CONCLUSIONS

It is found that MRA based conventional data hiding is not robust against image processing, intensity inversion, up-side-down of geometric conversion, and magnification. Secret image is much visible in the circulation images rather than the proposed lifting dyadic wavelet transformation based data hiding method. It is found the best location of component of MRA resultant images of which the secret image is replaced to it. Also the best level of MRA as well as support length of Daubechies base function for minimization of visibility of the secret image in the circulation images are found.

The proposed data hiding method is robust against data compression, JPEG and JPEG 2000. Also the secret image in circulation images with the proposed method is much invisible rather than the conventional method. Because the proposed method uses random number utilized pixel order exchanges for the secret images together with run-length coding of data compression. In the reconstruction process, scheme and initial value of the random number generator is known by receivers so that it is possible to reconstruct the embedded secret images from the circulation images. In this research, the secret image is binarized. The most appropriate threshold which allows minimization of RMS difference between extracted secret image and the original secret image is also found.

ACKNOWLEDGMENT

The authors would like to thank all the teaching staff and the students in the research group for their valuable comments and suggestions through conducting this research work.

REFERENCES

- [1] Kohei Arai, Fundamental Theory on Wavelet Analysis, Morikita Shuppan Publishing Co. Ltd., 2000.
- [2] Kohei Arai, Self Learning on Wavelet Analysis, Kindai-Kagakusha publishing Co. Ltd., 2006.

- [3] Kohei Arai and Kaname Seto, Data hiding method based on Multi-Resolution Analysis: MRA, Visualization Society of Japan, 22, Suppl.No.1, 229-232, 2002.
- [4] Kohei Arai and Kaname Seto, Data hiding method with coordinate conversion in feature space, Visualization Society of Japan, 25, Suppl.No.1, 55-58, 2005.
- [5] Kohei Arai and Kaname Seto, Improvement of invisibility of secret images embedded in circulate images based on MRA with coordinate conversion and Principal Component Analysis: PCA, Journal of Image and Electronics Society of Japan, 36, 5, 665-673, 2007.
- [6] Kohei Arai and Kaname Seto, Improvement of invisibility of secret images embedded in circulate images based on MRA with scanning scheme conversion, Visualization Society of Japan, 29, Suppl.No.1, 167-170, 2009.
- [7] Kohei Arai, Improvement of security and invisibility of secret images embedded in circulate images and based on MRA, Report of RIMS-Research Institute for Mathematical Sciences Kyoto University, ISSN188-2818,1684,93-113,2010.
- [8] S.Mallat and S.Zhong, "Characterization of signals from multiscale edges," IEEE Trans. Pattern Anal. Machine Intell., 14, pp.710-732, 1992.
- [9] http://vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/ (Accessed on March 11 2011).
- [10] Kohei Arai and Leland Jameson, Earth observation satellite data analysis based on wavelet analysis, Morikita-Shuppan Publishing Co., Ltd., 2001.
- [11] <http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/mt.html> (Accessed on March 11 2011).
- [12] Takagi and Shimoda Edt., Kohei Arai et al., Image Analysis Handbook, Tokyo University Shuppan-Kai, 1991.
- [13] M. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Image Processing, vol. 9, no. 8, pp. 1309–1324, Aug. 2000, originally as Hewlett-Packard Laboratories Technical Report No. HPL-98-193R1, November 1998, revised October 1999.
- [14] <http://www.uw-de.com/jpeg2000/>(Accessed on March 11 2011).

AUTHORS PROFILE

Kohei Arai received a PhD from Nihon University in 1982. He was subsequently appointed to the University of Tokyo, CCRS, and the Japan Aerospace Exploration Agency. He was appointed professor at Saga University in 1990. He is also an adjunct professor at the University of Arizona and is Vice Chairman of ICSU/COSPAR Commission A.

Yuji Yamada received BS degree of information science from Saga University in 2010 and is now in the master course of graduate school of Saga university.