Access Fee Charging System for Information Contents SharingThrough P2P Communications

Kohei Arai
Graduate School of Science and Engineering
Saga University
Saga City, Japan

***Abstract*—Charge system for information contents exchange through P2P communications is proposed. Security is the most important for this charge system and is kept with data hiding method with steganography and watermarking. Security level for this charge system is evaluated with image contents.**

Keywords-P2P communication; steganography; data hiding; watermarking; charge system; content security

I. INTRODUCTION

Although there are so many charge systems for client-server model of communications, a small number of charge system for P2P communications. From the begging of the information contents exchange and or selling and buying, information content provider is server and the customers are clients. Users' demands, however, are getting large for information contents exchange and or selling and buying through P2P communications. In particular, change system for information contents exchange through P2P communications is getting more necessary.

When users share their files, Instant Messaging: IM, information including voice communications on Internet Protocol: IP networks (VoIP), charge system is highly required. The well known package based digital content business models are no longer work. In order to realize charging system for information sharing, the followings are proposed,

1) gather a fixed amount for information content access fees by the provider side,

2) charge access fees through authentication server.

Users have to have a right for accessing information contents from information providers in the case of (1) while users are charged when they get an authentication from the authentication server (information content access fees may change by amount of information contents) in the case of (2). Internet (or digital) stock company used to use the case of (2).

In the case of (1), there are two major problems, access fees do not depend on accessing information contents, and it require time consumable contraction processes on information sharing services. On the other hands, there is serious problem on information contentaccessing procedure of which users have to get authentication before accessing information contents. Furthermore, it is desired to access information contents directly from users. Moreover, there is no authentication server in the P2P communications.

The following section describes the proposed charge system for information sharing among users through P2P communications followed by some experiments for the key components of the proposed charge system. Finally, conclusion is followed together with some discussions.

II. PROPOSED CHAGE SYSTEM

A. *Blockdiagram, Configuration, and Process Flow of the Proposed Charge System for Informtion Content Sharing Through P2PCommunications*

Process flow of the proposed charge system for information content sharing through P2P communications is shown in Figure 1.

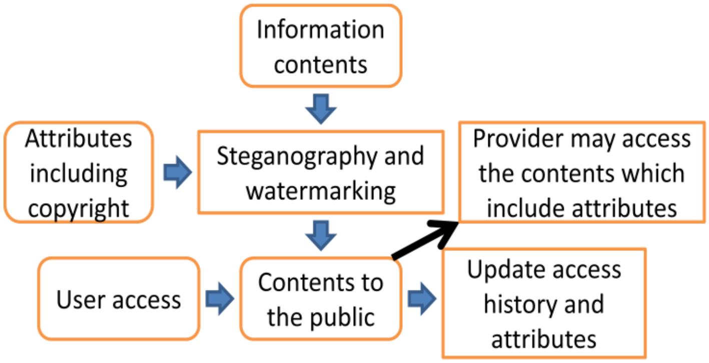

Information contents
Attributes including copyright
Steganography and watermarking
Provider may access the contents which include attributes
User access
Contents to the public
Update access history and attributes

Fig.1. Process flow of the proposed charge system for information content sharing through P2P communications

Attributes include copyright information as well as the other information which are required for charging of access fees and for protect the copyright of the information contents. All the aforementioned attribute information are coded and embedded into the original information contents based on data hiding, steganography and watermarking. Then the attribute information hidden information contents are ready to provide. Data hiding method based on wavelet Multi Resolution Analysis: MRA has been proposed already [1]-[3]. Also the method for keyword extraction from the original documents based on Analytic Hierarchical Process: AHP [1] has been proposed already [4]. Invisibility of hidden documents has also been improved by means of random scanning [5].

Information providers will make web search catalog. When users would like to access the information content in concern through looking at the catalog, the attribute information

[1] http://ja.wikipedia.org/wiki/%E9%9A%8E%E5%B1%A4%E5%88%86%E6%9E%90%E6%B3%95

containing information content in concern is accessed. In the catalog information, there is access fee ("Point" in the proposed system). At that time, attribute information which includes access history is updated automatically. Also the information content provider may look at the attribute information because the information provider, owner of the information content, and copyright holder knows how to reconstruct the attribute information. Thus, the information content provider can protect information contents, copyright, and also can get the information of access history, etc.

The "Point" is updated after the information contents are accessed. Therefore, the "Point" of the information contents providers is increased after the access. The "Point" may be used for accessing the other information contents in the public domain.

Therefore, the "Point" is increased when users' information contents are accessed while users may lose their "Point" when they access the other information content from the other users.

B. Specific Features of the Proposed Cahrge System

The proposed charge system has the following specific features,

1) Information content providers may confirm the facts that receivers (users) access the information contents in concern,

2) Information content providers may protect their copyright because the provided contents include copyright signatures (or forms) based on steganography and watermarking,

3) Information content provider may look at access history parameters such as the number of access, access user ID, the access date, IP address, etc.

4) No real money is required for information contents sharing. Only thing users have to have for information content sharing is the "Point". Therefore, there is no need to provide any personal information at all.

C. Key Components of the Proposed Cahrge System

Key component of the proposed charge system is steganography and watermarking. Wavelet Multi Resolution Analysis: MRA based watermarking method is used. The principle of the method is Laplacian pyramid which is shown in Figure 2.

Even if the general users who do not authenticated at all access to the information contents database server and acquire the information contents, such users could not decryption the original information contents at all because such users do not know the way for decryption of the information contents which are protected by steganography and watermarking.

Original image can be decomposed with horizontally and vertically low as well as high wavelet frequency components based on wavelet MRA which is expressed in equation (1).

$$F=C_n\eta \qquad (1)$$

Where$F$, C_n, and η is wavelet frequency component, wavelet transformation matrix, and input data in time and/or space domain. Because $C_n{}^t=C_n{}^{-1}$, η can be easily reconstructed with wavelet frequency component, F.

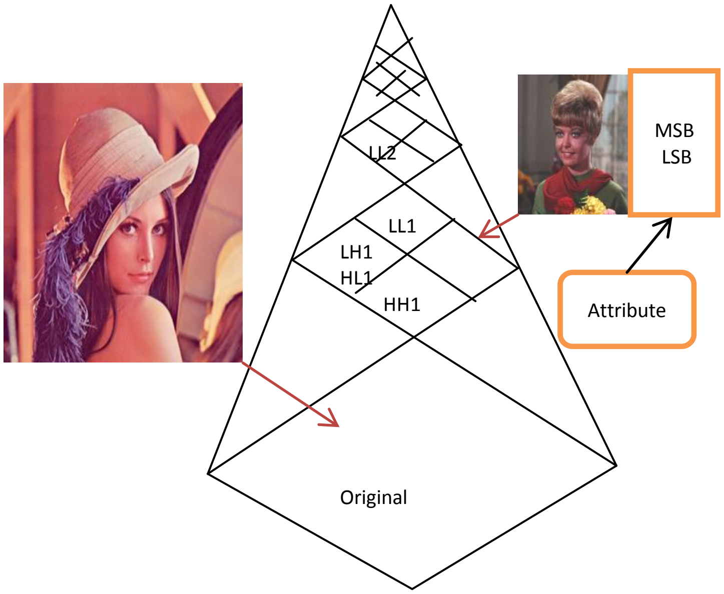


Fig.2. Schematic views of the proposed steganography and watermarking

Equation (1) is one dimensional wavelet transformation and is easily expanded to multi dimensional wavelet transformation.

$$F=(C_n\,(C_m\,(C_l\eta\,)^t)^t)^t\ldots \qquad (2)$$

In the case of wavelet transformation of images, two dimensional wavelet transformation is defined as follows. Horizontally low wavelet frequency component and vertically low frequency component is called LL_1 component at the first stage. Horizontally low wavelet frequency component and vertically high frequency component is called LH_1 component at the first stage.Horizontally high wavelet frequency component and vertically low frequency component is called HL_1 component at the first stage.Horizontally high wavelet frequency component and vertically high frequency component is called HH_1 component at the first stage. Then LL_1 component can be decomposed with LL_2, LH_2, HL_2, and HH_2 components at the second stage. Also LL_2 component is decomposed with LL_3, LH_3, HL_3, and HH_3 components at the third stage as shown in Figure 3.

Thus Laplacian pyramid[2] which is shown in Figure 2 is created. If these four decomposed components, LL_n, LH_n, $HL_{n,}$ and HH_n are given, then LL_{n-1} is reconstructed. Therefore, the original image can be reconstructed with all the wavelet frequency components perfectly.

The copied information contents can be replaced into the designated portion of wavelet frequency component. Furthermore, the Least Significant Bit: LSB is also replaced to the encrypted location of wavelet frequency component in which the copied information contents are replaced. Furthermore, attribute information are also can be embedded to the LSB. LSB data does not affect information contents, in particular for imagery data because imagery data is redundant

[2] http://en.wikipedia.org/wiki/Laplacian_pyramid

enough. Therefore, LSB data is not visible in the information content in the public domain. If the information content in concern is not imagery data, then MSB to LSB-1 bits of data can be used for information contents. Moreover, the encrypted location is randomly scanned with Mersenne Twister[3] of random number generator. Therefore, only the authenticated users who know the parameters of the random number generator can decode the location of the wavelet frequency component.

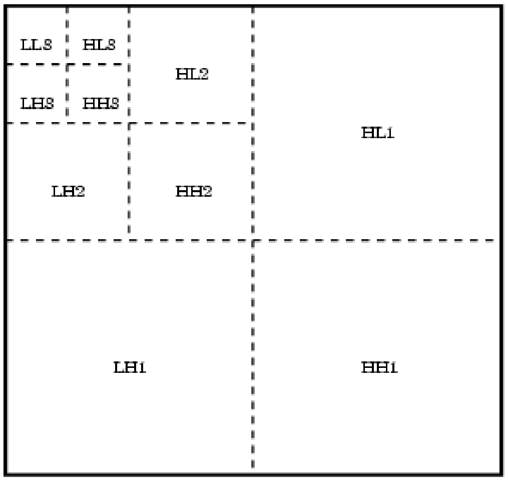


Fig.3. Two dimensional wavelet transformation

III. Experiments

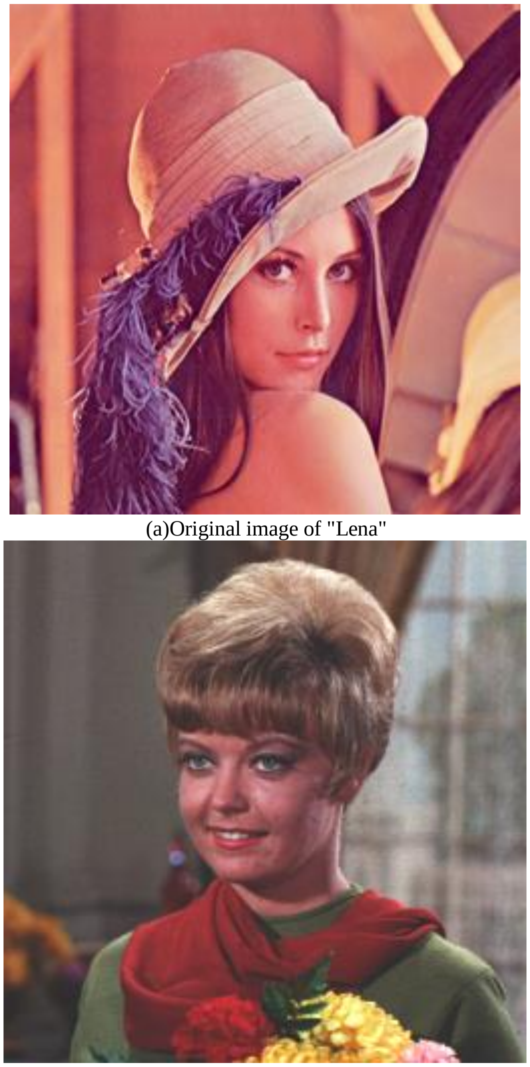
A. Data Used

Figure 4 shows example images of information content in concern. Figure 4 (a) shows "Lena" image which is opened to the public while Figure 4 (b) shows "Zelda" image of one of the information contentsin concern. Both images are derived from the well known standard image database, SIDBA. As shown in Figure 2, all the required information for reconstruction of "Zelda" image is included in the LSB of "Zelda" image together with copyright information. Then the designated wavelet frequency component image is replaced to this "Zelda" image. The authenticated user who knows the parameters for random number derived from Messene Twister access to the image (information content) in concern can reconstruct "Zelda" image. Otherwise, required information, attribute information cannot be decoded results in no reconstructed image can be obtained.

B. Experiemntal Results

Image quality of the "Lena" depends on the process parameters of the location of wavelet frequency component in which the information content in concern is replaced to it.

Figure 5 (a) shows the reconstructed image of "Lena" in which HH1 component is replaced to "Zelda" image while Figure 5 (b) shows the reconstructed "Lena" image in which HH1 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zelda" image is embedded into LSB component based on steganography. Through a comparison between Figure 5 (a) and (b), image defect due to steganography is almost invisible.



(a)Original image of "Lena"

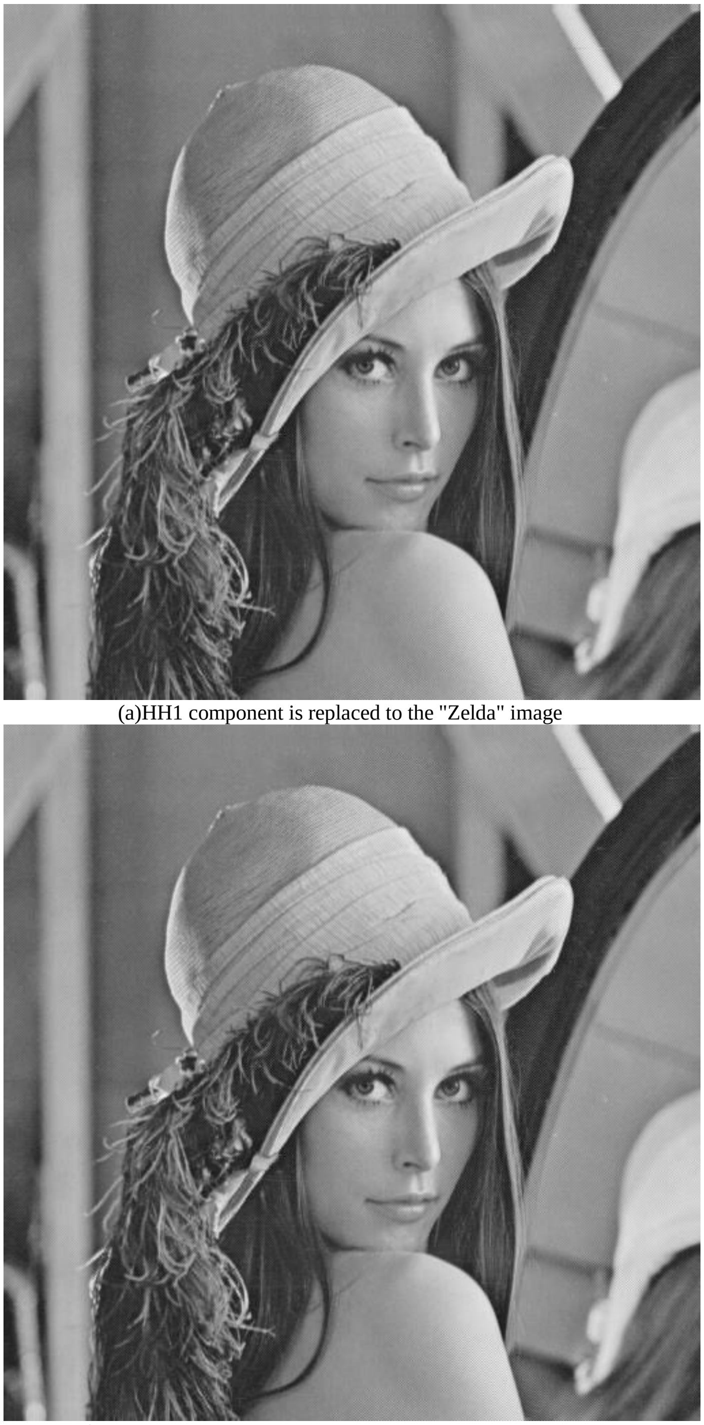
(b)Information content in concern of "Zelda"

Fig.4. Examples of images which is opened to the public and information content in concern

Figure 6 (a) shows the reconstructed image of "Lena" in which HH1 component is replaced to "Zelda" image while Figure 6 (b) shows the reconstructed "Lena" image in which HH2 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zelda" image is embedded into LSB component based on steganography. Through a comparison between Figure 6 (a) and (b), image defect due to steganography is almost invisible.

Figure 7 (a) shows the reconstructed image of "Lena" in which HH1 component is replaced to "Zelda" image while Figure 7 (b) shows the reconstructed "Lena" image in which HH3 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zelda" image is embedded into LSB component based on steganography. Through a comparison between Figure 7 (a) and (b), image defect due to steganography is almost invisible.

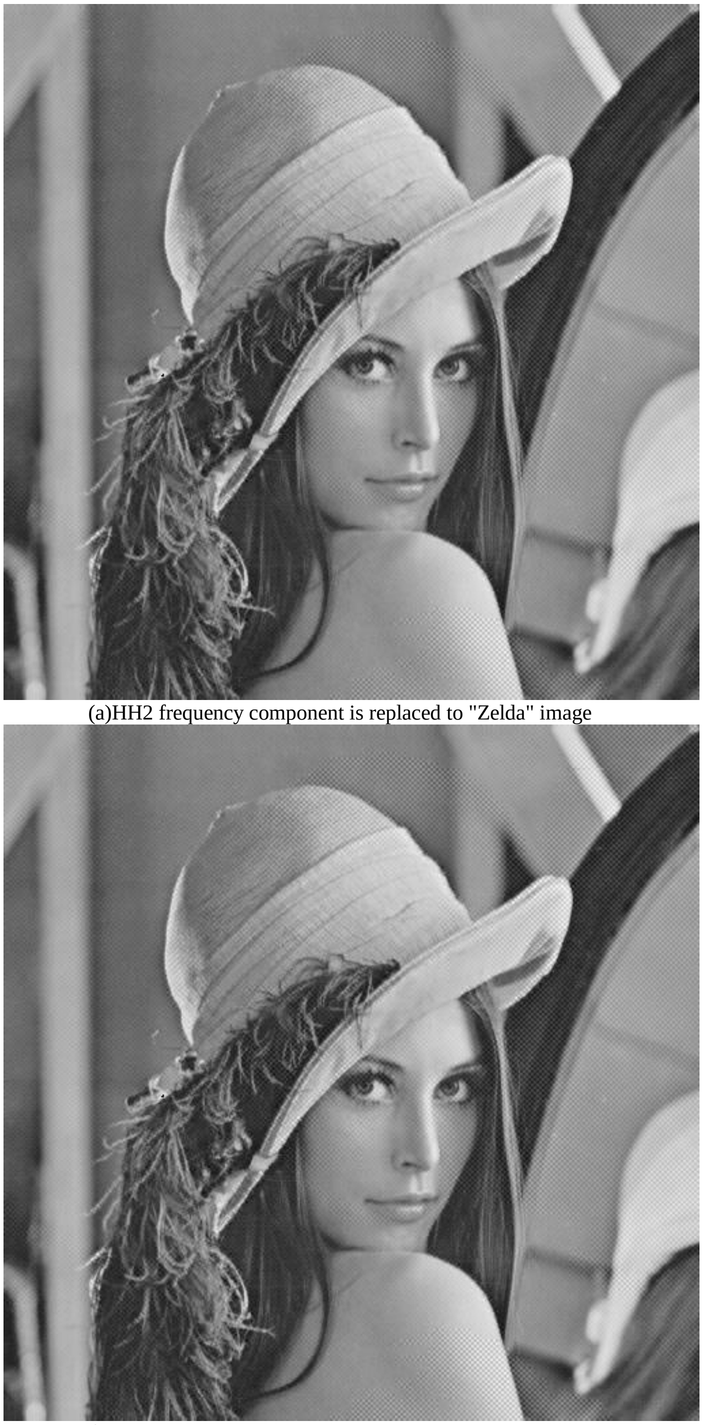
[3] http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/mt.html



(a)HH1 component is replaced to the "Zelda" image

(b)HH1 frequency component is replaced to the "Zelda" image together with all the required information of reconstruction of the "Zerlda" image is embedded into LSB component based on steganography

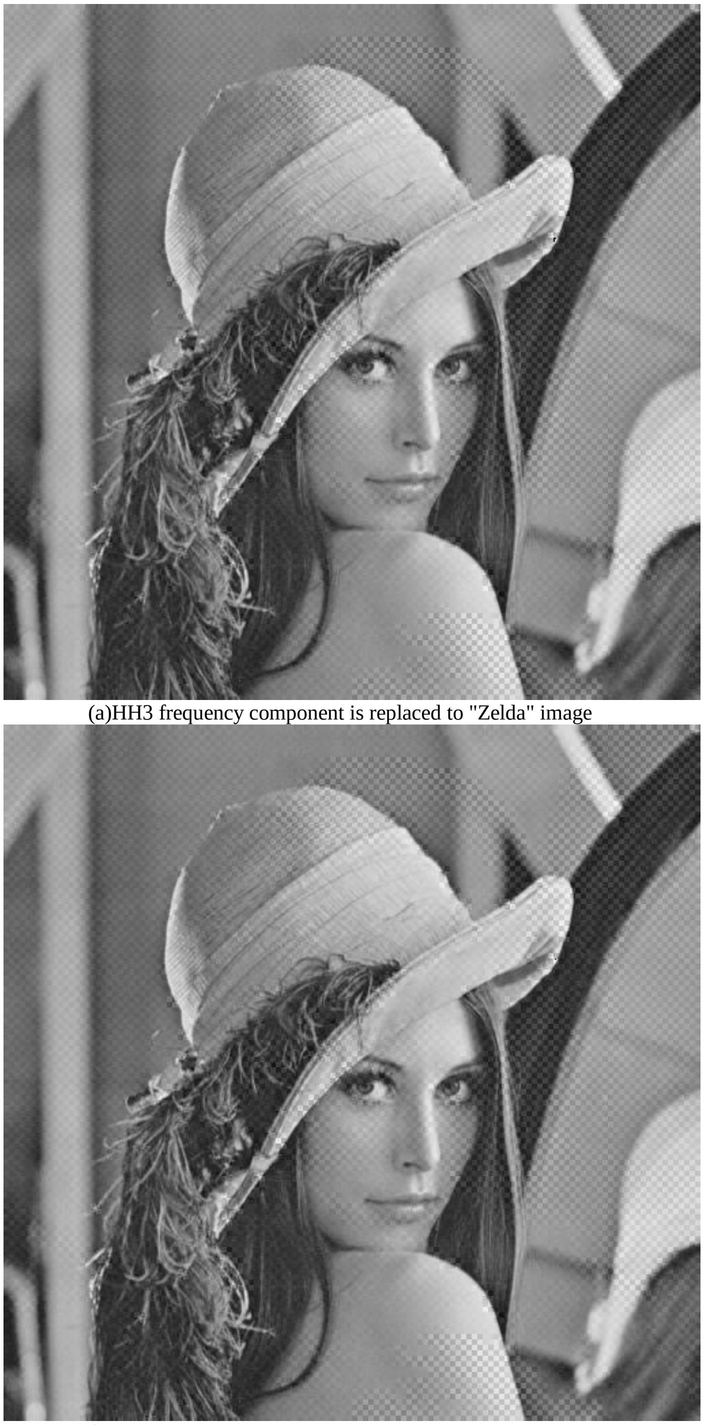
Fig.5. Reconstructed "Lena" images which containing "Zelda" image and "Zelda" and all the required information for reconstruction of "Zelda" image in concern



(a)HH2 frequency component is replaced to "Zelda" image

(b) HH2 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zerlda" image is embedded into LSB component based on steganography

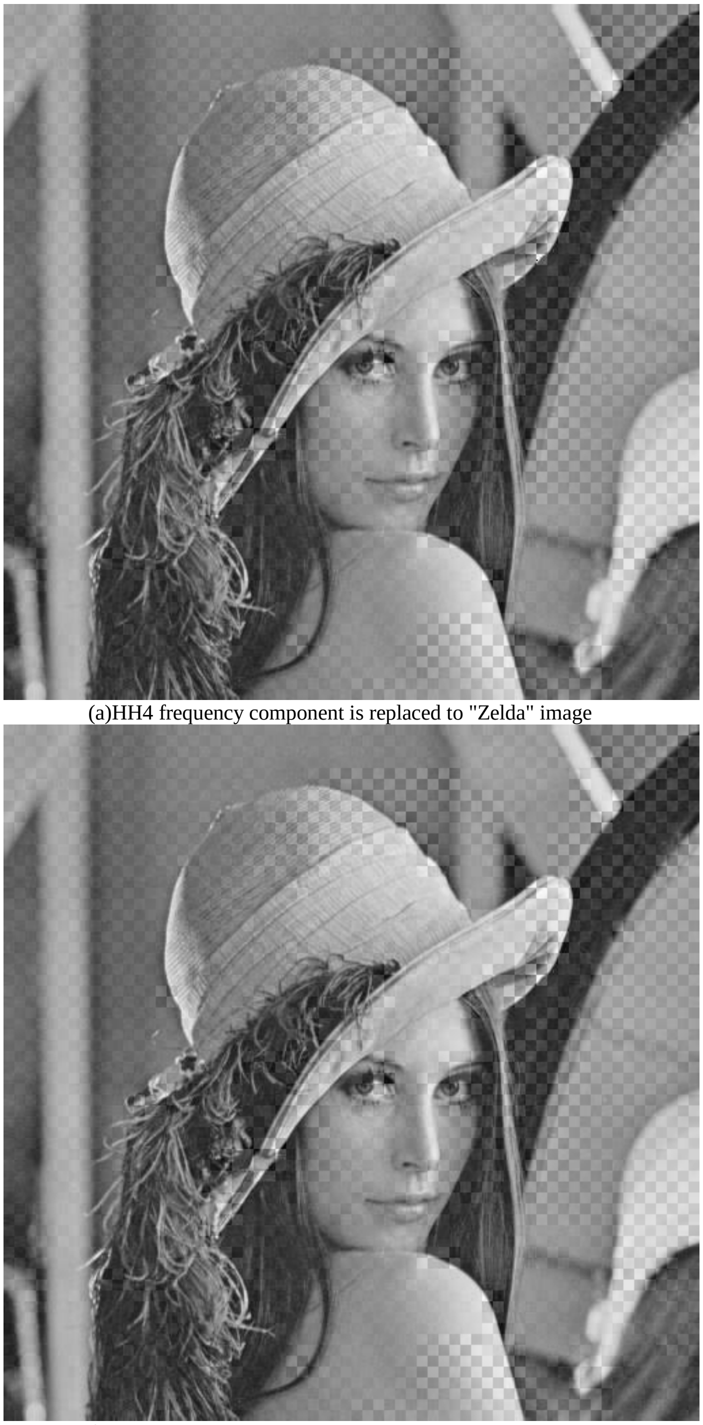
Fig.6. Reconstructed image from the image of which HH2 frequency component is replaced to "Zelda" image



(a)HH3 frequency component is replaced to "Zelda" image

(b) HH3 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zerlda" image is embedded into LSB component based on steganography

Fig.7. Reconstructed image from the image of which HH2 frequency component is replaced to "Zelda" image



(a)HH4 frequency component is replaced to "Zelda" image

(b) HH4 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zerlda" image is embedded into LSB component based on steganography

Fig.8. Reconstructed image from the image of which HH2 frequency component is replaced to "Zelda" image

Figure 8 (a) shows the reconstructed image of "Lena" in which HH4 component is replaced to "Zelda" image while Figure 8 (b) shows the reconstructed "Lena" image in which HH4 frequency component is replaced to "Zelda" image together with all the required information of reconstruction of the "Zelda" image is embedded into LSB component based on steganography. Through a comparison between Figure 8 (a) and (b), image defect due to steganography is almost invisible.

Image quality is decreases in accordance with the number of level or stage of MRA obviously. Also it is found that image defect due to steganography is not visible. Therefore, general users do not aware of the information content in concern (in this case, "Zelda" image). Root Mean Square: RMS difference between the reconstructed and the original "Lena" image is evaluated. The RMS difference between both images without steganography is shown in Table 1 while that with setganography is also shown in Table 2, respectively. For cases, HH1, HH2, HH3, and HH4 component is replaced to "Zelda" image. RMS difference for all these cases shows quite small.

Therefore, it is not easy to distinguish which is original or reconstructed image. It is also found that the RMS difference is getting large in accordance with the level, stage. Furthermore, image defect due to the steganography is small enough, negligible.

TABLE I. RMS DIFFERENCE BETWEEN BOTH IMAGES WITHOUT STEGANOGRAPHY

Stage, level	RMS diff.
1	0.01372
2	0.01435
3	0.01526
4	0.01691

TABLE II. RMS DIFFERENCE BETWEEN BOTH IMAGES WITH STEGANOGRAPHY

Stage, level	RMS diff.
1	0.01380
2	0.01443
3	0.01532
4	0.01688

On the other hands, authenticated users can reconstruct "Zelda" image because they know the location of frequency component which is derived from the LSB of the frequency component. Only thing they have to know is initial condition of random number which is generated by Messene Twister.

Also the information content providers may access to their contents. Then they can decode attribute information which includes copyright information the number of access, user ID of the user who accesses the contents. Thus "Point" can be updated after the information contents are serviced.

IV. CONCLUSION

Access fee charge system for information contents sharing through P2P communications is proposed. Security is the most important for this charge system and is kept with data hiding method with steganography and watermarking. Security level for this charge system is evaluated with image contents.

ACKNOWLEDGMENT

The author would like to thank Dr. KanameSeto for his effort to conduct the experiments on data hiding.

REFERENCES

[1] K.Arai and K.Seto, Data hiding method based on wavelet Multi Resolution Analysis: MRA, Journal of Visualization Society of Japan, Vol.22, Suppl.No.1, 229-232, 2002.

[2] K.Arai and K.Seto, Data hiding method based on wavelet Multi Resolution Analysis: MRA utilizing eigen value decomposition, Journal of Visualization Society of Japan, Vol.23, No.8, pp.72-79,2003.

[3] K.Arai and K.Seto, Data hiding method based on wavelet Multi Resolution Analysis: MRA utilizing image space coordinate conversion, Journal of Visualization Society of Japan, 25, Suppl.No.1, 55-58,(2005)

[4] K.Arai, Keyword extraction method from paper based documents, drawings, based on knowledge importance evaluation with Analitic Hiearchical Process: AHP method, Journal of Image and Electronic Engineering Society of Japan, 34, 5, 636-644, (2005)

[5] K.Arai and K.Seto, Data hiding method based on wavelet Multi Resolution Analysis: MRA utilizing random scanning for improving invisibility of the secret image, Journal of Visualization Society of Japan, 29, Suppl.1, 167-170, 2009.

AUTHORS PROFILE

KoheiArai, He received BS, MS and PhD degrees in 1972, 1974 and 1982, respectively. He was with The Institute for Industrial Science, and Technology of the University of Tokyo from 1974 to 1978 also was with National Space Development Agency of Japan (current JAXA) from 1979 to 1990. During from 1985 to 1987, he was with Canada Centre for Remote Sensing as a Post Doctoral Fellow of National Science and Engineering Research Council of Canada. He was appointed professor at Department of Information Science, Saga University in 1990. He was appointed councilor for the Aeronautics and Space related to the Technology Committee of the Ministry of Science and Technology during from 1998 to 2000. He was also appointedcouncilor of Saga University from 2002 and 2003 followed by an executive councilor of the Remote Sensing Society of Japan for 2003 to 2005. He is an adjunct professor of University of Arizona, USA since 1998. He also was appointedvice chairman of the Commission “A” of ICSU/COSPARin 2008. He wrote 30 books and published 332 journal papers.