2017 4th NAFOSTED Conference on Information and Computer Science

Hanoi, Vietnam
24-25 November 2017

IEEE Catalog Number: CFP17M51-POD
ISBN: 978-1-5386-3211-6

IEEE Catalog Number:	CFP17M51-POD
ISBN (Print-On-Demand):	978-1-5386-3211-6
ISBN (Online):	978-1-5386-3210-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Table of Contents

2017 4th NAFOSTED Conference on Information and Computer Science

Computational Intelligence

Communications and Networking

Foundation of Computer Science

Computational Intelligence

Communications and Networking

Foundations of Computer Science

Communications and Networking

LSI design and IoT Applications

Software Engnineering

Computational Intelligence

Communications and Networking

Multimedia

Distributed Redundant Image Storages and Reconstruction Algorithm to Contents Verification

Ta Minh Thanh
Dept. of Network Security, Le Quy Don Technical University, 236 Hoang Quoc Viet, Cau Giay, Ha Noi, Viet Nam. Email: thanhtm@mta.edu.vn.

***Abstract*—In this paper, we propose a novel contents verification method using the distributed redundant image storages and user-based reconstruction algorithm. There are two processes composing in our proposal such as the image dispersion method and the image reconstruction method. In the image dispersion method, the images are dispersed into many information patches and are stored on the distributed storages, $e.g$ Dropbox, Google Drive, ... Since the size of information patches is smaller than the full-size of image, the information patches can be distributed on cloud storages via network. Therefore, the resource of cloud storages is used effectively. On the other hand, in the image reconstruction method, the information patches of the image can be collected in order to reconstruct the image for user. The key point of idea in the image reconstruction method is that the reconstructed images should be distinguished each others and the producer can detect the user that it belongs to. The algorithm of reconstruction method employs the watermarking method to generate the watermark pattern based on the user's information such as license number. The demonstration results of our proposed method show that our system can be used as the contents verification in the digital contents distribution system.**

***Keywords*-Image Watermarking, Contents Verification, Cloud Storages, Redundant Image Storages, Image Reconstruction, Information Patches, Digital Rights Management (DRM).**

I. Introduction

A. Background

With the development of network, the data transmission and data storage via Internet has become the most popular way for various forms of digital media such as picture, audio, movie, and so on. The end-users also can buy and redistribute the digital contents anytime and anywhere in order to make more benefit. However, everyone can easily copy and alter or even stole the digital contents. It has outstretched the security concerns of digital multimedia content such as copyright protection, owner's right problem, legal user verification and so on. Therefore, the need for an effective dispersion cloud storages and contents rights management system, where only the legitimate users can access to the digital content, is required recently. Additionally, our technique proposes a new idea for employing the digital contents on the cloud system to digital rights management (DRM).

There are several solutions that are proposed for the purpose of contents verification and users verification. Encryption is an efficient solution for copyright protection since only the legal users who bought the decrypted key from the producers can access the encrypted contents. However, if the legal users redistribute illegally the decrypted contents to get more benefit, the producers cannot detect the redistributed source because there is no copyright information embedded into the contents. That means the encryption cannot protect the copyright of the evaluated contents so far.

In order to improve the disadvantage of encryption method, digital watermarking techniques are used for embedding directly the copyright information into the digital contents [1]. With the existence of the watermark information, watermarking technique can limit the users to distribute again the digital contents via network. However, the ignored users still distribute the contents widely in Internet, therefore, the watermarking techniques also cannot stop the illegal distribution and illegal use efficiently.

Especially, the user-based watermarking is also researched for detect the traitor when the legal users redistribute the digital contents [2], [7], [3]. However, once the user-based watermark is embedded, only a user can be detected and be proved. Therefore, the watermarking techniques should be improved for suiting to the distributed storages via network and detecting the multiple users.

There is an efficient solution for deterring the illegal distribution and protecting the copyright of contents. That solution is using the DRM (Digital Rights Management) [4], [5], [8], [9] in online purchasing system. The DRM system consists of encryption and watermarking technique to manage the digital contents. The legal users only can use the digital content if only if they use special devices or special software to embed the copyright information into the digital contents before using it. However, the encryption and the watermarking technique inside DRM device/software are implemented separately. It raises a risk problem so that the original contents can be achieved between the encryption and watermarking process. That means the original content can be leakage inside the special devices/softwares. Therefore, the content verification and users verification cannot be detectable.

978-1-5386-3210-9/17/$31.00 ©2017 IEEE

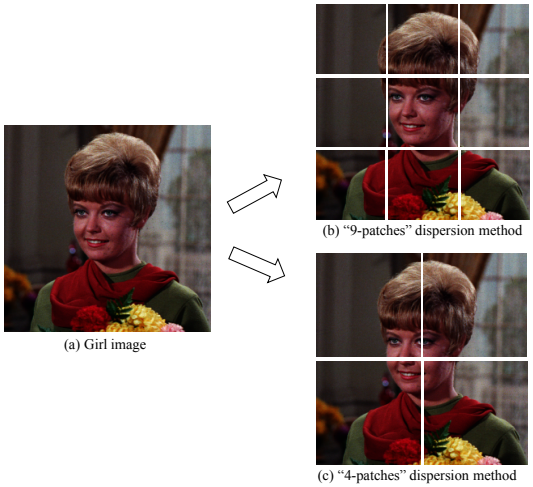

Figure 1. "9-patches" and "4-patches" of spatial dispersion methods.

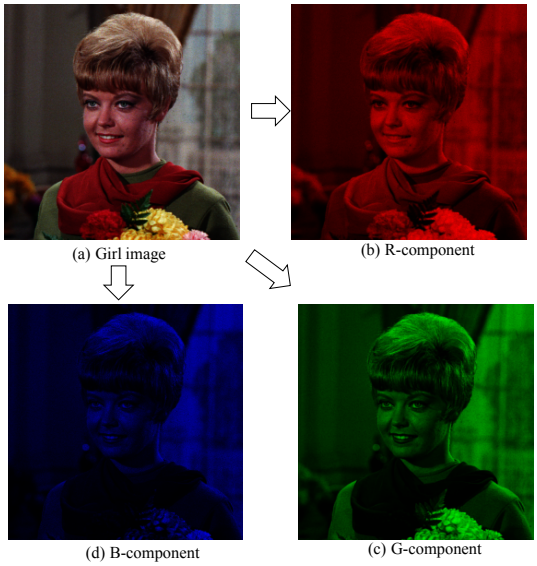

Figure 2. RGB component dispersion methods

B. Our contributions

In this paper, we propose a novel digital rights management system based on the distributed redundant image information on cloud storages and suggest a systematic information reconstruction algorithm for contents verification and users verification. The proposed method can control the number of information patches of digital images that will be dispersed to distributed storages. The digital contents are firstly dispersed to obtain the information patches and those will be saved in the distributed storage systems. We prepare numerous watermark logos to embed directly in to each information patch before dispersion on the cloud storages. Note that the information patches can be overlapped each other.

When the original contents are needed, the information patches are collected from many distributed storage systems and are reconstructed to create the digital contents based on the user's license provided by the producer. According to the license of the legal user, the appropriate information patches are collected. Therefore the reconstructed content is generated with the watermark pattern to distinguish user each other. That means that there are multiple watermark patterns are embedded into multiple information patches before saving those on the distributed storages. After the content reconstruction, the high quality of the digital contents can be obtained and the copyright information (watermark pattern) is determined into the reconstructed contents based on the license number of users. Our solution ensures that the owner of the reconstructed contents can be detected correctly. In particular, we make the following contributions in this paper:

1) Dividing the digital content into many information patches to disperse it on online storages such as cloud system. Our solution gives a new idea for implementing of DRM system. It also can employ distributed storages in order to managing the digital contents. That increases the efficiency of online data storage systems.
2) Our system embeds a logo into an information patch before distributing it on the online storages. The combination of information patches provides one pattern of combination watermark while reconstructing the contents to distinguish the users. Therefore, once the producer embeds the watermark into the information patches, he/she can sell the digital contents to multiple users by license and can detect the traitor exactly.
3) Proof the copyright of the individual users by using the license. The legal users can show the license number to producer when property dispute happens. The producer can extract the watermark pattern from the reconstructed content and compare it with the watermark pattern based on the license number. If the watermark pattern matches, the user is legal. Conversely, the user is illegal.
4) Since our proposed method can detect the owner of the reconstructed contents, it can limit the users to illegally redistribute the copyrighted contents via network.

This paper is organized as follows. The digital content dispersion methods are described in Section II. We also explain our proposed method by using the "n-patches" dispersion method combining the watermarking technique in Section III. Our simulation results are shown in Section IV. Section V concludes our paper.

II. Digital Content Dispersion Methods

In order to distribute the information patches on the cloud system, we should survey various digital content dispersion methods. According to the number of distributed databases,

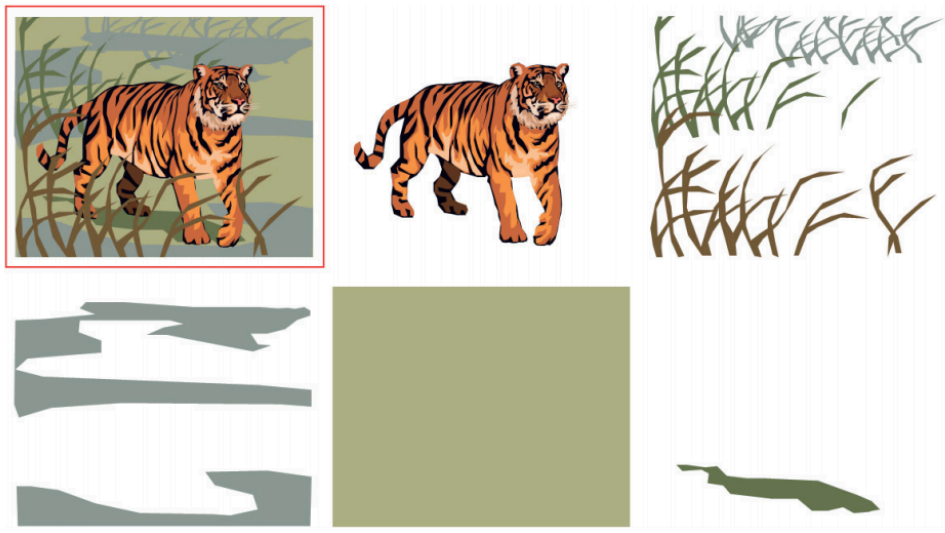

Figure 3. Object-based dispersion methods

the producer can separate the digital image into many information patches. Also, the size of information patches are needed to consider for using efficiently the resource of distributed storages.

1) Spatial dispersion methods: The most simple that can be considered first is spatial dispersion methods. The image I can be separated into "n-patches" information. Each patch information $I(i)$ then is distributed on the cloud storages, where $i = 1 \cdots n$. In general, the producer decides to disperse the image based on the number of online storages that they have.

Fig. 1 shows an example of "n-patches" information dispersion method. "9-patches" information method separates the Girl image into 9 patches of image (Fig. 1 (b)). "4-patches" information method separates the Girl image into 4 patches of image (Fig. 1 (c)). The size of each patch information should be controlled to fit the space of online storages.

2) Component dispersion methods: The digital image is normally constructed by some components color spaces such as RGB[1], YUV[2], YCbCr[3], and so on. Based on the color space, the data structure of the digital image is changed. However, according to the color space, the component of image can be separated to reduce the size of image and saved them in the online storages.

Fig. 2 describes how to separate the R-, G-, B-component of the normal image [6]. 8-bit image is separated from 24-bit image, therefore, the size of the component of image is reduced before redistributing on the online storages.

[1]https://en.wikipedia.org/wiki/RGB_color_model
[2]http://en.wikipedia.org/wiki/YUV
[3]https://en.wikipedia.org/wiki/YCbCr

3) Object-based dispersion methods: In the nature image, there are many objects inside the image. If we can fragment all objects separately, we can manage each object to distribute on several storages.

For instance, Fig. 3 can be fragmented into several objects such as a tiger, grasses, ground, background, and the shadow of the tiger. Each object can be saved in the separate storages in the internet. When the digital image is needed, all objects are collected from those, then the image is reconstructed back.

Object-based dispersion method is quite complex method. It requires time consuming and hard to implement.

III. Proposed Distributed Redundant Image Storages and Reconstruction System

In this section, we explain about the idea of distributed redundant image combination of watermark embedding and license based image reconstruction method. We employ the spatial dispersion method in order to fragment the digital images. "N-patches" spatial dispersion method is implemented. Before distributing, M patterns of watermark are embedded into each patch to create M patterns of information patches. By doing so, the producer can prepare $N \times M$ patches for managing the value digital images. The detailed steps of those processes are given as follows.

A. Redundant image storages combining watermark embedding

Suppose that the digital image I is used to sell to users. It is fragmented into N patches information. Before embedding, we prepare M patterns of logomark $W(i)$ as watermarks information, where $i = 1, \cdots, M$. Fig. 4

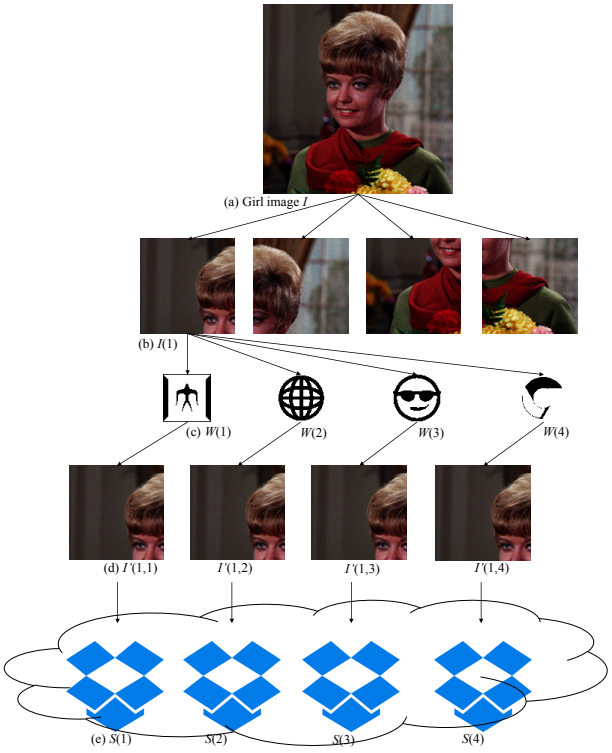

Figure 4. Redundant image storages combining watermark embedding system.

describes the detailed steps in our proposed method. The fragmentation process is explained as follows:

–**Step 1.** Fragment the image I into N patches of $I(j)$, where $j = 1, \cdots, N$ (See Fig. 4(b)).

–**Step 2.** All watermark patterns $W(i)$ are embedded into each patches $I(j)$ by the embedding function $E(\cdot)$ to create M patterns of each patch.

$$I'(j,i) = E(I(j), W(i)), i = 1, \cdots, M, j = 1, \cdots, N \quad (1)$$

$I'(j,i)$ denotes that the watermark pattern $W(i)$ is embedded into the output image $I'(j)$ (See Fig. 4(d)). The watermark embedding method of $E(\cdot)$ can be referred from paper [10], [11].

–**Step 3.** Each patch image $I'(j,i)$ is distributed via network on the online storages $S(i)$ (See Fig. 4(e)).

According to above process, we can fragment the digital image into some patches information then distribute it on the online storages in order to (i) efficiently use the free space of the online storages system, (ii) enhance the security of saving digital contents by distributed storages instead of central saving digital contents.

B. Reconstruction algorithm to contents verification

The reconstruction algorithm is performed based on the license number of the legal users. According to the license number, the appropriate patches information are collected from the distributed storages. Basic steps involved in the reconstruction algorithm, shown in Fig. 5, are given as follows:

–**Step 1.** In order to reconstruct the digital image, the producer generates the license $L(k)$ for each user $R(k)$ based on his/her information.

–**Step 2.** According to the license L, the patches information $I'(j,i)$ are collected from $S(i)$. Note that, the parameter (j,i) of patches information determines the logomark embedded into the patches information. For instance, in Fig. 5(b), the patches information $I'(1,2), I'(2,2), I'(3,1)$, and $I'(4,3)$ are collected from $S(1), S(4), S(3)$, and $S(2)$, respectively. That means the logomarks of those patches information are $W(2), W(2), W(1)$, and $W(3)$.

–**Step 3.** When the producer need to verify the users are whether legal or not, he uses the license L to confirm the watermark pattern $\sum_{n=1}^{M} W(i)$. Afterward, he can extract the watermark information from the patches information $I'(j,i)$ to construct the watermark pattern $\sum_{n=1}^{M} W'(i)$. Compare $\sum_{n=1}^{M} W(i)$ and $\sum_{n=1}^{M} W'(i)$, producer can judge the user.

C. Users verification

Suppose that, our system employs "N-patches" method to fragment the digital image I. We also prepare M of logomarks for embedding in each patch information. Therefore, the number of patches information that is generated to distribute on the online storages, is $M \times N$ patches.

In order to sell the digital contents to users, the producer can reconstruct the digital contents by combination of all patterns of patches information. The number of users that can be distinguished by using our proposed method, is M^N.

IV. Experimental Results and Discussion

A. Experimental environment

For assessing the performance of the proposed algorithm, we conducted seven color and grayscale images of SIDBA (Standard Image Data-BAse) database[4]. All these test images are with size 512×512 pixels, and 4 logomarks used in our experiments are the binary image with size 64×64 which is shown in Fig. 4(c).

In order to evaluate the quality of watermarked images, we employ PSNR (Peak Signal to Noise Ratio) criterion [2]. The PSNR of $H \times W$ pixels of image $I(l,m)$ and $I'(l,m)$ is calculated with,

$$PSNR = 20 \log \frac{255}{MSE} \quad [\text{dB}] \quad (2)$$

$$MSE = \sqrt{\frac{1}{H \times W} \sum_{l=0}^{H-1} \sum_{m=0}^{W-1} \{I(l,m) - I'(l,m)\}^2}$$

(MSE : Mean Square Error).

[4]www.vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES/

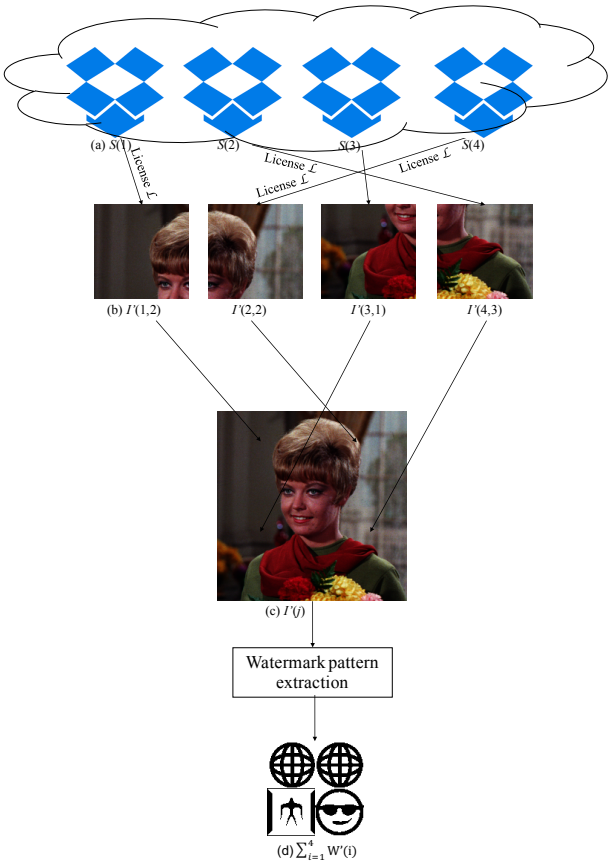

Figure 5. Reconstruction algorithm to contents verification system.

Table I
PSNR[DB] AND WATERMARK PATTERNS OF RANDOM TEN LICENSE NUMBER L (GIRL IMAGE).

Image	PSNR	License L	Watermark pattern
Girl	55.89	LICENSE142	3-3-2-2
Girl	55.84	LICENSE157	3-1-1-2
Girl	55.85	LICENSE100	1-2-3-4
Girl	55.79	LICENSE67	1-4-4-2
Girl	55.84	LICENSE17	3-4-4-2
Girl	55.82	LICENSE182	2-1-4-2
Girl	55.78	LICENSE2	4-4-1-1
Girl	55.87	LICENSE211	3-3-1-4
Girl	55.79	LICENSE141	3-1-4-1
Girl	55.78	LICENSE221	1-1-2-4

Table II
PSNR[DB] AND WATERMARK PATTERNS OF ALL EXPERIMENTAL IMAGES.

Image	PSNR	License L	Watermark pattern
Girl	55.87	LICENSE136	3-3-2-4
Lena	55.90	LICENSE187	2-2-3-3
Baboon	55.93	LICENSE217	4-1-2-1
Barbara	55.91	LICENSE16	2-2-2-2
Goldhill	55.92	LICENSE156	2-4-1-2
Couple	55.84	LICENSE6	4-4-2-2
Peppers	55.89	LICENSE164	1-2-4-2

B. Experimental results

We implemented the "N-patches" dispersion method with $N = 4$. That means the experimental images are separated into four patches of image informations. Then four logomarks are embedded into each patch image in order to generate the embedded patches information. Afterward, the embedded patches information are distributed to four Dropbox servers.

To reconstruct the digital contents, we generate the license number L and collect four patches information from the Dropbox server. By doing so, we can reconstruct the digital contents with the watermark pattern inside based on the license number L. We try with various of license number to confirm the efficiency of our proposed method. We confirm the quality of the reconstructed images and also try to extract the watermark patterns from those.

First of all, we try to confirm the dispersion method and reconstruction method by using the random license number L. Based on the license number L, we reconstruct the digital images and compute the PSNRs values. We generate random ten license number L and reconstruct the digital image based on L. The experimental results are shown in Table I.

According to Table I, we recognize that the quality of the reconstructed images is over than 55dB. That means the reconstructed images are good for sell. Additionally, the watermark patterns are successfully extracted from the reconstructed images to distinguish the legal users. For example, the watermark pattern "3-3-2-2" means the combination of the logomarks $(W(3), W(3), W(2)$, and $W(2)$(see Fig. 4)(c)) including the reconstructed image.

We also try to test with seven images of the test database. The results are shown in Table II. The results in Table II shows that our proposed method is suitable for image distribution system. We can easily manage to separate the digital image and save the patches information on the online storage ($e.g$ Dropbox servers). According to the extracted watermark patterns, our system also can distinguish the users. Therefore, the proposed method can limit the illegally redistribution of the reconstructed contents beforehand.

Fig. 6 shows our experimental results of Table II. The experimental results show that the reconstructed images are excellent images with high quality. In additional, the extracted watermark patterns are visible to detect the copyright information. It also shows the efficiency of our proposed system for new idea of DRM system employing the distributed online storages.

C. Discussions

Our proposed method shows a new idea to implement the digital right management system. The combination of the dispersion technique and the watermarking method gives

Figure 6. Some samples of our proposed results.

us an efficient way to embed the watermark including users distinction. Our proposed watermarking method is difference from the normal watermarking methods. Once, the logomarks are embedded into the patches information, the logomarks are used to combine to make various watermark patterns for many legal users. On the other hand, in the conventional methods [11], [2], after embedding the watermark into the digital images, only a legal user is specified.

In addition, in this paper, we do not discuss about the watermark embedding technique. In fact, the producer can employs various watermarking techniques for implementing our proposed system. That makes our system more flexible for DRM system.

V. Conclusion

We have proposed a novel distributed redundant image storages and reconstruction algorithm to contents verification and users authentication system, which is not yet proposed for watermarking field before. The digital images are separated and distributed on the online storages after embedding the logomarks inside the patches information. The watermark patterns are generated based on the license number sold to the legal users. Those can be used for specify the legal users. Therefore, our proposed method also can limit the illegal distribution. According to our experimental results, the embedded watermark patterns can be successfully extracted and distinguished each others.

In the future works, we try to apply the proposed method on another digital format such as digital audio, video, and so on.

References

[1] F. Y. Shih (eds.), "Digital Watermarking and Steganography: Fundamentals and Techniques," Taylor & Francis Group, CRC Press., Inc., Boca Raton, FL, USA, 2008.

[2] M. Iwakiri, T. M. Thanh, "Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management," The 26th IEEE International Conf. on AINA, pp. 763–770, 2012.

[3] T. M. Thanh, M. Iwakiri, "Fragile Watermarking with Permutation Code for Content-Leakage in Digital Rights Management System," Journal of Multimedia System, ISSN 1432-1882, Springer, 2015.

[4] S. Okamura, M. Yoshida, T. Fujiwara, "An Unlinkable Interactive Drama Delivery System Allowing Rechoice of a Scene," Symposium on Cryptography and Information Security 2006, 2F3-3, 2006.

[5] S. Emmanuel, M.S. Kankanhalli, "A Digital Rights Management Scheme for Broadcast Video," Multimedia Systems, Vol.8, Issue 6, pp.444–458, 2003.

[6] https://en.wikipedia.org/wiki/RGB_color_model

[7] Iynkaran Natgunanathan,Abid Mehmood, Yong Xiang, Guang Hua, Gang Li, Shaun Bangay, "An overview of protection of privacy in multibiometrics, " Multimedia Tools and Applications, pp. 1–21, 2017.

[8] Hyejoo Lee, Suwan Park, Changho Seo, Sang Uk Shin, "DRM cloud framework to support heterogeneous digital rights management systems," Multimedia Tools and Applications, vol. 75, issue 22, pp 14089–14109, 2016.

[9] Goo-Rak Kwon, Ramesh Kumar Lama, Jae-Young Pyun, Chun-Su Park, "Multimedia digital rights management based on selective encryption for flexible business model, " Multimedia Tools and Applications, vol. 75, issue 12, pp. 6697?6715, 2016.

[10] T. M. Thanh, M. Iwakiri, "A proposal of digital rights management based on incomplete cryptography using invariant Huffman code length feature," Journal of Multimedia System, ISSN 1432-1882, Vol. 20, Issue 2, pp. 127–142, Springer, 2013.

[11] T. M. Thanh, P. T. Hiep, T. M. Tam, K. Tanaka, "Robust semi-blind video watermarking based on frame-patch matching," J. of Electronics and Communications, ISSN 1434-8411, 2014.