7

Evaluation of Multimedia Fingerprinting Image

Kang Hyeon RHEE
College of Electronics and Information Engineering,
Chosun University, Dept. of Electronics Engineering, Gwangju,
Korea

1. Introduction

It would observe an enormous growth about a use and distribution of multimedia content in Internet, and an illegal copy and redistribution of multimedia content are also increased with a serious proclivity for a wrongdoer.

Among multimedia content specially, a digital image has been widely used in a variety of applications, from web, digital camera photography, military information and digital art to medical diagnosis and personal blog. As like this, digital image is more and more important media in an information society. Therefore, a necessity for a reliable multimedia content has been rising rapidly in recent years. How to protect the original creator's Intellectual Property Rights (IPR) and integrity of digital products is a realistic problem urgently needing to be solved [1]. Accordingly, the copyright of a content creator has to be protectable for IPR and discriminate between the original from an illegal copy.

Furthermore, a tracing of an illegal distribution has to be a necessary for a copyright protection and a cutoff of an illegal copy of multimedia content. The methods to prevent from an illegal reproduction and distribution are categorized into two ways. The one is enable to use and transmit within a boundary of admitted limitation for authorized users, and the other is to trace how people reproduce and redistribute the content illegally, when they are found to be illicit in contact with an unauthorized content [2].

In the early, the studies of content copyright protective are limited in application by encryption method, a watermarking technology introduced by the alternative.

Watermarking method inserts the original owner information to content. After piracy, the watermarking information is extracted from content, and then it compares with the original watermarking information [3]. So this method could be proving the original owner. But, watermarking method can only confirm the copied illegal content, and it never confirms the illegal distributor and the distributed path.

Digital watermarking method indicates the copyright which is made with a provider's self information and directly inserted into multimedia content. This orientation of technology comes from an intention to protect a copyright because multimedia contents on a web are easy to redistribute. Fig. 1 and 2 show the process of the watermark insertion and watermark detection.

According to the developed technology of watermarking, multimedia fingerprinting technology [4-6] was rising also. Multimedia fingerprinting technology includes owner's

and user's information of content so that multimedia fingerprinting technology is to solve these problems. Colluders try to remove the inserted fingerprinting code in content then they regenerate the collusion codes and can redistribute illegally the pirated content by insert the collusion code. Thus, multimedia fingerprinting code has to be generated in order to be robust in this kind of the collusion attack by the colluders.

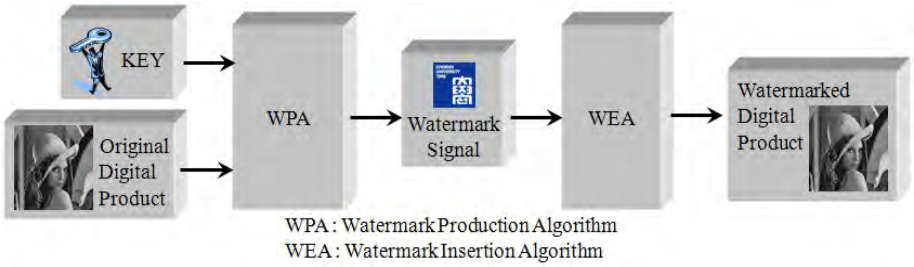


Fig. 1. Watermark insertion

Fig. 2. Watermark detection

So, that would be robustness in this collusion attack into multimedia fingerprinting code should be created [7]. For the fingerprinting code of multimedia content protection, application of BIBD (Balanced Incomplete Block Design) code that satisfies the specification of ACC (Anti-Collusion code) was studied in several papers [8-16].

1.1 Prior art

The resistances of digital watermark to linear collusion attacks have been studied recently [16-18]. W. Trappe [16] presented a fingerprinting system using BIBD code derived from combinatorial design system proposed by D. R. Stinson [20], which proposed a fingerprint code system that satisfies “Frame-proof code” by using combinational design theory first time.

When a copyright infringement has been occurred, copyrighters can choose to insert the watermark into their content to acknowledge who is responsible for the original contents.

One of the first collusion resistant fingerprints was proposed by [4] for generic data. The watermarks were assumed to satisfy the marking assumption, that is, the users cannot change the state of an undetected mark without rendering the object useless [11].

Also, multimedia fingerprinting is a technology for copyright protection of the content’s creators. It is a process of insertion in a distinct set of marks into a given host signal to produce

a set of fingerprinted signals that each appears identical to use. If an illegal copy is detected, it's possible to trace the dishonest users. However, colluders may get together comparing their copies and make a new copy to avoid being incriminated, known as collusion attack [10].

For the multimedia content protection, BIBD code that satisfies the characteristics of ACC, so the application of BIBD code on the fingerprinting code was progressed in many researches [8-16]. The BIBD matrix is modified to form fingerprinting codes that had collusion resistant, even if all the users collude [8]. And ACC was proposed to accommodate more users while providing collusion-resistance [16].

Accordingly, a multimedia fingerprinting technology was rising. The insertion method of fingerprinting code to multimedia content was variously studied. When it inserts fingerprinting code in content, the robustness of orthogonal modulation technology is limited on Averaging attack by colluders, but a code modulation technology has robustness for Averaging attack.

Thus, a resilience code is used to fingerprinting code [16], which is derived from BIBD code, but this method is difficult to define the threshold value according to the change of the threshold setting value by the number of colluders when the collusion code is detected from an illegal content on used Averaging attack [12].

1.2 Article organization

In this article, the collusion code generated using a fingerprinting code based on BIBD is estimated and PSNR of the experimental images according to BIBD v value is computed also. The kind of collusion attacks used for the evaluation method of the considered collusion code generation is an average computing (Averaging) and logical operations (AND, OR and XOR).

It now summarizes the main focus and contributions of this article.

1. Fingerprinting code generation based on BIBD code.
2. Collusion code generation of Logic operation (AND, OR and XOR) and Averaging.
3. Evaluation of the generated collusion codes for an effect increasing of anti-collusion, and elimination of the useless collusion codes.
4. In consideration of image quality, evaluation of fingerprinting code length by the measurement of the PSNR.
5. Computation of fingerprinting code length by image transforms.

The rest of the article is organized as follows. In Section 2, the theoretical background of BIBD characteristic and collusion attack are introduced, and the evaluation algorithm of the collusion code is proposed in Section 3. Then in Section 4, the detection range of colluder by effect of the collusion code was computed and evaluated, and also fingerprinting code length is evaluated by image PSNR values. Lastly, the conclusion is drawn in Section 5.

2. Theoretical background

2.1 BIBD property

In this section, BIBD property is briefly introduced as for a requirement of multimedia fingerprinting code. Multimedia fingerprinting is content's security technology based on

watermarking technology. To improve the weak point that illegal content distribution process remains an unknown, fingerprinting technology has been being researched.

The theory of block designs is a field of mathematics that has found application in the construction of error correcting codes and the statistical design of experiments.

Compounding a problem of BIBD {v,b,r,k and λ}, which is using a matrix model to produce code satisfied with constraints.

Where v: points, number of elements of X.
k: number of points in a block.
b: number of blocks.
r: number of blocks containing a given point (k<v).
λ: number of blocks containing 2 (or more generally t) points.

Upper 5 parameters are satisfying following two limitation conditions.

$$vr = bk \tag{1}$$

$$r(k-1) = \lambda(v-1) \tag{2}$$

BIBD is simply able to express with {v, k, λ}.

$$b = \frac{v(v-1)\lambda}{k(k-1)} \tag{3}$$

$$r = \frac{\lambda(v-1)}{k-1} \tag{4}$$

b=v or r=k then BIBD is symmetrical.

If $X = \{X_i\}_{i=1}^{v}$ and $A = \{A_j\}_{j=1}^{b}$, then BIBD's incidence matrix becomes $\boldsymbol{M}$ as Eq. (5).

Therefore, $\boldsymbol{M}$ satisfies Eq. (6).

$$m_{ij} = \begin{cases} 1 & if \quad x_i \in A_j \\ 0 & otherwise \end{cases} \tag{5}$$

$$\boldsymbol{M}\boldsymbol{M}^{\mathrm{t}} = (r-\lambda)I + \lambda J \tag{6}$$

For example, when {v,k,λ} are {7,3,1}, $\boldsymbol{M}$ is presented in (7).
In block design, In Eq. (7), when {v, k, λ} is {7,3,1} is shown the incidence matrix $\boldsymbol{M}$ of BIBD.

The reader can be found more specific information in [19].

All row vectors of the incidence matrix $\boldsymbol{M}$ in BIBD became a multimedia fingerprinting code and then authorize users. This $\boldsymbol{M}$ can be used like ACC in (7).

For example, BIBD code for multimedia fingerprinting is also appeared in (7). The author can have gained the incidence matrix $\boldsymbol{M}$ about one of the block designs based on BIBD when {v, k, λ} are {7,3,1}. This code requires 7 bits for 7 users and 1-resilience since any two column vectors share a unique pair of 1 bit.

In Eq. (7), v_n's row vector (n=1~7) will be *User n*'s fingerprinting code for his purchased media content.

$$\boldsymbol{M} = \begin{array}{|c|ccccccc|}\hline m_{ij} & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ \hline v_1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ v_2 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ v_3 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ v_4 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ v_5 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ v_6 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ v_7 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ \hline \end{array} \quad (7)$$

2.2 Collusion attack

An early work on digital fingerprinting code design and collusion attacks were proposed in [4], which assumed that the colluders can detect a specific fingerprint code bit if it takes different values between their fingerprinted copies and can change it to any value [21].

In here, let's see how to make collusion code by some colluders using Averaging attack. If 3 colluders use their user's fingerprinting code from the row the incidence matrix $\boldsymbol{M}$ of {7,3,1} BIBD code as an ACC, 3 colluders can add their user's fingerprinting code, then the added values are on an average. Therefore, the reader can know that 3 illegal users have collusion attack according to the only their user's fingerprinting code by adding and averaging [1].

For example, if $User_2$, $User_4$, and $User_6$ intend collusion attack by Averaging with each one code from (7):

$$User_2 = (1\ 0\ 0\ 1\ 1\ 0\ 0),\ User_4 = (0\ 1\ 0\ 0\ 1\ 0\ 1) \text{ and } User_6 = (1\ 0\ 0\ 0\ 0\ 1\ 1)$$

The generated a new collusion code(or new User's code) is (0 1 0 1 0 0 1). This is illustrated figured in Fig. 3, which shows the collusion attack [16] of Averaging.

In Fig. 3, the new collusion code (1 0 0 0 1 0 1) is no row vector in BIBD's incidence matrix $\boldsymbol{M}$ in (7). Once the new user code is detected, it knows $User_2$, $User_4$, and $User_6$ would be colluders as like corrupt users. So this collusion-secure fingerprinting scheme may resist collusion attack of 3 users ably, for example. In here, according to the varied threshold value, the generated collusion code would be a variety result.

The code efficiency, as well as the averaging resistance, is an important factor for the fingerprinting code design. The code efficiency refers to the number of recipients that can be handled by code length. The higher code efficiency, the better content fidelity can be achieved since fewer bits of information are inserted as well as better robustness [12]. And some papers [12,16] attempt the incidence matrix $\boldsymbol{M}$ to the bit-complement matrix $\boldsymbol{C}$ for increasing the resilience. In (7), if $\boldsymbol{M}$ has the bit-complement to {7,4,2} $\boldsymbol{C}$ afterwards the resilience is increased 1 to 2. Thus, the effect of anti-collusion is increased. $\boldsymbol{C}$ from (7) is shown in (8) by bit-complement.

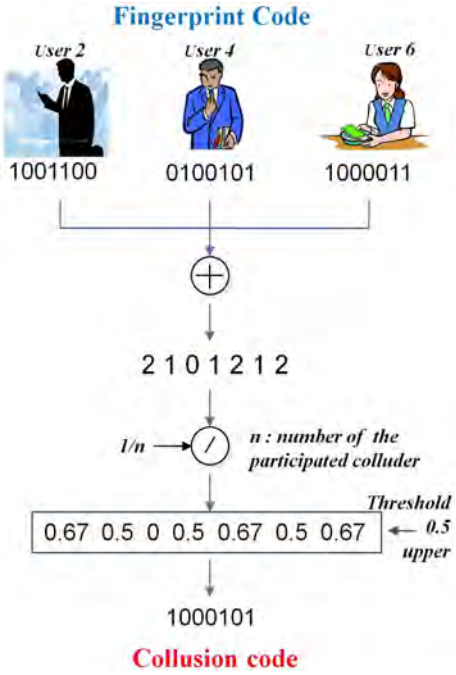


Fig. 3. Collusion attack by Averaging

M is transformed to the bit-complement matrix ***C*** then all row vectors of ***C*** will be fingerprinting code of each user. ***C*** can be used like ACC (Anti-Collusion code), which is presented in (8), in here row vectors (***n***=1~7) will be *User* ***n***'s each fingerprinting code and 2-resilience since any two column vectors share a unique pair of 2 bits for his purchased media content too.

$$C = \begin{array}{|c|c|c|c|c|c|c|c|}\hline m_{ij} & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ \hline v_1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline v_2 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline v_3 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline v_4 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline v_5 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline v_6 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ \hline v_7 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hline \end{array} \quad (8)$$

2.3 Color model [32,33]

Color space is a complicated topic. Colors don't really exist, like dust does. We human being use colors to describe what we see. The most common way to describe what we see in terms of color is using combination of red, green and blue, which is referred as RGB color space.

2.3.1 RGB color space

The RGB color space consists of the three additive primaries: red, green and blue. Spectral components of these colors combine additively to produce a resultant color.

The RGB model is represented by a 3-dimensional cube with red green and blue at the corners on each axis which is shown in Fig. 4. Black is at the origin. White is at the opposite end of the cube. The gray scale follows the line from black to white. In a 24-bit color graphics system with 8 bits per color channel, then red is (255, 0, 0) green is (0, 255, 0) and blue is (0, 0, 255). On the color cube, red is (1, 0, 0), green is (0, 1, 0) is (0, 0, 1).

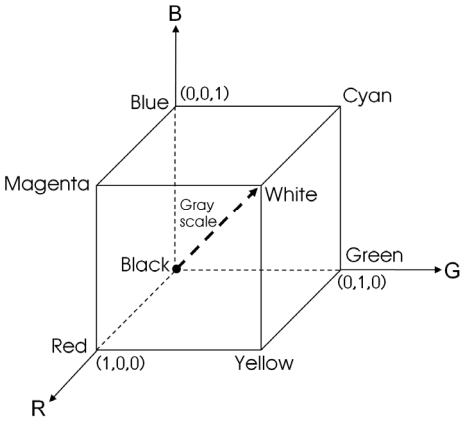


Fig. 4. RGB color cube

2.3.2 Grayscale

It converts RGB to grayscale values by forming a weighted sum of the R, G and B components as Eq. (9) below.

$$\text{Grayscale} = 0.2989R + 0.587G + 0.114B \tag{9}$$

2.3.3 YCbCr color space

A color space is simply a model of representing what we see in tuples. YCbCr is one of the popular color space in computing. It represents colors in terms of one luminance component/luma (Y), and two chrominance components/chroma(Cb and Cr).

Human eyes are sensitive to luminance, but not so sensitive to chrominance.

YCbCr color space has been defined in response to increasing demands for digital algorithms in handling video information, and has since become a widely used model in a digital video.

It belongs to the family of television transmission color spaces. The family includes others such as YUV and YIQ. YCbCr is a digital color system, while YUV and YIQ are analog spaces for the respective PAL and NTSC systems. These color spaces separate RGB (Red-Green-Blue) into luminance and chrominance information and are useful in compression applications however the specification of colors is somewhat unintuitive.

The YCbCr image can converted to/from RGB image. There're several standards defined for the conversion at different context. The conversion below is based on the conversion used in JPEG image compression.

The conversion can be expressed as Eq. (10) and (11) below.
From 8-bit RGB to 8-bit YCbCr :

$$\begin{aligned} Y &= 0.299R + 0.587G + 0.114B \\ Cb &= -0.16874R - 0.33126Green + 0.5B \\ Cr &= 0.5R - 0.41869G - 0.08131B \end{aligned} \tag{10}$$

From 8-bit YCbCr to 8-bit RGB :

$$\begin{aligned} R &= Y + 1.402Cr \\ G &= Y - 0.34414Cb - 0.71414Cr \\ B &= Y + 1.772Cb \end{aligned} \tag{11}$$

The YCbCr color space is widely used for digital video. In this format, luminance information is stored as a single component (Y), and chrominance information is stored as two color-difference components (Cb and Cr). Cb represents the difference between the blue component and a reference value. Cr represents the difference between the red component and a reference value.

Application of YCbCr is a commonly used color space in digital video domain. Because the representation makes it easy to get rid of some redundant color information, it is used in image and video compression standards like JPEG, MPEG1, MPEG2 and MPEG4.

3. Proposed evaluation algorithm of fingerprinting scheme

As introduced Section 1, most research had attempted multimedia fingerprinting for ACC on Averaging attack [12,15,16]. And in [16,22-28], AND-ACC is dealt with AND attack considered to ACC. On the author's opinion about using $\boldsymbol{C}$ from $\boldsymbol{M}$ ((7) and (8) in Section 2.2), if a number of resilient code increases for ACC, thus the effect of ACC would be increased.

Because of this reason, the author utilizes different logical operations such as OR-ACC and XOR-ACC along with the conventional AND-ACC. Clearly, if the factor of resilient code increases, then occurrence frequency of same collusion code will be increased also. These same code causes an attending colluder to be a non-attending user lucratively or a non-attending user to be an attending colluder unfortunately.

Thus, the author would like to reduce the same some collusion code keeping a lower resilient factor and the effect of ACC. It must adopt several logical operations as like AND, OR and XOR if have a lower resilient factor. Then the number of same collusion codes will be decreased and no necessary to change from the incidence matrix $\boldsymbol{M}$ to bit-complete $\boldsymbol{C}$.

In this article, according to the author adopts these criteria of the requirements, the evaluation algorithm of multimedia fingerprinting using BIBD code is proposed and shown in Fig. 5.

For the evaluation of multimedia fingerprinting in this article, the proposed system design can be classified in into 3 steps, namely the generation of the BIBD code as multimedia

fingerprinting code on ① in Fig. 5. After then, the collusion code is generated by Logic operations and Averaging in which, there are occurred in case of the bitstream all '1' bit codes, all '0' bit codes and the same user fingerprinting codes. These codes are useless for collusion code because down to the effect of anti-collusion.

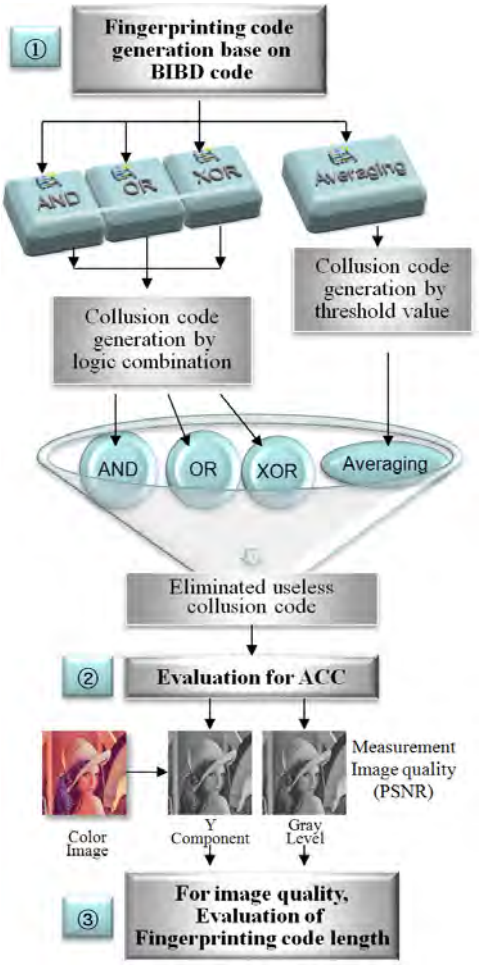


Fig. 5. The proposed evaluation algorithm of the collusion codes of the multimedia fingerprinting based on BIBD

After the useless collusion codes are eliminated, then on ② in Fig. 5, the rest of collusion codes is useful and must evaluate truly as anti-collusion code for the detection and the trace of the colluders which must satisfy for fingerprinting criteria.

And lastly, the useful fingerprinting codes will be inserting into digital images for the measurement of image quality PSNR on ③ in Fig. 5, in which Y component and gray level of color image are experimental image. The transform of Y component and gray level from

color images is a very important transformation in image signal processing area. So these 2 kinds of transformation methods are adopts for the experiment of PSNR measurement.

In this article, the evaluation criterion is put in force 2 kinds of an effect of anti-collusion and fingerprinting code length in Section 4.

4. Experimental results

4.1 Evaluation of fingerprinting and anti-collusion code based on BIBD

The evaluation algorithm of the collusion code which are generated by Logical combinations (AND, OR and XOR) and Averaging for the effect increasing of anti-collusion. And also the collusion code will be separating for the definition of the usable or useless attack code.

In the theoretical collusion attack, BIBD {7,4,2} code able to make 119 numbers of collusion codes, and n-1 or fewer users have attended with collusion attack. Now, let it be counting the useless collusion code existed, and then they must be eliminated about each attack for the effect increasing of anti-collusion. Firstly, Averaging attack would be experimented.

On Averaging attack, Table 1 and Fig. 5 show the number of the collusion codes with BIBD {7,4,2} code, in which they cann't use according to the threshold value. Among 119 codes which would be to collude, the useless collusion codes are 56 least at threshold value 0.34~0.39 in Fig. 6. Eq. (12) computes to decide the number of the useless collusion codes about Averaging attack.

$$Averaging\_attack_{useless\_code} = Threshold \cdot \frac{1}{n} U_i code \tag{12}$$

where $Threshold$: 0.34~0.39

k: number of the colluders.

$U_i code$: colluder's user fingerprinting code based on BIBD code.

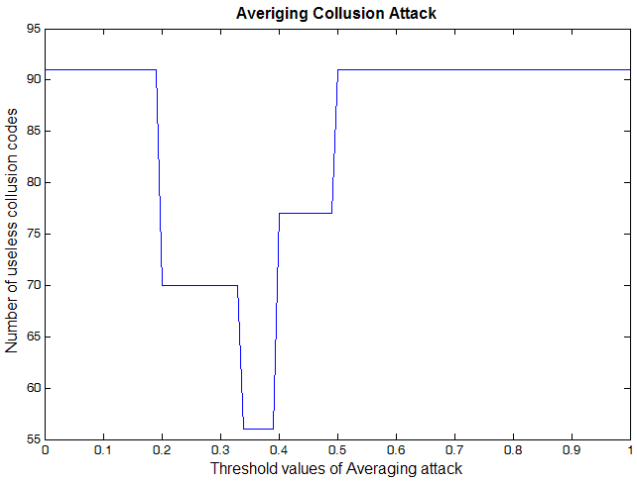


Fig. 6. Number of useless collusion codes by threshold value of Averaging attack

Threshold values of the average collusion attack	Number of the useless collusion codes
0~0.19	91
0.2~0.33	70
0.34~0.39	***56***
0.40~0.49	77
0.5~1	91

Table 1. Number of the useless collusion codes by threshold value of Averaging attack with BIBD {7,4,2} code

And secondly, Logical operation attacks would be experimented. On Logical operation attack with AND, OR and XOR, there are some same codes are appeared as like bitstream all '0' and all '1' codes by AND, OR and XOR attack. According to these results, the number of useless collusion codes is shown in Table 2 about Logical operation attack.

Number of the useless collusion codes		
AND collusion attack	**OR collusion attack**	**XOR collusion attack**
Useless codes caused by all '0' codes and user fingerprinting codes.	Useless codes caused by all '1' codes and user fingerprinting codes.	Useless codes caused by all '0' and '1' codes and user fingerprinting codes.
91	**63**	**49**

Table 2. Number of the useless collusion codes by AND, OR and XOR attacks with BIBD {7,4,2} code

For more number of content's users, if BIBD parameter v value is increased, and then a number of colluders is increased too. Thus, the proprietor of content must be knowing the number of useless collusion codes by v value and the number of attendable colluders.

In the experimental results, the fingerprinting code based on BIBD code proposed in this article is generated and evaluated for the effect of anti-collusion. Threshold value in Eq. (12) is using 0.34~0.39 for a minimum number of useless collusion code. This choice is that although the effect of anti-collusion is decreasing, which is not decrease and would be keeping their effect because another Logical operation(AND, OR and XOR) is performed with Averaging operation for the improving performance of anti-collusion.

According to Table 1 and 2, the efficiency ratio of useful collusion code is shown in Table 3 for anti-collusion.

Collusion attack kinds	Efficiency ratio of usable collusion code(%)
AND	23.5
OR	47.1
XOR	58.8
Averaging	47.1
Average	**44.13**

Table 3. Efficiency ratio of usable collusion code by the type of attacks

According to the kind of collusion operation and the number of the colluders, the number of the useless collusion codes Y_c is formed like Eq. (13)~(15). In here c is 3 kinds of Logic operations(AND, OR and XOR).

$$y_{AND-useless\_code} = 0.88{c_n}^4 - 12.25{c_n}^3 + 51.63{c_n}^2 - 54.25c_n - 14 \tag{13}$$

$$y_{OR-useless\_code} = 2.63{c_n}^4 - 43.75{c_n}^3 + 256.38{c_n}^2 - 614.25c_n - 511 \tag{14}$$

$$y_{XOR-useless\_code} = 0.58{c_n}^4 - 8.17{c_n}^3 + 37.92{c_n}^2 - 65.33c_n - 35 \tag{15}$$

where, c_n : number of colluders.

The number of the traceable colluders is n-1 with the effect 44.13% of collusion code with only 1-resilience BIBD code (7) not 2-resilience BIBD code (8). Table 4 is shown the compared performance of the number of the traceable colluders between the conventional scheme and the proposed algorithm.

Fingerprinting schemes	Method	Possible to trace the number of colluders.
Dittman[29]	d-detecting	2
Boneh [4]	c-secure	2
Trappe [16]	AND ACC	2
Domingo_Ferrer [30]	3-secure	3
This article	**AND, OR, XOR and Averaging attacks**	***n*-1**

(n: number of the total users)

Table 4. Compared performance of the number of the traceable colluders between the conventional scheme and the proposed algorithm.

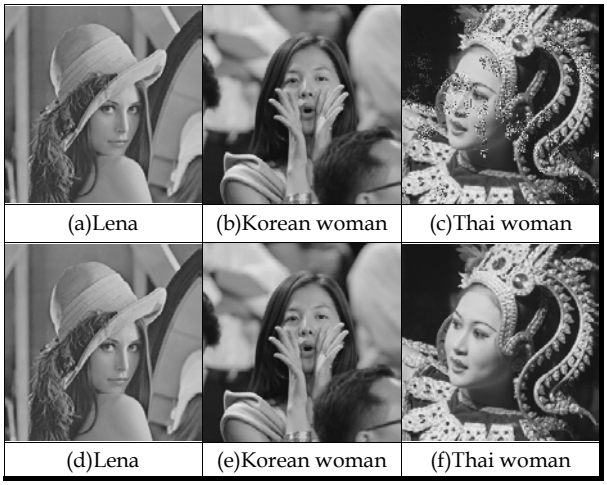
4.2 Image quality measurement

The PSNR of real image is measured by the length of the inserted fingerprinting code based on BIBD code. The evaluation and measurement of image quality PSNR by the fingerprinting code is the main focus of this section on 4 kinds of the collusion attack. In here collusion code is inserted into Y component of color image and gray level image. The choice purpose of Y component and gray level images is that it is very important transform in an image processing area for the compression and pre-processing of multimedia communication, etc.

For the experiment of the used real 3 images are Lena, Korean woman and Thai woman. And the numerous fingerprinting code in this article is applied to 128x128, 256x256 and 512x512 color images. The 7~127bits fingerprinting code length was inserted in Y component and gray level image of 3 original color images, and then each image quality PSNR was measured. Fig. 7 is shown the original images which used in an experiment. Fig. 8 (a)~(c) are shown Y component images of original color images, and (d)~(f) are shown the images of the inserted 39bits fingerprinting code. Fig. 9 (a)~(c) are shown the gray level images of original color images, and also (d)~(f) are shown the images of the inserted 39bits fingerprinting code. And Table 3 and 4 represent PSNR measured values of Y component and gray level images according to the fingerprinting code length.

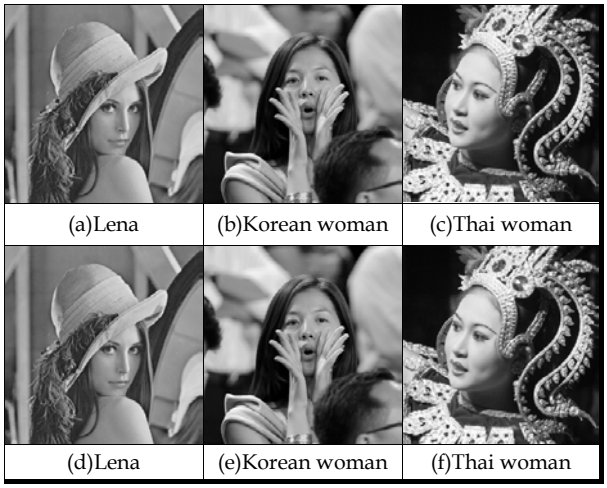
(a)Lena	(b)Korean woman [31]	(c)Thai woman

Fig. 7. Original images(256x256)



(a)Lena	(b)Korean woman	(c)Thai woman
(d)Lena	(e)Korean woman	(f)Thai woman

Fig. 8. (a)~(c): Y Component images of original images; (d)~(f): inserted fingerprinting code images



(a)Lena	(b)Korean woman	(c)Thai woman
(d)Lena	(e)Korean woman	(f)Thai woman

Fig. 9. (a)~(c): Gray level images of original images; (d)~(f): inserted fingerprinting code images

In Table 5 and 6, 2nd~4th columns are measured individually PSNR of Y component and gray level images about 3 kinds of 256x256 images by fingerprinting code length 7~127bits. And 5th~7th columns are shown the average PSNR of 3 images about 3 sizes.

At the consideration of fingerprinting code length is 7bits, the measured PSNRs of Y component images are 85.26, 90.63 and 97.13 on 3 kinds of image size. When a length is 39bits, PSNRs are 77.75, 83.37 and 90.11dB, and also length is 127bits, PSNRs are 72.64, 78.37 and 84.29dB by 3 kinds of image size individually.

And also, consider PSNR values of gray level image under the same condition too, the measured PSNRs are 84.35, 91.70 and 99.72 on 3 kinds of image size. When a length is 39bits, PSNRs are 78.08, 84.03 and 88.85dB, and also length is 127bits, PSNRs are 72.28, 78.06 and 84.86dB by 3 kinds of image size individually.

In these results, the variation of PSNR value is not proportional to same fingerprinting code length under the different images of Y component and gray level each. The author would be making a close examination in Eq. (16).

And also with the measured PSNR values in Table 5 and 6, polynomial expression of fingerprinting code length is evaluated in Eq. (16) by regression analysis of the measured PSNR values. And polynomial coefficients are represented in Table 7. As the evaluation of the fingerprinting code length, 3 polynomial coefficients a_n and a constant C are existed in Eq. (16) for Y component and gray level each.

This expression can be shown to predict a fingerprinting code length by a measured PSNR of Y component or gray level image.

$$Fingerprinting_{Code\_lenght} = a_3 x^3 + a_2 x^2 + ax + C \tag{16}$$

where x: PSNR value

Fingerprinting Code Length (bit)	Lena	Korea_ woman	Thai_ woman	Average		
	Image size 256x256			Image size 128x128	256x256	512x512
7	93.3	89.3	89.3	85.26	90.63	97.13
11	87.8	87.3	87.8	82.31	87.63	94.58
15	88.5	85.9	86.8	81.75	87.07	93.64
19	87.3	87.8	86.3	81.29	87.13	93.80
23	85.9	85.2	84.5	79.25	85.20	91.53
31	85.2	83.1	85.2	79.24	84.50	90.32
39	83.1	84.3	82.7	77.75	83.37	90.11
47	83.1	83.1	81.8	76.48	82.67	88.60
63	82.1	80.2	81.7	75.57	81.33	87.25
79	80.6	80.9	80.3	74.34	80.60	86.24
95	79.2	79.4	79.2	73.45	79.27	85.50
127	78.6	77.8	78.7	72.64	78.37	84.29

Table 5. Measured PSNR(dB) of Y component images

Fingerprinting Code length (bit)	Lena	Korea_ woman	Thai_ woman	Average		
	Image size			Image size		
	256x256			128x128	256x256	512x512
7	93.3	91.5	90.3	84.35	91.70	99.72
11	89.3	90.3	89.3	82.76	89.63	95.39
15	90.3	88.5	88.5	82.12	89.10	95.97
19	87.8	86.8	87.8	81.58	87.47	92.26
23	85.5	86.8	85.9	79.39	86.07	91.41
31	85.9	85.2	84.0	78.78	85.03	91.41
39	84.5	83.1	84.5	78.08	84.03	88.85
47	81.5	84.0	82.9	76.18	82.80	88.24
63	81.5	81.2	81.2	75.39	81.30	87.76
79	80.9	80.2	81.5	74.78	80.87	86.41
95	78.8	79.7	79.7	73.09	79.40	85.52
127	78.0	78.2	78.0	72.28	78.07	84.86

Table 6. Measured PSNR(dB) of gray level images.

And with Eq. (16), the computed result of fingerprinting code length is shown in Fig. 10. In the case of larger 86dB PSNR, the inserted fingerprinting code length in Y component image is shorter than gray level image processing. And in the case of lower 86dB PSNR, the inserted fingerprinting code length of gray level image is shorter than Y component image processing.

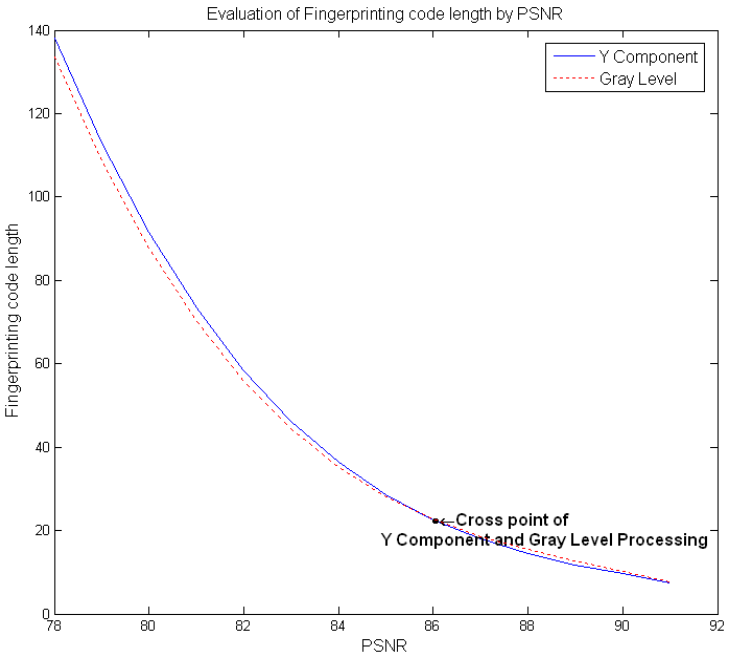


Fig. 10. Evaluation of fingerprinting code length by PSNR value.

Polynomial Coefficient	a_3	a_2	a	C
Y Component	-0.054102	14.677	-1329.2	40,196
Gray level	-0.061901	16.621	-1490	44,609

Table 7. Polynomial coefficients of Eq. (13). (Y component and Gray level)

5. Conclusions

The proposed algorithm in this article, firstly, multimedia fingerprinting code is generated base on BIBD code. Secondly, the usable collusion codes are evaluated for the effect increasing of anti-collusion by the proposed scheme, and the usable collusion codes could be manifesting for an attending colluder would be changing a non-attending user lucratively or a non-attending user would be changing an attending colluder unfortunately. Thirdly, for the increasing image quality, the fit fingerprinting code length is evaluated when user fingerprinting code is inserted into content.

It confirmed that the efficiency of useful collusion codes is 44.13%, the tracing number of the attending colluder is extending to n-1 users with 1-resilient code. Thus, this fingerprinting code would be enough satisfying the criteria of ACC. Furthermore, if it emphasizes a protection or security of content copyright, an inserted fingerprinting code length can't but be long more, and then image content's quality can't but relatively decrease.

The creator or proprietor of content is desiring to keep high PSNR image content, they can choose a fit fingerprinting code length according to the desirable PSNR value. As a experimental results, the reference values of PSNR and fingerprinting code length are evaluated 86dB and 22bits each to the image of Y component and gray level both. When 7~127bits BIBD code was used as fingerprinting code for multimedia content, in the choice of larger 86dB PSNR, the fingerprinting code length will be great to insert into Y component image for shorter than gray level transform. On the other hand, in the choice of lower 86dB PSNR, the fingerprinting code length will be great to insert into gray level image for shorter than Y component transform.

In this article, the implemented algorithm could be widely applied to trace up the illegal distributor of multimedia content on the various colluded attacks, which consisted of Logical operation and Averaging of fingerprinting code base on BIBD code.

6. Acknowledgment

This study was supported in part by Korea Government, Ministry of Education, Science and Technology Fund 2011-0026144.

And this article is rearranged (IDC), 2010 6th International Conference on, Print ISBN: 978-1-4244-7607-7, INSPEC Accession Number: 11526187

7. References

[1] Jie Yang, Pingg Liu and Guo Zhen Tan, "The Digital Fingerprint Coding Based on LDPC," *ICSP'04 Proceedings,* pp.2600-2603, 2004.

[2] K. H. Rhee, "DRM Implementation by Multimedia Fingerprint," *IEEK Computer Society,* Vol.46, No.3, pp.50~56, 2009. 5.

[3] K. H. Rhee, "An Embedded Watermark into Multiple Lower Bit planes of Digital Image," *IEEK Computer Society,* Vol. 43, No. 8, pp.101-109, 2006. 11.

[4] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Tran. on Information Theory,* vol. 44, pp. 1897–1905, September 1998.

[5] Trappe W., Min Wu, Ray Liu K.J., "Collusion-resistant fingerprinting for multimedia," *IEEE International Conference on Acoustics, Speech, and Signal Processing 2002, Proceedings (ICASSP '02),* vol.4, pp.IV-3309-IV-3312, 13-17 May 2002.

[6] Lin W. S., Zhao H. V., Ray Liu K. J., "Scalable Multimedia Fingerprinting Forensics with Side Information," *IEEE International Conference on Image Processing, 2006,* pp.2293-2296, 8-11 Oct. 2006

[7] W. G. Kim, S. H. Lee and Y. S. Seo, "Robustness Digital Fingerprinting Technology to Collusion Attack," *KIISE,* ISSN 1015-9908, Vol.23, No. 8, pp. 52~60, Sept. 2005

[8] Jie Yang, Xiaoxia Xu, "A Robust Anti-collusion Coding in Digital Fingerprinting System," *IEEE Asia Pacific Conference on Circuits and Systems, APCCAS 2006,* pp.996 - 999, 4-7 Dec. 2006

[9] Shashanka D., Bora P.K, "Collusion Secure Scalable Video Fingerprinting Scheme," International Conference on Advanced Computing and Communications, *ADCOM 2007,* pp.641-647, 18-21 Dec. 2007

[10] Jie Yang, Xiaoxia Xu, "A Robust Anti-collusion Coding in Digital Fingerprinting System," *The 8th International Conference on Signal Processing,* Volume 4, 2006

[11] Zang Li and Trappe W, "Collusion-resistant fingerprints from WBE sequence sets," *IEEE International Conference on Communications, ICC 2005,* Vol. 2, pp. 1336-1340, 16-20 May 2005.

[12] In Koo Kang, Choong-Hoon Lee, Hae-Yeoun Lee, Jong-Tae Kim, Heung-Kyu Lee, "Averaging attack resilient video fingerprinting," *IEEE International Symposium on Circuits and Systems, ISCAS 2005,* Vol. 6, pp.5529-5532, 23-26 May 2005.

[13] J. S. Noh, K. H. Rhee, "Detection of Colluded Multimedia Fingerprint by Neural Network," *IEEK Computer Society,* Vol.43, No.4, pp.80~87, July 2006.

[14] K. H. Rhee, "Detection of Colluded Multimedia fingerprint using LDPC and BIBD," *IEEK Computer Society,* Vol.43, No.5, pp.68~75, Sept. 2006.

[15] J. Kilian, T. Leighton, L. R. Matheson, T. G. Shammon, R. E. Tarjan and F. Jane, "Resistance of Digital Watermarks to collusive Attacks," *Tech. Rep., TR-585-98, Dept. of Computer Science,* Princeton University, 1998.

[16] Wade Trappe, Min Wu, Jane Wang and K. J. Ray Liu, "Anti-collusion Fingerprinting for Multimedia," *IEEE Tran. on Signal Processing,* VOL.51, NO.4, pp.1069~1087, April 2003.

[17] F. Ergun, J. kilian and R. Kumar, "A note on the limits of collusion-resistant watermarks," *in Eurocrypt* '99, pp.140-149, 1999.

[18] J. K. Su, J. J. Eggers and B. Girod, "Capacity of digital watermarks subjected to an optimal collusion attack," in *European Signal Processing Conference (EUSIPCO 2000)*, 2000.

[19] Willard H. Clatworthy, "Tables of two-associate-class partially balanced design," *National Bureau of Standards,* Washington D.C., U.S., 1973.

[20] D. R. Stinson and R. Wei, "Combinatorial Properties and Construction of Traceability Schemes and Frame proof codes," *J. of Discrete mathematics,* Jan. 1997.

[21] H. Vicky Zhao, MinWu, Z. JaneWang, and K. J. Ray Liu, "Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting," *IEEE Transactions on Image Processing,* Vol. 14, No. 5, pp.646-661, May 2005

[22] Shuhui Hou, Tetsutaro Uehara, Takashi Satoh, Yoshitaka Morimura and Michihiko Minoh, "Integrating Fingerprint with Cryptosystem for Internet-Based Live Pay-TV System," *Security and Communication Networks, Volume 1, Issue 6,* pp.461 – 472, 18 Nov. 2008.

[23] Byung-Ho Cha, and C.-C. Jay Kuo, "Robust MC-CDMA-Based Fingerprinting Against Time-Varying Collusion Attacks," *IEEE Transactions on Information Forensics and Security,* Vol. 4, NO. 3, pp.302-316, September 2009.

[24] Jae-Min Seol and Seong-Whan Kim, "A Scalable Fingerprinting Scheme for Tracing Traitors/Colluders in Large Scale Contents Distribution Environments," *Proceedings of the 2005 5th International Conference on Intelligent Systems Design and Applications (ISDA'05)*, 2005.

[25] Dalwon Jang and Chang D. Yoo, "A Novel Embedding Method for an Anti-Collusion Fingerprinting by Embedding Both a Code and an Orthogonal Fingerprint," *ICASSP 2006*, pp.V485-488, 2006.

[26] Yongdong Wu, "Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting," *ICASSP 2005*, pp.II13-16, 2005.

[27] Wade Trappe, Min Wu, and K. J. Ray Liu, "Anti-Collusion Codes: Multi-User and Multimedia Perspectives," *Image Processing. 2002. Proceedings 2002 International Conference on,* Vol. 2, pp.II149-II152, 2002.

[28] InKoo KANG, Kishore SINHA and Heung-Kyu LEE, "New Digital Fingerprint Code Construction Scheme Using Group-Divisible Design," *IEICE Trans. Fundamentals, Vol.E89–A, NO.12,* pp.3732-3735, December 2006

[29] J. Dittmann, "Combining Digital watermarks and Collusion Secure Fingerprints for Customer Copy Monitoring," *Proc. IEE Seminar Sec. Image & Image Auth.,* pp. 128-132, Mar. 2000.

[30] F. Sebe and Domingo-Ferrer, "Short 3-Secure Fingerprinting Codes for Copyright Protection," *Lecture Notes in Computer Science,* Vol. 2384, pp. 316-327, 2002.

[31]http://news.joins.com/component/htmlphoto_mmdata/200907/htm_20090727152308c000c010-001.JPG, 10. Oct. 2008

[32] Sanjay Kr. Singh1, D. S. Chauhan, Mayank Vatsa, Richa Singh,"A Robust Skin Color Based Face Detection Algorithm," Tamkang Journal of Science and Engineering, Vol. 6, No. 4, pp. 227-234 (2003) 227

[33] http://www.roman10.net/?p=485