Frame Background Influence Based Invisible Watermarking to Visible Video Watermarking

Ta Minh Thanh*†, Pham Thanh Hiep‡
* Tokyo Institute of Technology, 2-12-2, Ookayama, Meguro-ku, Tokyo, 152-8552, Japan.
† Le Quy Don Technical University, 100 Hoang Quoc Viet, Cau Giay, Hanoi, Vietnam.
Email: thanhtm@ks.cs.titech.ac.jp
‡School of Engineering, Yokohama National University, Yokohama, Japan.
Email:hiep@kohnolab.dnj.ynu.ac.jp

***Abstract*—In this paper, we propose a novel watermarking scheme where both visible and invisible watermarking are embedded into video sequences. Our invisible watermarking is implemented based on the influence of background after embedding the visible watermarking by the adaptive cross correlation (ACC) method. By doing so, our method can be used to achieve two purposes: 1) to announce the ownership of video and 2) to distinguish the legal user. Experimental results showed that our proposed method is suitable for digital e-commerce business and is robust against slight geometrical attacks and video processing attacks.**

***Index Terms*—Visible Watermarking, Invisible Watermarking, Adaptive Cross Correlation (ACC), Video Sequences.**

I. Introduction

Recently, digital multimedia distribution via network has grown rapidly as a result of the latest developments in network and computer technologies. With the continuously developing availability of the Internet, the e-commerce of digital multimedia is also increased. However, the digital multimedia can be easily shared, processed or used causing serious security problems such as ownership identification, illegal distribution and so on. As a promising solution to this problem, many watermarking are now under investigation for protecting owner's intellectual property rights and tracing illegally source distribution.

Generally, there are two types of watermarking : invisible watermarking [1] and visible watermarking [2]. Visible watermarking is used to announce the ownership of the digital content such as TV programs, online video broadcasting video and so on. The owner usually visibly embeds his logo into the digital contents. Therefore, the visible watermarking is required that it should be easily visible, unobtrusive, and non-removable. In invisible watermarking, the embedded information should not appear in the video *i.e.*, it must be perceptually invisible [1]. The invisible watermarking techniques are mainly used for copyrights protection, ownership identification, detection of illegal source redistribution, *etc.* The invisible watermarking provides more security to video with less distortion, though the visible watermarks protect the digital data in more active manner.

However, there are some benchmarks that endeavor to remove the embedded information from digital multimedia. In case of visible watermarking, some attackers is interested in removing the visible watermarking from videos because of visible watermarking decreases the quality of videos. In fact, there are some techniques is developed for removing the visible watermark to obtain the high quality of videos [3], [4], [5]. In order to remove the visible watermark in video, the attacker has to detect the logo location first, then repair the video region where the logo is occupied by replacing the logo region with the estimated video region [6]. With another idea, Yan *et al.* [9] proposed another method to detect logo by exploring the temporal correlation of video frames and Huang *et al.* [3] employed the image inpainting techniques to erase video logos. After removing the logo, they hope they can obtain the high quality of digital multimedia.

According to Wu [10], to enhance the robustness of visible embedding, he can randomize the logo in frames of location, shape, scalar, and a lot of distortion methods without reducing the logo. Wu's method made it becomes difficult to manually erase logos in video by attacker. However, the robustness of visible watermarking just enhances to announce the ownership of creator. If a user purchases the digital video from creator and redistributes again via network to get extra profit, he is not judged as illegal distributor because of there is not evidence to prove his action. Therefore, it is necessary to develop a invisible watermarking to digital multimedia with visible watermarking to ensure that creator can trace the illegal distribution source.

In this paper, we propose a scheme of an invisible watermarking technique based on adaptive cross correlation (ACC) to provide additional protection for visible watermarking in video. Our method first implement the visible watermarking and then extract the visible watermarking logo to calculate the normalization cross correlation (NCC) of logo regions. After that, the invisible watermarking, *e.g.* user ID, can be embedded into visible logo regions of video by using proposed ACC method.

The rest of the paper is organized as follows: in Section 2, we briefly review problem of business model for visible watermarking and analyze the need of invisible watermarking on that. The proposed watermarking technique based on ACC is detailly explained in Section 3. Experimental results on several video sequences are presented in Section 4 to demonstrate the performance of proposed method in the network distribution

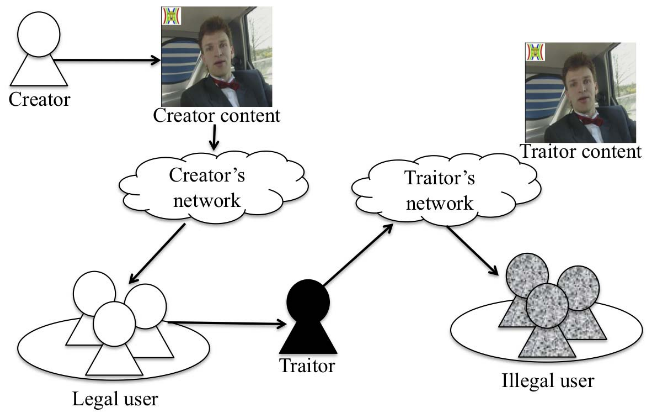

Fig. 1. Problem of digital multimedia business model.

system. Finally, we conclude in Section 5.

II. Why We Need Invisible Watermarking beside Visible Watermarking?

In general, in the digital multimedia business model, creator C always embed own logo to announce the ownership of digital content P. He widely sell his digital content to users via network as shown in **Fig. 1**. User U can purchase the digital content and use it with the license of legal user. However, if an user (traitor) redistributes the digital content P via another network (traitor's network), he can get extra profit from illegal users without the permission of creator. Therefore, creator will lose the benefit from the online business and he has no way to detect the traitor.

From the problem that is analyzed above, we need an invisible watermark that can enhance ownership protection of the visibly watermarked logo and it can be used to detect the traitor. So we need the invisible watermarking scheme in the dual watermarking system for our purposes: 1) to announce the ownership of video and 2) to distinguish the legal user and 3) to detect the traitor.

III. Proposal of Video Watermarking based on Adaptive Cross Correlation

In this section, we explain the mechanism to embed the visible watermarking and then to embed the invisible watermarking in the visible watermarking region based on adaptive cross correlation (ACC). Since Wo $et\ al.$ [10] proposed a method that made it becomes difficult to manually erase logos in video, we employ the method of [10] to enhance the robustness of visible embedding first; and use the invisible watermarking which is embedded into logo region of creator to detect the traitor. In the following subsections, we describe the details of the proposed invisible watermarking scheme to visible watermarking system.

A. Video embedding

The overview of proposed embedding method is shown in **Fig. 2**. First, we randomly and automatically embed the visible logo of creator at the right-top or right-bottom of

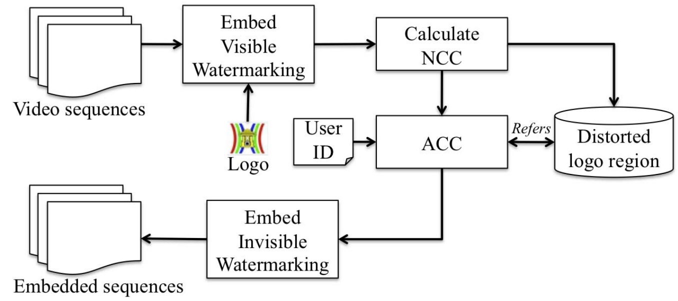

Fig. 2. The overview of embedding method.

every frame in video. Then, we extract again the embedded logo region to calculate the NCC of the embedded logo comparing the original logo. After calculating the NCC values of the embedded logo, we control the embedded logo region based on user information, $i.e$ user ID, by using the adaptive cross correlation (ACC) method to implement the invisible watermarking. The details of embedding method is following,

1) Visible watermark embedding: We use the visible watermarking to announce the ownership of creator. In order to achieve the robustness of visible watermarking, we apply the method of [10] to embed the visible logo. Suppose that the original logo L_o is embedded into the frame F to make the watermarked frame F_w. The watermarking method is represented as follows,

$$F_w = (1-\alpha)F + \alpha L_o \tag{1}$$

where α is watermarking strength, $\alpha = 1$ indicates overlapped watermarking, $\alpha = 0$ means that the frame is skipped for embedding, otherwise, transparent watermarking.

We can randomly change the logo of creator for several frames based on the random logo database which is prepared beforehand. The random logos are created by image processing tools, $e.g.$ Adobe Photoshop^{TM}, GIMP 2.8, ImageMagick, etc. We also can change the location of logo in the frame but we embed the logo at the same location to easily understand. Although we embed the logo of creator at the same location, it is difficult to be completely removed from a frame by attacker as mentioned in [10].

Fig. 3 shows the example of the embedding of visible watermarking. We can randomly embed the distorted visible logo L_d of creator into every frame. The distorted logos L_d are generated by GIMP 2.8[1] with the image processing such as Rotation, Emboss, Shift Pixel and so on. Note that, in our method, L_d can be used to replaced L_o in (1) to enhance the robustness of the visible watermarking as [10]. Since a logo in video merely announces the copyright or ownership of video content, it is clear that the quality of the logo is not very important, and the fidelity of the logo is decided by the viewers. Therefore, the embedding of the distorted logos L_d will not disturb the viewers anymore. Reader should

[1]http://www.gimp.org/

Fig. 3. The embedding of visible watermarking. The distorted logos are created by GIMP 2.8. If shot change is detected, the visible logo is randomly embedded. The embedding strength $\alpha = 0.5$.

note that we only focus on the distortion of creator's logo to present the invisible watermark, $e.g.$ user ID. The details of invisible watermark embedding method is explained in subsection III-A3.

2) Preprocess: average $\overline{NCC}$calculation: After the creator's logo L_d embedding, the effectiveness of watermark strength α and the influence of video background make the quality of logo more distortion. Therefore, we can employ the distortion of visible logo region to embed the invisible watermarking into visible logo region. First, we extract the embedded the logo regions L_d and calculate the normalization cross correlation (NCC) of those with the original logo L_o as below,

$$NCC(i) = \frac{\sum_{l=1}^{M}\sum_{k=1}^{N}[L_o(l,k) \times L_w(l,k)]}{\sum_{l=1}^{M}\sum_{k=1}^{N}[L_o(l,k)]^2} \tag{2}$$

where $NCC(i)$ is the NCC value of the distorted logo in the i^{th} frame. L_w is the extracted logo region after embedding and $M \times N$ is the size of logo region.

In order to prepare the threshold for invisible watermark embedding, we calculate the average NCC ($\overline{NCC}$) is following,

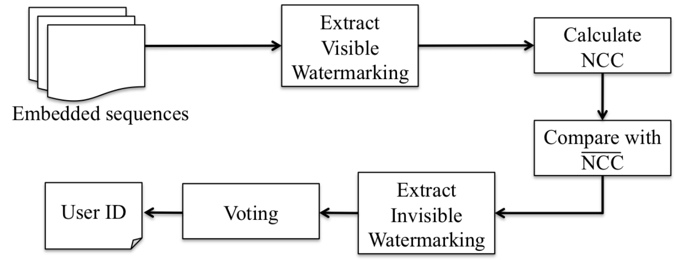

Fig. 4. The overview of extraction method.

$$\overline{NCC} = \frac{\sum_{i=1}^{F_N} NCC(i)}{F_N} \tag{3}$$

where F_N is the number of frame in video. We employ the $\overline{NCC}$ as the threshold to embed the invisible watermark into the visible logo region of creator. After calculating the $\overline{NCC}$, we divide the distorted visible logos L_w into two categories (C_1 and C_0) according to the embedded bit, that C_1 consists of L_w with $NCC > \overline{NCC}$ and C_0 consists of L_w with $NCC \leq \overline{NCC}$.

3) Invisible watermark embedding based on ACC: Given a watermark information W as the user ID of legal user. We extract one bit $W(i)$ from W and control the visible logo region based on $W(i)$ and $NCC(i)$. According our embedding method, the NCC value of visible logo in i^{th} frame is adapted based on the $W(i)$. The adaptation control is described as follows,

- When $W(i)$ = "1": if $NCC(i) > \overline{NCC}$, then nothing changes. Otherwise, we randomly choice another distorted logo from category C_1 and replace it at the location of visible logo in frame.
- When $W(i)$ = "0": if $NCC(i) < \overline{NCC}$, then nothing changes. Otherwise, we randomly choice another distorted logo from category C_0 and replace it at the location of visible logo in frame.

We repeat above process until all frames of video are marked by W and obtain the embedded video sequences.

B. Invisible watermark extraction

Fig. 4 describes how to extract the invisible watermark information W from the visible logo regions. We extract the visible logo regions from all frames of video. After that, we calculate the $NCC(i)$ by equation (2) and then obtain $\overline{NCC}$ as equation (3). The embedded bit can be extracted by comparing $NCC(i)$ and $\overline{NCC}$: If $NCC(i) > \overline{NCC}$ then $W'(i) = 1$, otherwise $W'(i) = 0$, where $W'(i)$ is the extracted bit which is retrieved from logo region in i^{th} frame of the embedded video sequences.

After the watermark is extracted from all the frames. Since there are F_N frames, the number of the extracted bits will

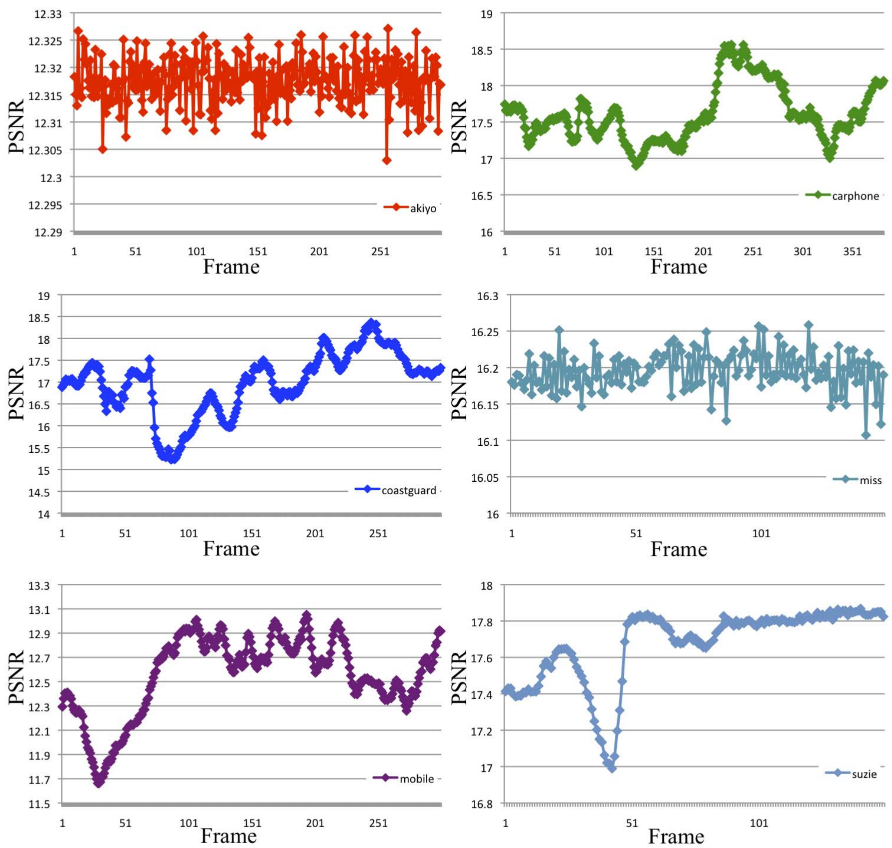

Fig. 5. The PSNR values of logos in video in case of the watermark strength $\alpha = 0.5$. Top row: Akiyo, Carphone; middle row: Coastguard, Miss; bottom row: Mobile, Suzie.

also be F_N . The final watermark W_v needs to be constructed from these F_N watermark bits based on some decisions. In our method, voting method is made using maximum occurrence of bit value (either bit "0" or bit "1") corresponding to same pixel location in all extracted watermarks. This voting method can be represented by mathematical method using the following equation,

$$W_v(t) = voting(W'(i)), 1 \leq t \leq \frac{F_N}{W_L} \tag{4}$$

where W_L is the length of W.

IV. Simulation Results

In this section, we implement the invisible watermarking in visible watermarking by using ACC method. By doing so, we can prove the efficiency of proposed method for ownership of video and tracing the illegal users.

A. Experimental environment

All experiments were performed in the Mac OSX 10.6.8 system. The invisible watermark is generated by random binary sequences with the length $W_L = 20$. GCC version 4.0.1[2] and the MPlayer version 1.1-4.2.1[3] were used to convert and view the experimental video data. $rand()$ function with $seed = 1$ is employed to generate the invisible watermark.

To evaluate the proposed method fairly, we used different standard of six video sequences[4] (Akiyo: 300 frames, 25fps; Coastguard: 300 frames, 25fps; Carphone: 382 frames, 12fps; Miss: 150 frames, 25fps; Mobile: 300 frames, 25fps; Suzie: 150 frames, 25fps) in QCIF format ($Width \times Height = 176 \times 144$).

1) Evaluation of quality for visible watermarking: We used PSNR (Peak Signal to Noise Ratio) [13] to evaluate the logo region quality. The PSNR of $M \times N$ pixels of original logo $L_o : g(i,j)$ and extracted logo $L_w : g'(i,j)$ is calculated with

$$PSNR = 20 \log \frac{255}{MSE} \quad \text{[dB]} \tag{5}$$

$$MSE = \sqrt{\frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \{g(i,j) - g'(i,j)\}^2}$$

$$(MSE : Mean\ Square\ Error).$$

In these experiments, we applied the visible watermark embedding to video file and the PSNR of the watermarked region against the original logo were calculated to observe. It

[2]http://gcc.gnu.org/

[3]http://www.mplayerhq.hu/design7/dload.html

[4]http://media.xiph.org/video/derf/ (Accessed on 25 May 2013)

is clear that the PSNR values of logo regions are very low (lower than 20dB) as shown in **Fig. 5** but the logo is still well recognized as a valid logo to announce the ownership of content. Therefore, the measure PSNR of visible logo may be not suitable for evaluating the acceptance of visible logo embedding. According to Fig. 5, it is clear that the frame background obviously affects the quality of visible watermarking. Especially, the unstable background which has many motions such as Carphone, Coastguard and Mobile, may affect a lot the quality of visible watermarking. Whereas, the stable background such as Akiyo, Miss and Suzie, gives us the stable PSNR value for quality of visible watermarking (logo region). However, in order to embed the invisible watermarking by using the region of visible watermarking, the unstable background in the logo region is desirable because we can easily control the logo region to describe the bit information by the proposed ACC method.

2) Evaluation of embedding for invisible watermarking: First, we embedded the random watermark information W (20 bits) into the visible logo regions by adaptation of NCC value of the visible logo regions. We repeated to embed W until all frames are processed.

Since our method depends on the frame to embed the invisible watermark into the visible logo regions, thus, our method may be not robust against the temporal attacks such as frame dropping, frame insertion, frame transposition, frame averaging and so on. Such kind of attacks will be resolved in our future work.

In order to test the robustness of our proposed method, we implemented a video watermarking attack tool named VirtualDub[5] program to modify the watermarked videos with various types of attacks. Then, we extracted the invisible watermark information from the modified videos. The experimental results are assessed by the bit correct rate (BCR) of the extracted watermark, as the following equation,

$$BCR = \frac{e}{m} \times 100\% \tag{6}$$

where e is number of correct bits of the extracted watermark, and m is the number of total bits of the extracted watermark. If BCR is close to 100%, the more higher of the correct rate. In our work, let the threshold $T_b = 70\%$ that is determined by experiments. If BCR$> T_b$, the watermark is detected.

The experimental results are shown in **Table. I**. Since our embedding method compares with the average NCC ($\overline{NCC}$) of logo regions in the all frames to embed and extract the invisible watermark, therefore, our invisible watermark can survive under some attacks. Clearly, when the logo regions are distorted, $\overline{NCC}$ is changed, thus we could correctly extract the invisible watermark by comparing with $\overline{NCC}$. **Fig. 6** shows all attack methods that were performed on the embedded video sequences. Only 10^{th} frame of Vid2 is shown in Fig. 6. Table. I showed that our extraction rate was over than $T_b = 70\%$, and our proposed method seems to be robust against some attacks.

[5]http://www.virtualdub.org/

TABLE I
EXPERIMENTAL RESULTS OF ROBUSTNESS.

Attack	Vid1	Vid2	Vid3	Vid4	Vid5	Vid6
No attack	95	95	95	95	95	95
Rotation w. crop (1^0)	75	95	50	50	50	70
Rotation w. crop (2^0)	75	95	60	50	50	50
Scaling 1.0-2.0-1.0	70	80	90	50	50	80
Grayscale	50	95	50	50	50	80
Blur	50	90	50	90	50	80
Brightness & Contrast	80	95	50	60	50	75
TV Y-channel	50	95	50	80	50	50
Invert Color	50	90	50	50	50	50
Smoother	95	95	50	50	50	50
Emboss	50	85	60	50	50	50
Deinterlace	50	90	50	90	50	50

Note: Vid1: Akiyo, Vid2: Carphone, Vid3:Coastguard, Vid4:Miss, Vid5:Mobile, Vid6: Suzie

TABLE II
COMPARISON BETWEEN OUR PROPOSED METHOD WITH [10].

Comparison	*Ours*	[10]
Announce ownership	◯	◯
Distinguish user	◯	×
Robustness of visible watermarking	◯	◯
Robustness of invisible watermarking under some attacks	◯	×

In addition, we compared our proposed method with [10]. The detail of comparison of our method with [10] is shown in **Table. II** ("◯" means very Good; "×" means Bad). It is very clear that our method is beter than [10] because ours has the additional invisible watermarking. Therefore, our method can be used to distinguish the legal users and it can be survise under some attacks.

According to the above results, we have established the invisible watermark embedding system based on the ACC for visible watermark. Our proposed method does not disturb the quality of the whole frame, just distorts the visible logo regions but viewers do not care about it. Then, we can use the logo region to perform the invisible watermarking that is user's information. Using our proposed technique, the producer does not only announce the ownership of video, but also distinguish the legal user.

V. CONCLUSION

In this paper, we have presented a scheme of an invisible watermark embedding to the visible watermark using ACC. The effectiveness of the proposed scheme has been demonstrated with the aid of experimental results. Our proposed scheme can be used to embed the invisible watermark into logo regions without the perception of viewers. Experimental results also showed that the proposed method was more robust to video processing attacks such as blur, smoother, rotation, scaling and so on.

In the future work, we want to implement our method more robust against the temporal attacks and speed the embedding/extraction watermark.

Fig. 6. The example of attacked video Vid2 . From top-line to bottom-line: No attack, Rotation w. crop (1^0), Rotation w. crop (2^0), Scaling 1.0-2.0-1.0, Grayscale, Blur, Brightness & Contrast, TV Y-channel, Invert Color, Smoother, Emboss, Deinterlace

REFERENCES

[1] I. J. Cox, J. Kilian, T. Leighton, and T. G. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia,h IEEE Trans. on I. Proc., 6(12):1673-1687,1997.

[2] J. Meng, S.F. Chang, "Embedding visible video watermarking in the compressed domain,h ICIP, 474-477, 1998.

[3] SC.H. Huang, and J.L. Wu, "Inpainting attacks against visible watermarking schemes,h Proc. SPIE Conf. on Security And Watermarking Of Multimedia Contents, vol. SPIE 4314, pp. 376–384, 2001.

[4] Yongjian Hu, Sam Kwong, Jiwu Huang, "An algorithm for removable visible watermarking," IEEE Trans. Circuits Syst. Video Techn., 16(1), pp.129-133, 2006.

[5] Ying Yang, Xingming Sun, Hengfu Yang, Chang-Tsun Li, "Removable visible image watermarking algorithm in the discrete cosine transform domain," J. Electronic Imaging 17(3): 033008, 2008.

[6] S.P. Mohanty, M.S. Kankanhalli, K.R. Ramakrishnan, "A DCT domain visible watermarking technique for images,h Proc. of ICME, pp.1029–1032, 2000.

[7] Ta Minh Thanh, K. Shinoda, "A video watermarking method to objects robust against various attacks," Enriched Multimedia, IEICE Technical Report, Vol. 112, No. 190, pp. 43-48, Aug. 2012.

[8] Ta Minh Thanh, Pham Thanh Hiep and Ta Minh Tam, "Frame-Patch Matching based Robust Video Watermarking using KAZE Feature," Proc. of ICME, 2013 (to appear).

[9] Wei-Qi Yan, Jun Wang, Mohan S. Kankanhalli, "Automatic Video Logo Detection and Removal,h Multimedia Systems, 10(5): pp.379–391, 2005.

[10] Yongdong Wu, "Protection of Video Logo with Randomization," Proc. of IEEE ICME, pp.1341–1344, Toronto, 2006.

[11] P.W.Wong and N.Memon,"Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Trans. on Image Processing, vol.10, pp. 1593–1601, 2001.

[12] S.P. Mohanty, K.R. Ramakrishnan, M.S. Kankanhalli, "A dual watermarking technique for images," ACM Multimedia (2), pp. 49–51, 1999.

[13] I. Munetoshi, Ta Minh Thanh, "Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management," The 26th IEEE AINA-2012, 2012.