UNSEEN VISIBLE WATERMARKING

Shang-Chih Chuang, Chun-Hsiang Huang and Ja-Ling Wu

Department of Computer Science and Information Engineering,
National Taiwan University, Taipei, Taiwan
E-mail: {peiz, bh, wjl}@cmlab.csie.ntu.edu.tw

ABSTRACT

A novel data-hiding methodology, denoted as unseen visible watermarking (UVW), is proposed. The proposed scheme is inspired by real-world watermarks and possesses advantages of both visible and invisible watermarking schemes. After watermark embedding, the differences between the original work and the stego work are imperceptible under normal viewing conditions. However, when the hidden message is to be extracted, no explicit watermark extracting module is required. Semantically-meaningful watermark patterns can be directly recognized from the stego work as long as common imaging-related functions, e.g. gamma-correction or even simply changing the user-viewing angle relative to the LCD monitor, are performed. The proposed scheme outperforms existing invisible watermarking methods in its capability to practically convey metadata to users of legacy display devices lacking renewal capability. On the other hand, it does not suffer from the annoying quality-degradation problem of visible watermarking schemes. Limitations and possible extensions of the proposed schemes are also addressed. We believe that many interesting new applications can be facilitated using such unseen visible watermarking schemes.

Index Terms—*Watermarking, Unseen Visible Watermarking, Image Enhancement, Metadata Delivery*

1. INTRODUCTION

Real-world watermarks being embedded into physical objects like bills or letter papers are invisible or at least unobvious under normal viewing conditions. However, when the viewing condition changes in certain ways, e.g. looking at the watermark carrier against light sources, watermark patterns will become recognizable by naked eyes. Fig. 1 shows the typical usage scenario of real-world watermarks for authenticating bills.

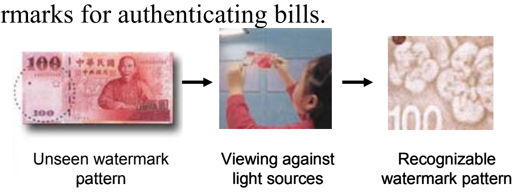


Fig. 1 Real-world watermarking-based bills authentication

After entering the digital era, digital watermarking technologies have emerged to facilitate various applications. Roughly speaking, digital watermarking schemes can be divided into two categories: visible watermarking schemes [1-4] embedding unobtrusive but visible patterns into works and invisible watermarking systems [5-7] introducing imperceptible alternations to the cover work in order to hide some messages. Comparisons between the two types of watermarking schemes are summaries in Table I.

Table I: Comparing invisible and visible watermarking schemes

Characteristics	Invisible Watermarking	Visible Watermarking
Fidelity	Imperceptible	Unobtrusive but visible
Possible Attacks	Media processing or malicious removal	Malicious removal, e.g. [8]
Message Form	Arbitrary (any binary representation)	Meaningful patterns
Explicit Extractor	Required	Not required
Message Notifying	Passive	Active
Complexity	Often higher	Simpler

One of the major disadvantages of visible watermarking lies in the visibility of marked patterns. Though embedded patterns are claimed to be unobtrusive, content viewers still feel annoying about the degrading visual quality. Consequently, applications of visible watermarking are often limited to content browsing or previewing.

As for the invisible watermarking, though good fidelity is always guaranteed, the requirement that an explicit extraction module must exist in the extraction side does introduce additional deployment cost and security problems. To make things worse, in scenarios such as conveying metadata (e.g. annotations, contextual information or copyright claims) to users of legacy display devices lacking modern updating/renewing capability, deploying extractors of invisible watermarking schemes is totally infeasible.

In this paper, a novel watermarking scheme possessing characteristics of both visible and invisible watermarking systems is proposed. Fig. 2 shows a simple illustration of the watermarking system. Since the marked work does not show visible patterns under normal viewing configurations, content users can enjoy high-quality viewing experience of contents. But when viewing conditions change, recognizable watermark patterns will “appear” on the stego work and can be clearly recognized by naked eyes. We denote this methodology as *unseen visible watermarking* since it is basically a visible watermarking scheme. However, the visual quality is close to invisible watermarking schemes under normal viewing conditions. In fact, the architecture of the proposed scheme is more similar to the real-world watermarking scheme, as shown in Fig. 1, than all existing visible or invisible watermarking systems.

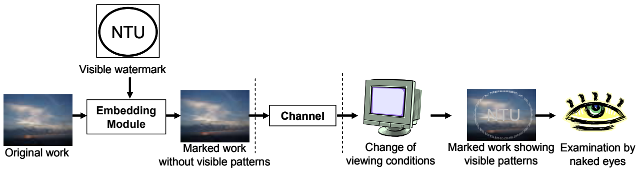

NTU
Visible watermark
Embedding Module
Original work
Marked work without visible patterns
Channel
Change of viewing conditions
NTU
Marked work showing visible patterns
Examination by naked eyes

Fig. 2 The unseen visible watermarking system

This paper is organized as follows. Section 2 illustrates the basic idea behind unseen visible watermarking and demonstrates several feasible viewing-condition alternations. Implementation details and experimental results are provided in Section 3. Section 4 discusses some important application scenarios of the unseen visible watermarking. In Section 5, conclusions and some potential extensions are provided.

2. REVEALING HIDDEN MESSAGES BY IMAGE ENHANCEMENT SKILLS

2.1 Motivations

Image enhancement skills are often applied to help interpreting photographs taken under geographically constrained conditions. As an example, Fig. 3 shows the images of Phobos (one of the Mars moons). Unseen surface details can be clearly recognized after adequately adjusting the contrast settings. However, from another viewpoint, if the unprocessed picture is hypothetically regarded as a stego image hidden with some unseen information (the surface details), the image enhancement process inherently corresponds to the process of altering the viewing condition and revealing the hidden watermark, as illustrated in Fig. 2. Therefore, we investigate some common image enhancement operations in the rest of this section and try to facilitate a new data-hiding approach based on this idea.

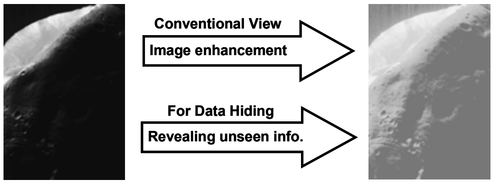


Fig. 3 Viewing image enhancement as watermark extraction

2.2. Gamma Correction

Many display devices possess power-law input-output characteristics, i.e. the output gray level *s* and the input gray level *r* follow the formula:

$$s = cr^{\gamma} \qquad (1)$$

where c and γ are constants. Since many devices tend to produce darker images than they should be, the value of γ usually varies between 1.8 and 2.5. Therefore, the so-called gamma correction is often applied to correct this power-law response phenomenon by applying another power-law gray-level transformation on the image using γ value less than 1. Note that in the cases of common gamma correction ($\gamma < 1$), a narrow range of dark input values will be mapped to a wide range of output gray-level values. Therefore, if we hide some patterns into darker areas of images by performing minute modification to gray-level values of selected pixels, the patterns may be clearly recognizable when gamma corrections are applied to these marked images.

Most importantly, the gamma-correction capability is built in almost all computer monitors or TV sets. Therefore, the application range of unseen visible watermarking schemes can be quite large.

2.3 Different Viewing Angle Relative to LCD Monitors

Liquid crystal display (LCD) monitors have become necessary system components for daily works and entertainment. Basically, LCD displays function by controlling the states of liquid crystal molecules to alter the light-passing conditions of the light source. If an LCD is viewed from different viewing angles, its screen will show different contrast behavior. Though this phenomenon can not be formally formularized due to the lacking of manufacturing details, it can also be utilized to achieve the unseen visible watermarking schemes.

In fact, almost all contrast-adjusting operations, including those introduced in Sections 2.2 and 2.3, can be represented as a specific mapping function between input and output intensity values. These mapping functions often emphasize the contrast within certain ranges of intensity values. Therefore, the unseen visible watermarking scheme can be regarded as a data-hiding approach that hides weak message patterns in areas consisting of pixels whose intensity values lies within the prescribed ranges. After performing certain contrast-adjusting operations, since contrast for those areas are enhanced, users can clearly see the originally unseen watermarks.

3. UNSEEN VISIBLE WATERMARKING

In this section, we illustrate the implementation of unseen visible watermarking schemes in details and show extensive experimental results based on operations introduced in Section 2.

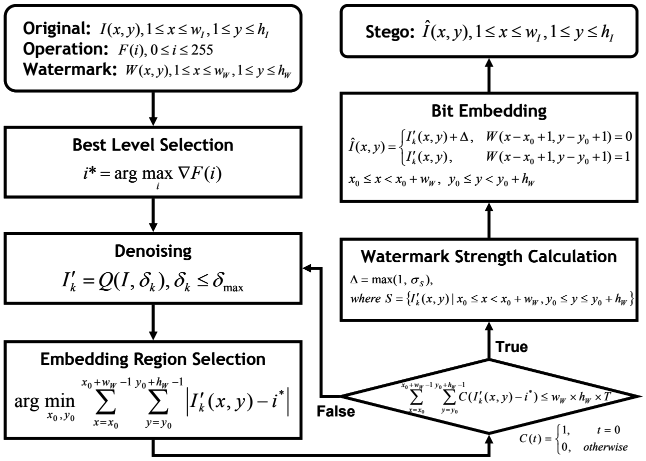

Original: $I(x,y), 1 \le x \le w_I, 1 \le y \le h_I$
Operation: $F(i), 0 \le i \le 255$
Watermark: $W(x,y), 1 \le x \le w_W, 1 \le y \le h_W$
Best Level Selection
$i^* = \arg\max_i \nabla F(i)$
Denoising
$I'_k = Q(I, \delta_k), \delta_k \le \delta_{\max}$
Embedding Region Selection
$\arg\min_{x_0, y_0} \sum_{x=x_0}^{x_0+w_W-1} \sum_{y=y_0}^{y_0+h_W-1} \left| I'_k(x,y) - i^* \right|$
$\sum_{x=x_0}^{x_0+w_W-1} \sum_{y=y_0}^{y_0+h_W-1} C(I'_k(x,y) - i^*) \le w_W \times h_W \times T$
$C(t) = \begin{cases} 1, & t = 0 \\ 0, & otherwise \end{cases}$
False
True
Watermark Strength Calculation
$\Delta = \max(1, \sigma_S)$,
$where\ S = \{I'_k(x,y) \mid x_0 \le x < x_0 + w_W, y_0 \le y \le y_0 + h_W\}$
Bit Embedding
$\hat{I}(x,y) = \begin{cases} I'_k(x,y) + \Delta, & W(x - x_0 + 1, y - y_0 + 1) = 0 \\ I'_k(x,y), & W(x - x_0 + 1, y - y_0 + 1) = 1 \end{cases}$
$x_0 \le x < x_0 + w_W, \ y_0 \le y < y_0 + h_W$
Stego: $\hat{I}(x,y), 1 \le x \le w_I, 1 \le y \le h_I$

Fig. 4 Flowchart of embedding unseen visible watermarks

3.1 Implementation Details

Fig. 4 shows the flowchart describing the k^{th} iteration of the proposed video/image watermarking scheme. Note that operations introduced in Section 2 show the common characteristic that contrast will be altered so that a small range of gray-level values will be mapped to a wider range. Therefore, given an intensity mapping function F describing such operations, the intensity level i^* that has the largest gradient value (calculated according to the mapping function) will be selected as the best level, i.e. the intensity level most suitable for hiding data. And since contrast-adjusting operations also magnify minute noises within original works, image smoothing operations like bilateral filtering or scalar quantization, controlled by a parameter δ_k, are performed. Then, an area that the sum of absolute differences between the gray-level of its consisting pixels and the best level is the smallest among all candidate areas is selected as the embedding region. If the percentage of pixels whose intensity value equals the best level in the selected region is less than a predefined threshold T, a stronger de-noising operation will be performed and the prescribed embedding-region selection procedure will be repeated. Note that the effect of iterative de-noising operations (if needed) can never be too severe due to fidelity concerns and will be limited by an upper bound $\delta_{\max}$. After selecting the embedding region, the watermark patterns are embedded by slightly adjusting the intensity values of pixels within the embedding region. Note that the degree of adjusting is bounded by the standard deviation of intensity values of pixels within the embedding region.

3.2 Experimental Results

Fig. 5 demonstrates two pairs of marked images before and after performing gamma correction simulated by image processing software. It is obvious that the images under normal viewing conditions show good visual quality without being interfered by the watermark pattern. But when gamma corrections are performed, all the hidden watermark patterns clearly appear in the images. To prove that the same experimental results can be reproduced by using the gamma correction functions provided by common display systems, Fig. 6 shows snapshots taken on a Lenovo X60's LCD monitor with a Mobile Intel(R) 945GM Express Chipset Family.

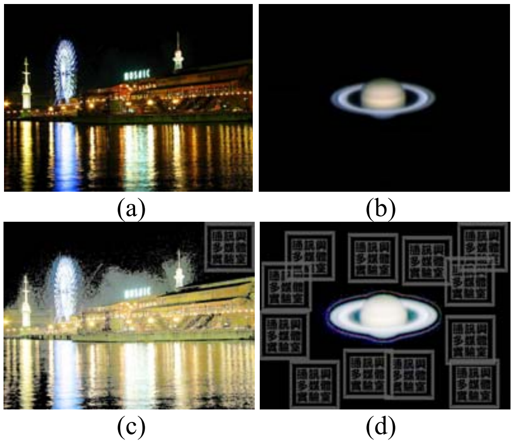


Fig. 5 (a) and (b) are marked images before performing gamma correction; (b) and (d) are gamma-corrected versions.

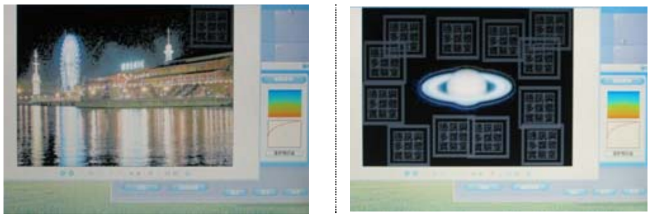


Fig. 6 Snapshots of LCD Displayed marked images when gamma-corrections have been performed.

If we treat video frames as individual images, the embedding procedure shown in Fig. 4 can be directly applied. Note that the embedding position in each frame will change frequently. Fig. 7 shows some snapshots of a marked video sequence (with dimension of 502x338 and bit-rate of 25 frames per second) when performing gamma correction.

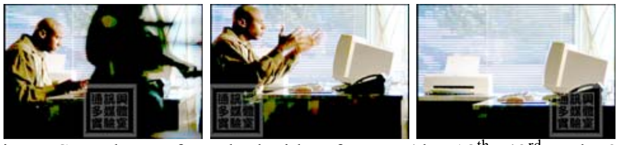


Fig. 7 Snapshots of marked video frames (the 18th, 43rd and 79th frames) before and after performing gamma correction

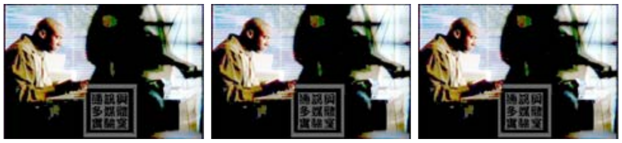


Fig. 8 Gamma-corrected frames out of a H.264 video sequence compressed using different QP values (QP=6, 12 and 18) respectively.

The proposed scheme also shows moderate robustness against common file format conversion. Fig. 8 shows the snapshots of a gamma-corrected video frame undergoing the H.264 video compression using different QP values. Note that the larger the QP value, the worse quality the compressed video sequence will have. The embedded patterns can be recognized out of gamma-corrected video clips that have been compressed with acceptable viewing quality. As for low-quality video, only rough outlines of the hidden patterns can be visualized due to the introduction of larger compression noises. A straightforward solution would be using a larger and simpler watermark pattern instead.

Moreover, this scheme can be used as an alternative mechanism to visible watermarks for digital document readers. Since most digital documents are using white backgrounds, the watermark embedding procedure for digital documents is quite similar to the procedure given in Fig. 4, except that the embedding-position selection function now searches for a bright area within each page. Then, before performing the gamma-correction based extraction operation, the digital documents should be displayed in inverse intensity. The inverse display function is readily provided by common image processing tools. Fig. 9 shows a marked document and the inversed version clearly demonstrating the embedded patterns.

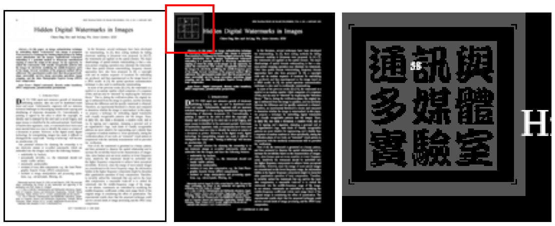
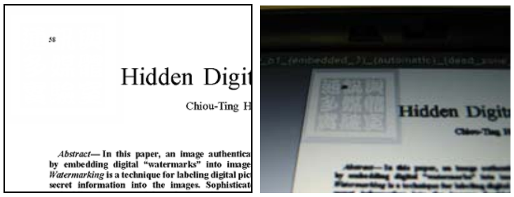


Fig. 9 A digital document marked with the proposed scheme and the extracted result out of the inversed version. Enlarged view of the marked area is also listed.



58

Hidden Digit

Chiou-Ting H

Abstract— In this paper, an image authentica by embedding digital "watermarks" into image *Watermarking* is a technique for labeling digital pic secret information into the images. Sophisticat

Fig. 10 Viewing the marked document displayed in the LCD monitor of an IBM Lenovo X60 laptop within and out of normal range of viewing angles

Furthermore, since different viewing angles related to LCD monitors also result in different contrast behavior, the hidden visible watermark patterns can be revealed by viewing the marked work from certain viewing angles. Due to the unavailability of detailed manufacturing parameters of certain LCD monitors, only empirical experimental results can be presented. Fig. 10 shows different views of the marked document displayed in the LCD monitor of a laptop. When the viewing angle is out of normal range for common users, the hidden watermark patterns appear clearly.

4. LIMITATIONS AND APPLICATIONS

There are two major limitations of this simple scheme: generality and security. Since the range of gray-levels that will be expanded is limited to dark values, for images or videos lacking dark areas occupying sufficient dimensions, the scheme based on gamma correction may not be easily applied. This problem can be easily alleviated by adopting global enhancement operations like histogram equalization or introducing additional extraction steps like the inversing operation as illustrated in the presdcribed document case.

As for the security aspect, since the chosen embedded areas are flat due to the adopted noise removal operation, an malicious attacker can remove the embedded message by automatic smoothing all flat areas in the digital content and still keeps good visual quality. However, for applications that convey additional useful metadata without security concerns, e.g. showing object annotations in an image or displaying the video owner's contact information but not prohibiting the playback, there is no need for any user to deliberately remove the hidden message. Furthermore, previous experimental results also show its potentials in actively detering illegal distribution of read-only documents like PDF file.

To sum up, the proposed scheme does provide cost-effective labeling function for visual contents being displayed in legacy displays lacking renewal capabilities. This simple scheme does surpass existing visible watermarking scheme in viewing quality and defeats curent invisible watermarking schemes since the need of deploying additional watermark extraction module is now totally removed.

5. CONCLUSIONS

The unseen visible watermarking methodology retains both advantages of visible and invisible watermarking schemes. Currently, we are working on devising similar schemes with better generality and higher security so that a wider application range could be achieved.

6. REFERENCES

[1] G. Braudaway, K.A. Magerlein, and F. Mintzer, "Protecting Publicly Available Images with a Visible Image Watermark, " Proceedings of the SPIE, International Conference on Electronic Imaging, San Jose, CA, February 1-2, 1996.

[2] J. Meng and S. F. Chang, "Embedding visible watermarks in the compressed domain," Proc. of ICIP 98.

[3] M.S. Kankanhalli, Rajmohan and J. R. Ramakrishnan, "Adaptive Visible Watermarking of Images," IEEE International Conference on Multimedia Computing and Systems, 1999.

[4] S. P. Mohanty, J. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking technique for images," Proc. of ICME 2000.

[5] I. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, Morgan Kaufmann Publishers, 2002.

[6] M. Wu and B. Liu, Multimedia Data Hiding, Springer-Verlag, 2003.

[7] C. S. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing, 2004.

[8] C. H. Huang and J. L. Wu, "Attacking Visible Watermarking Schemes," IEEE Transactions on Multimedia, Feb. 2004.