Digital Invisible Ink and its Applications in Steganography

Chun-Hsiang Huang
Dept. of CSIE, National Taiwan Univ.
886-2-23625336 ext 213
bh@cmlab.csie.ntu.edu.tw

Shang-Chih Chuang
Dept. of CSIE, National Taiwan Univ.
886-2-23625336 ext 505
peiz@cmlab.csie.ntu.edu.tw

Ja-Ling Wu
Dept. of CSIE, National Taiwan Univ.
886-2-23625336 ext 220
wjl@cmlab.csie.ntu.edu.tw

ABSTRACT

A novel information-hiding methodology denoted as digital invisible ink is introduced. The proposed approach is inspired by the invisible ink in the real world and can be regarded as an extension of the informed-embedding methodology. Messages hidden in digital contents using digital invisible ink cannot be correctly or clearly revealed unless certain pre-negotiated manipulations have been applied to the marked work. To facilitate such behavior, models and implementations based on both spread-spectrum and quantization-based watermarking approaches are investigated. Finally, benefits and limitations for applying digital invisible ink in common steganography systems and secret communications enabling plausible deniability are discussed.

Categories and Subject Descriptors

D.2.11 [**Software Engineering**]: Software Architectures – *information hiding.*

General Terms

Security

Keywords

Digital invisible ink, steganography, plausibly deniability, spread-spectrum watermarking, quantization-based watermarking

1. INTRODUCTION

Before the digital era, writing with invisible ink is one of the most renowned steganography skills [1]. Certain liquids like lemon juice have proved popular and effective since ancient times. In general, the ink is invisible during writing or soon thereafter. Later on, the hidden message may be developed (made visible) by different methods according to the type of adopted invisible ink. Development methods for different types of invisible inks include heating, applying chemical liquids or vapors upon the paper, viewing the paper under ultraviolet light, and so on. Figure1 shows an espionage scenario in which invisible ink is used. Note that, usually, the paper delivering secrets also carries some cover messages written with normal ink since sending a blank sheet of paper might arouse suspicion. The supervisor could not find any anomaly in the cover paper under common viewing conditions. When the intended receiver gets the cover paper, some pre-arranged manipulations, e.g. the heating operation shown in Figure 1, should be performed first to reveal the secret message. An introduction to invisible ink used by secret operation agents during World-War II can be found in [2].

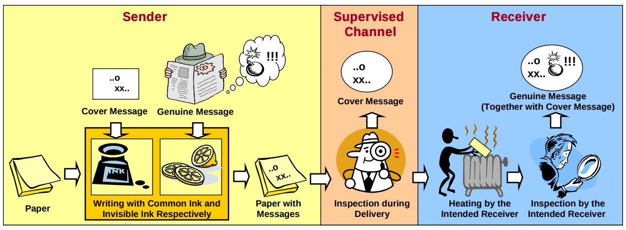

Sender
Supervised Channel
Receiver
..o xx..
!!!
Cover Message
Genuine Message
INK
Paper
Writing with Common Ink and Invisible Ink Respectively
..o xx..
Paper with Messages
..o xx..
Cover Message
Inspection during Delivery
..o xx.. !!!
Genuine Message (Together with Cover Message)
Heating by the Intended Receiver
Inspection by the Intended Receiver

Figure 1. A real-world espionage scenario using invisible ink

After entering the digital era, the attention paid to delivering secrets over physical objects or via human actions has been moved to hiding information in digital media. Delivering secret messages can be achieved by employing digital data-hiding schemes. Introduction to important digital data-hiding schemes and applications can be found in [3-5].

In this paper, a digital data-hiding methodology analogous to the invisible ink in the real world, named as digital-invisible-ink (DII) data hiding, is proposed. Similar to the real-world steganography scenario based on invisible ink, messages hidden with DII schemes will never be correctly or clearly extracted unless (one or more) pre-negotiated manipulations have been performed on the marked work in the receiving end. Potential benefits and limitations achieved by applying DII schemes in common steganography scenarios and plausibly deniable steganography schemes are illustrated. Definitions and details about plausible deniability of steganography schemes will be illustrated soon.

This paper is organized as follows. Section 2 introduces principles and models of digital invisible ink. Models based on important blind-detection data-hiding schemes, including spread-spectrum approaches and quantization-based techniques, are also illustrated. Section 3 addresses the pros and cons of building general steganography schemes over DII techniques. Section 4 discusses the plausible deniability of steganography systems and a novel implementation based on DII data-hiding. Conclusions and future works are provided in Section 5.

2. BASICS OF DIGITAL INVISIBLE INK

2.1 Characteristics of Digital Invisible Ink

Important characteristics that a DII data-hiding scheme shall possess are listed:

(1) Only when the cover work has undergone certain pre-negotiated manipulations will the hidden messages in the marked work produced by DII data-hiding schemes be correctly or clearly extracted.

(2) To extract the genuine secrets, the intended receiver will deliberately and seriously distort the marked work. But note that for the channel supervisor or non-intended users, the

MM&Sec'06, September 26–27, 2006, Geneva, Switzerland.

marked work is still perceptually similar to the original cover work.

(3) In certain applications of DII, the payloads extracted by the intended receiver will consist of both a cover message and a genuine message. The intended receiver can easily distinguish between the cover message and the genuine message.

To facilitate the characteristics listed above, DII models based on both blind-detection spread-spectrum watermarking schemes and quantization-based methods are illustrated in sections 2.2 and 2.3.

2.2 DII Models Based on Blind-Detection Spread-Spectrum Schemes

Spread-spectrum watermarking techniques, e.g. those introduced in [6, 7], are correlation-based schemes. The process of embedding one payload bit using spread-spectrum schemes can be formulated as:

$$c_{wn}=c_o+n+a \cdot b \cdot w \qquad (1)$$

where c_o is the original cover work, c_{wn} is the distorted and marked work, n is the additive noise caused by malicious attacks or media processing. b is the payload bit represented as 1 or -1, a is the weighting factor deciding the embedding energy of watermark signals (which can be determined according to perceptual models or specific embedding rules), and w is the predefined watermark vector (often a pseudo-random chip sequence in common spread-spectrum schemes).

In order to identify whether the suspected work c_s has been marked, the correlation value between c_s and w is calculated. If the correlation value is larger than a positive threshold value T, c_s can be regarded as hidden with a payload bit of 1 (i.e., $b=1$). On the contrary, if the correlation value is less than a negative threshold value $-T$, it means that c_s is carrying a payload bit of -1.

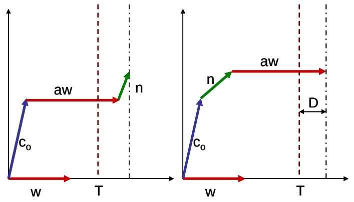
Figure 2(a) shows the geometric model illustrating the prescribed embedding/detection processes. c_{wn}, c_o, n and w are often regarded as vectors in a multi-dimensional hyperspace. With adequately normalized w, the obtained correlation value is in fact the projection of c_s in the direction of w.

In an informed-embedding case, i.e. assume the effects of the cover work c_o and n are known, the weighting factor a can be adjusted to guarantee a successful detection such that:

$$w \cdot c_o+w \cdot n+a \cdot w^2 > T+D \qquad (2)$$

where D is a guaranteed amount over the threshold value T. Figure 2(b) demonstrates this situation. Note that though the noise vector n is directly connected to c_o in Figure 2(b) and subsequent figures, such a representation is purely for the ease of illustration. Operations causing distortions are actually performed on the marked work, rather than on the cover work directly.

In general-purpose watermarking applications, exactly grasping all kinds of possible attacks is far from reality. However, it is a different story in steganography applications since all possible distortions are predictable or even controllable. If both the host-interference caused by c_o and the distortion due to the sender-imposed lossy compression (simulated by n) are predictable, detection results can be fully controlled. The DII data-hiding schemes proposed in this paper are in fact extensions of such an informed-embedding methodology. In the following discussions about DII spread-spectrum scheme, an informed-embedding model incorporating with an additional noise vector k due to pre-negotiated manipulations will be introduced, and some constraints on this system model will be exploited to facilitate the invisible-ink specific behavior. Without loss of generality, the noise denoted by n will be omitted in the following discussions.

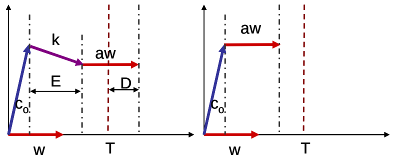


(a) (b)

Figure 2. Geometric models of spread-spectrum watermarking: (a) the general case and (b) the informed-embedding case

In a DII data-hiding scheme, the most essential principle is that the existence of a noise k caused by certain pre-negotiated manipulations is necessary for the successful detection of the payload bit, as illustrated in Figure 3. In Figure 3(a), a detection result of $b=1$ is guaranteed by employing informed-embedding approach similar to Eqn. (2). The only difference is that, now, the effect of k is considered instead of n. If k is not applied to the marked content, as the case shown in Figure 3(b), a different embedding result ($b=-1$) will be obtained.

When performing general spread-spectrum watermark embedding and detection, the desired situation illustrated in Figure 3 does not always occur. According to the aforementioned geometric model, some requirements must be satisfied. First, the angle between the noise k and the watermark vector w must be within the range of $[90^o, -90^o]$. In other words, the noise vector k must contribute positively to the extraction result. Furthermore, the magnitude that the vector k projects on the direction of w, denoted as E in Figure 3(a), must be larger than the guaranteed amount D over the detection threshold T. That is, k must contribute significantly to the detection result. If the two requirements are not satisfied, the DII data hiding scheme “fails” (i.e. the extracted payload bit is the same no matter whether the pre-negotiated manipulations are applied to the marked work or not).



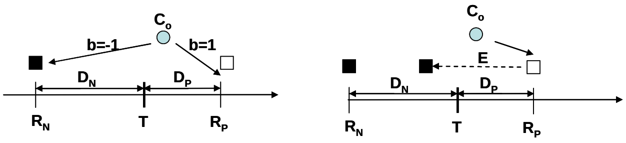
(a) (b)

Figure 3. In a DII scheme, detection results rely on whether pre-negotiate manipulations exist (a) or not (b).

2.3 DII Models Based on Quantization Watermarking Schemes

Quantization watermarking, as introduced in [8, 9], is another important class of blind-detection data-hiding schemes. In quantization watermarking methods, payload bits are embedded by quantizing components of the cover work according to some predefined quantizer. Without loss of generality, As shown in

Figure 4(a), a chosen component of the cover work c_o will be quantized to a reconstruction point larger (R_P) or smaller (R_N) than the predefined decision threshold T, depending on whether the watermark bit is positive ($b=1$) or negative ($b=-1$). During payload extraction, whether a watermark bit is 1 or -1 can be easily read out by comparing corresponding component of the marked work with the decision threshold T. Note that the quantization step represented as (D_P+D_N) is often determined by human perceptual models in order to satisfy the fidelity requirement or even key-dependent for the concerns in system security. For the ease of illustration, we only discuss the simplest case where a watermark bit b is embedded using a non-uniform single-bit quantizer. However, the DII principles can be applied to more generalized schemes with careful adjustments.



(a) (b)

Figure 4. (a) Watermarking using a single-bit quantizer. (b) The DII-based scheme where the case of *b=-1*, is illustrated.

Figure 4(b) illustrates the model of DII data hiding schemes based on single-bit quantization watermarking. The original watermarking procedures are modified to satisfy the essential principle of DII data hiding – applying specific manipulations to the marked work is necessary for the successful detection of payload bits. Assume that the current payload bit b is -1. Since the extractor must output a different extraction result (as if $b=1$) as long as the required media manipulation is not performed, c_o shall be firstly quantized to the wrong reconstruction point (R_P). Then, the required manipulation must distort the marked work along the direction from the wrong reconstruction point to the correct one. This is the corresponding positive-contribution requirement of quantization-based DII data-hiding scheme. Furthermore, since the manipulated content should indicate the intended extraction result (i.e., $b=-1$), the magnitude of distortion caused by the manipulation on the quantized value, represented as E in Figure 4(b), must be larger than D_P. This is the significant contribution requirement of DII quantization data hiding. Similarly, the case of embedding $b=1$ can be easily worked out.

3. GENERAL STEGANOGRAPHY SYSTEMS BASED ON DII

The most straightforward application of DII is building steganography systems upon it, as shown in Figure 5. The most apparent characteristic of a DII-based steganography system is the existence of pre-negotiated manipulations in the receiving end. Here we assume that the manipulations are provided by common media-processing tools available in the receiver's environment to avoid deploying additional steganography-related modules. .

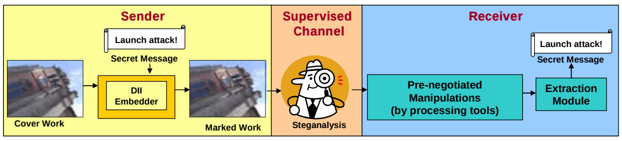


Figure 5. Architecture of a DII-based steganography system

The prescribed DII spread-spectrum model is utilized to implement this steganography system. Here, an iterative informed-embedding process, as demonstrated in Figure 6, is employed. More specifically, the weighting factor of each payload bit, denoted as a in Eqn. (1), is now gradually increased until the corresponding payload bit can be extracted after the marked work underwent the pre-negotiated manipulations. Throughout all the iterations, the extraction result for each embedded payload bit against the pre-negotiated attacks will be checked, but the marked work being delivered at last is not actually distorted. As long as a certain payload bit is successfully embedded, the increase of the weighting factor corresponding to that payload bit stops. The iterative process stops when all payload bits can be successfully extracted against the pre-negotiated manipulation, i.e. the minimal watermarking energy required to facilitate a 100% extraction against the pre-negotiated attacks have been determined. Since the interval of the progressive increase is small and the increase for each payload bit stops immediately when the corresponding payload bit is successfully embedded, the amount of correlation value over the detection threshold, denoted as D in the prescribed DII spread-spectrum watermarking model, will be small. In other words, all the payload bits are embedded weakly, but all of them can be extracted when the pre-negotiated manipulations are performed on the marked work before extraction is performed.

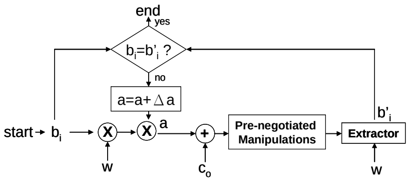
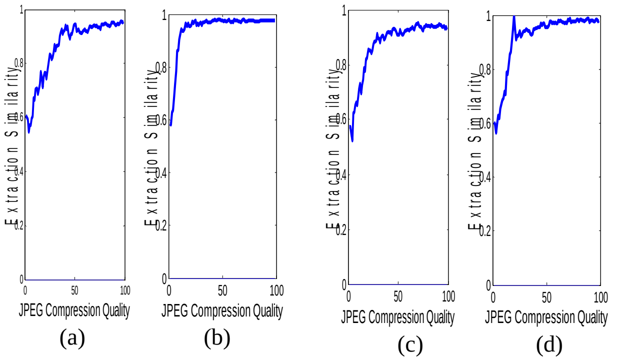


Figure 6. The iterative informed-embedding scheme for the DII spread-spectrum data-hiding system

Does this iterative informed-embedding scheme satisfy the two requirements of DII spread-spectrum data hiding? For the positive-contribution requirement, since the predefined watermark vector is pseudo-randomly distributed, there are always payload bits whose corresponding angle between the noise resulting from the pre-negotiated manipulations and the predefined watermark sequence lies within the range of [90^o, -90^o]. On the contrary, it also means that the first condition is only satisfied in a relaxed manner since this condition does not hold for all payload bits. As for the second condition, since the iterative watermarking approach produces weakly embedded works, the magnitude of correlation value over the detection threshold (denoted as D) is consequently small. Therefore, as long as the pre-negotiated manipulations cause significant distortions along the direction of watermark vector, the second condition can be satisfied.

However, since the noise vector tends to be near-orthogonal to the pseudo-randomly distributed watermark vector, the projection of the noise vector in the direction of watermark vector may be insignificant for most payload bits. These deficiencies inherently impose a limit on the types of payload bits – index values indicating reference messages or pointing to certain hash items will be more adequate for this implementation than human-recognizable patterns. This is because, when an attacker successfully figures out media manipulations close to the pre-negotiated one and performs them to the marked work before extraction, a message not exactly the same as the genuine one but very similar to it may be extracted. Such a message represents subtly different semantic meanings when the payload bits indicate uncorrelated index values, but it will reveal significant information that the genuine message contains when the payload bits represent recognizable patterns. Fortunately, it is not very easy for an attacker to guess out the exact combination of manipulations since the key space is moderately large. Exploitations about the size of key space formed by potential manipulations will be given soon.

Figure 7 shows the extraction results using the 512x512 Lena image and a 250-bit message. Each payload bit is hidden with a pseudo-random chip sequence of 100 bits. The interval Δa used to iteratively adjust the weighting factor of watermarks is set to 0.1, and the finally embedded image has a PSNR value of 39.20 dB. Significant pre-negotiated distortions, including histogram equalization, blurring using 7x7 filters and JPEG compression with quality factor being set to 20, are applied in turn on the marked work based on the prescribed informed-embedding scheme. As we expected, only the payloads hidden in the marked image compressed with exactly the same manipulations can be extracted.



(a) (b) (c) (d)

Figure 7. Extraction results for the DII spread-spectrum data-hiding system where the pre-negotiated manipulations consist of histogram equalization, blurring and significant JPEG compression (Q=20) in turn. (a) and (b) show extraction results for cases where histogram equalization and blurring are missing respectively. (c) is the extraction results after performing all the three manipulations, but the order is wrong. (d) is the extraction result when all the three manipulations are performed in correct order.

The major advantage of DII-based steganography system over existing security solutions lies in that: the genuine meaning of the hidden message can be protected without deploying additional security-related modules like ciphers or authentication modules. Therefore, when the supervisor detects the secret communication, even the watermark extractor is available to him; the genuine message is still safe from being interpretation. The supervisor has no clues about how to extract the real message. On the contrary, the existence of cipher modules or prompts for password/key input required for the protection of delivered messages in conventional schemes will surely lead to further cryptanalysis attack.

Though the prescribed advantage is of practical values, modern security analysis assumes that the attacker understands the methods to hide and protect the message. In other words, the entire security of a particular method must lie in the selection of keys and not in proprietary nature of adopted methods. From this viewpoint, the involved pre-negotiated manipulations can be viewed as a key in a large key space. For example, assume that there are m possible manipulations provided by a common content processing tool and each type of manipulations has n_i ($1 \leq i \leq m$) adjustable parameter settings. If only k manipulations ($k<m$) are adopted to form an extraction key due to the convenience of human memorization or key management, the total number of keys in the key space formed by the combination of all possible manipulations will be $(m! \cdot \prod_{m} n_i)$.If the attacker successfully figures out the value of k, an exhaustive attack will require $(P_k^m \cdot \prod_{k} n_i)$operations. In a conservative hypothesis where $m=20$, $k=5$ and $n_i=(1000, 100, 10, 10, 1)$, the expected cost of an exhaustive search will need about 2^{43} trials. That is, moderate security of the delivered message can be provided without installing any additional security-specific modules. Note that there many existing media operations whose parameters are real-valued and may lead to tremendous key spaces.

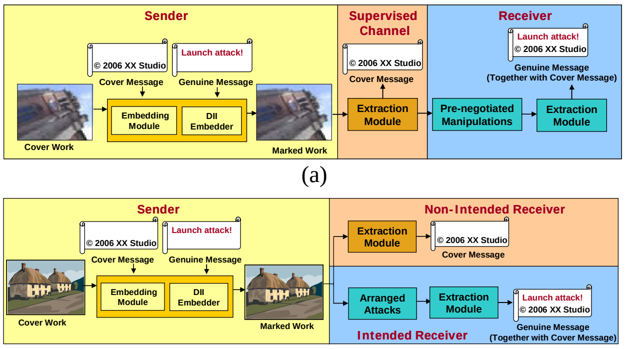
However, the proposed DII spread-spectrum implementation of steganography system still suffers from other drawbacks. In additional to the inherent deficiencies mentioned above, due to the pseudo-randomness of spread-spectrum schemes, the extraction result corresponding to each payload bit cannot be controlled at will. Furthermore, due to the weak-embedding nature, the scheme fails when the supervisor introduces slight modifications to the received works. Finally, the iterative embedding procedure is always time consuming.

4. THE DII-BASED PLAUSIBLY DENIABLE STEGANOGRAPHY SYSTEM

When compared with the spread-spectrum counterpart, quantization-based DII data-hiding model is relatively powerful. If the embedding domain and the pre-negotiated manipulations are chosen adequately, the extraction result corresponding to each payload bit against pre-negotiated manipulations can be accurately controlled. Furthermore, since the payload bits need not to be weakly embedded, robustness against slight distortions made by the supervisor can be provided. In order to demonstrate the strength of quantization-based DII data hiding, a plausibly deniable steganography system is illustrated.

In the literature of steganography, plausible deniability means the capability to deliver some genuine message under the cover of other innocuous messages. When the presence of hidden information is detected and the sender of the cover medium is forced to reveal the secret communication, he can simply turn over another innocuous message and claim that no other information is hidden. Plausible deniability is often achieved by hiding multiple messages into non-overlapping components of the carrier medium. And at the receiving end, receiving keys determine the message that will be extracted. Here, a novel steganography system enabling plausible deniability based on DII quantization watermarking is proposed.

Now, additional to the genuine message being embedded with the DII embedder, another cover message is also embedded into the cover work using a common embedding module. Note that the same extraction module is assumed to be available to both the channel supervisor and the receiver, and the sender of marked work may willingly announce the algorithm details of the cover data-hiding scheme and the existence of the cover message. Therefore, when steganalysis tools employed by the channel supervisor detects that the marked work carries certain information, the cover message will be readily extracted in order to hide the very existence of the genuine message. However, after the receiver performs the pre-negotiated manipulations on the received marked work, the genuine message will be extracted together with the cover message. The scheme shown in Figure 8(a) is in fact an analogy to the real-world steganography scenario shown in Figure 1. Figure 8(b) is another variant where identical copies of a marked work will be distributed. For example, DVD marked with DRM-related messages or supplemental metadata naturally fits this type. In this case, security-threatening messages can be distributed under the cover of legal messages and being intercepted by more than one intended receivers simultaneously.



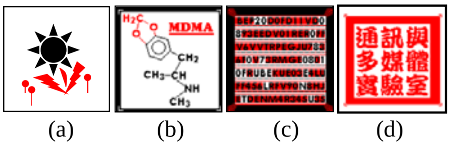
(a)

(b)

Figure 8. Architectures of (a) a typical plausibly deniable steganography system and (b) the system where multiple copies of marked works may be distributed simultaneously

Different from the spread-spectrum scheme, the payload bits now form semantically meaningful patterns. Figure 9 shows some sample watermark images consisting of both cover messages and genuine messages. Cover messages are represented as black pixels in each figure and the genuine one are shown in red. In Figure 9(a), the semantic meaning of the watermark image (originally a sun pattern) changes (now a flower) after the genuine message is revealed. Fig 9(b) illustrates the danger that an illegal message (the formula of MDMA, an addictive drug) may be disguised as an insensitive message (the formula of Methamphetamine, a valueless chemical compound). Figure 9(c) demonstrates that the extraction of genuine message may eliminate unnecessary information so that a meaningful message (indicating a time/location pair in this case) can be revealed out of seemingly random patterns. To the extreme, the cover watermark may be a null pattern and all information capacity is reserved for the genuine watermark, such as the one shown in Figure 9(d).

Figure 10 illustrates details of the corresponding implementation. Assume that during the process of payload extraction, if the value being read out is less than the detection threshold, a black pixel will be displayed. Otherwise, a white pixel is shown. Payload bits representing the cover message and white spaces in the watermark are embedded with a normal quantization watermarking scheme. As for payload bits indicating the genuine message, the effect caused by some pre-negotiated manipulation, denoted as *E*, is considered in the embedding module. To be more specific, different versions of marked works are generated based on iteratively-increasing *D* values for all payload bits and the same pre-negotiated manipulations are applied on the marked work to test what the extraction results are. The value of *D* for individual payload bit will be set as the maximal value that the pre-negotiated manipulation will "flip" the extracted pixel from white to black – i.e. the desired invisible-ink like behavior.



(a) (b) (c) (d)

Figure 9. Examples of watermark patterns consisting of both cover messages and genuine messages

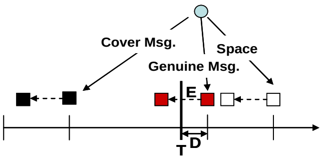
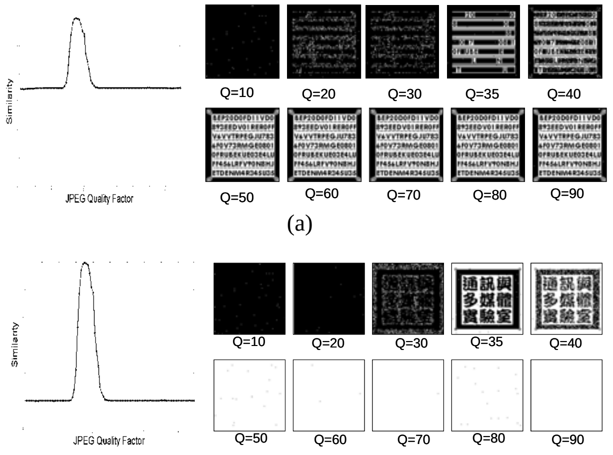


Figure 10. The quantization-based DII model facilitating the plausibly deniable steganography system

Both the cover message and the genuine message are embedded by altering the AC coefficients in the DCT blocks of the test images. According to the analysis provided by [10], common image manipulations can be classified into two classes: the first class reduces the magnitudes of AC coefficients and the latter one increases the magnitudes of AC coefficients. Operations like JPEG compression or blurring belongs to the first class while edge enhancements and adding noises are classified as the latter one. In this experiment, JPEG compression of certain quality setting is chosen to be the pre-negotiated attack. The value of the quantized and scaled DC coefficient in each block is chosen to be the detection threshold due to the invariance of its magnitude against most image manipulations. For the ease of implementation, the cover messages are embedded by modifying corresponding AC coefficients to a fixed value smaller than the detection threshold. The reconstruction points for pixels representing genuine messages are determined by the prescribed iterative informed-embedding procedure, denoted as *T+D*. The reconstruction points for pixels in the white space are set as *T+D+⊿*, where ⊿ is a small value (⊿=4 in the following experiments) to facilitate the desired phenomenon that the whole watermark image will be totally black when the attack performed by an attacker is stronger than the pre-negotiated attack.

Figure 11 shows the extraction results using the 128x128 binary watermark images shown in Figures 9(c) and 9(d) respectively. The watermarks are embedded into the 512x512 Lena image. According to the dimension ratio between watermarks and cover works, 4 watermark bits will be embedded into each 8x8 DCT block by altering 4 predefined AC coefficients. Both statistical and visual extraction results obtained from different versions of the marked image created by applying different degrees of JPEG compression (quality factors ranging from 99 to 1) are illustrated. As expected, messages indicating the time/location information and the Chinese characters are not visible until the manipulations very close to the pre-negotiated one is performed. Note that though the pre-negotiated attack is assumed to be JPEG compression with quality setting of 40, the best extraction result occurs when JPEG compression of quality 35 is applied to the marked work. This is a nature result since the iterative informed-embedding procedure used to determine the most-adequate watermark energy is only approximated due to practical computation resources. In fact, the sender may just select the operation parameter generating best extraction performance as the pre-negotiated manipulation and deliver the marked work to the intended receiver to achieve best extraction performance.

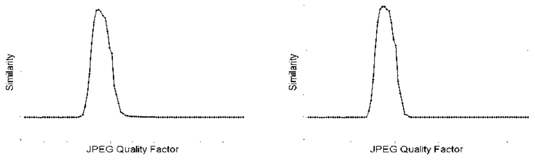


(a)

(b)

Figure 11. Statistical and visual views of extraction results out of marked works undergoing different JPEG compressions

Figure 12 shows the robustness of the proposed scheme when the "active-warden" case in the famous "Prison's problem" [11] is assumed. Before the receiver performs the pre-negotiated manipulation, the supervisor adds white Gaussian noises (with SNR 25 and 40 respectively) to the marked work. According to the results, the proposed scheme can survive the attacks imposed by the supervisor.



(a) (b)

Figure 12. Extraction results against the noise-adding attack: (a) SNR=25dB and (b) SNR=40dB

In the plausibly deniable scheme, employing the DII marking module is no longer the details that the sender shall reveal when the security of cover data-hiding applications is analyzed. In fact, the sender of illegal messages will just actively announce the algorithm details of the cover data-hiding system. Since all the required alternations made according to embedding rules of the cover watermarking system may be complicated or even content/key dependent, the channel supervisor cannot easily tell the difference between the deniable marked work and the one purely generated using a cover watermarking system. Even the supervisor knows that the sender may employ the DII scheme; the proposed DII-based steganography system enabling plausible deniability still matches or surpasses the conventional multiple-watermark approaches against certain steganalyses. Details about the steganalysis under different constraint are not listed due to the paper length.

5. CONCLUSIONS AND FUTURE WORKS

In this paper, a novel data-hiding methodology behaves like the invisible ink in the real world is proposed. Steganography systems based on the invisible-ink like methodology, including the general steganography system and the plausibly deniable schemes, are demonstrated. The proposed approaches can be viewed as extensions of existing informed-embedding approach. It would be our future work to discover more interesting and important applications of digital-invisible-ink data-hiding.

6. ACKNOWLEDGEMENT

This work is supported by NSC95-2752-E-002-006-PAE, National Science Council, Taiwan.

7. REFERENCES

[1] Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 2nd Edition, Chapter 1, Springer, 2000

[2] Rigden, D. *SOE Syllabus: Lessons in Ungentlemanly Warfare, World War II*, Gardeners Books, 2004

[3] Katzenbeisser, S. and Petitcolas, F.A.P. *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Publishers , 2000

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

[5] Furht, B. and Kirovski, D. *Multimedia Security Handbook*, CRC Press, 2005

[6] Cox, I. J., Kilian, J., Leighton, T.and Shamoon, T. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, December 1997

[7] Marvar, H. S. and Florencio, A. F. "Improved Spread Spectrum: A New Modulation Technique for Robust Watermarking," IEEE Transactions on Signal Processing, vol. 51, no. 4, April 2003

[8] Swanson, M. D., Zhu B. and Tewfik, A. h. "Data hiding for video-in-video," Proceedings of International Conference on Image Processing, 1997

[9] Chen B. and Wornell F. "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," IEEE Transactions on Information Theory, vol. 47, pp1423-1443, May 2001

[10] Lu, C. S., Huang, S. K., Sze, C. J. and Liao, H. Y., "Cocktail Watermarking for Digital Image Protection," IEEE Transactions on Multimedia, vol. 2, No. 1, December 2000

[11] Simmons, G. J. "The prisoner's problem and the subliminal channel," Proceedings of CRYPTO '83, 1984