ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7673-7677

Secure Data hiding in Multi-level using Digital Invisible Ink based on Spread Spectrum Watermarking

T. Ezhil Sindhu, Guide - P. Sripriya
School of Computing Sciences, Vel's University,
Pallavaram, Chennai-600 117.
gncezhil@gmail.com
Assistant Professor School of Computing Sciences, Vel's University,
Pallavaram, Chennai-600 117
sripriya@velsuniv.org

ABSTRACT

Watermarking schemes has been proposed as a protection of data or in other words preventing illegal copying of data, but still this security is yet to be well defined. The approach of watermarking is sometimes considered too theoretical. Hence, a whole new casting of watermark security is proposed, called the effective key length. Through this approach it would be a nightmare for any hacker who tries to find access to the original data and also digital watermarking technique is used as the embedding process for data hiding, apart from using security keys, because finding the key should not be the best mode in breaking the system therefore multiple level of security is proposed in this paper. The analysis paves way to the spread spectrum scheme to initiate the theoretical and practical application of the effective key length. For data hiding, ISS (Improved Spread Spectrum) offers a better security and robustness and it is adopted to implement digital invisible ink method.

Index terms - Watermarking, Spread Spectrum, Digital Invisible Ink, Multi-Level Security.

1. INTRODUCTION

Looking back in olden days certain measures involving data hiding or secretly sent/received were found in many mines of human civilization. Before the current digital period steganographic skills. These techniques fall into two main branches, linguistic steganography and technical steganography. Linguistic steganography consists of two classes of methods, delivery of secret messages via an open code where prior agreements about the true meaning of apparently risk-free phrases, indication or terminology must be negotiated in progress, as well as semagrams that secrets are spoken in the form of visible but small graphic details in a picture or writing. Plausible Deniability in Steganography is used as a vital turning point in this project.

A. The real world Invisible Ink

In technical steganography, writing with invisible ink is the most celebrated ability. Well known methods like use of liquids such as lemon juice or milk have proven as the natural invisible ink and hence it is popular and effective since prehistoric times. Broadly, invisible ink is a essence used in steganographic schemes so that secret messages can be undetectably written on papers. The ink is invisible subsequently or sometimes even during writing. Afterward the hidden messages can be made visible by various methods according to the type of invisible ink used. For example, secrets written with diluted acid liquids on paper can be found by heating the same. Other Development methods or types of invisible inks embrace applying chemical liquids or vapors over the paper, viewing the paper under ultraviolet light, and so on. Fig. 1.1 shows a conventional surveillance scenario in which invisible ink is used. If a sender wants to send some secret message to a certain receiver over a controlled or watched channel, he can write that secret messages on the paper using some liquid which we said above. It is also important to be noted that the paper also carries some wrapped messages written with normal ink which is visible to plain eyes. This is because to avoid doubts. Sending a blank sheet of paper might provoke suspicions. Hence it is impossible to the supervisor of the channel to find any abnormality in the paper under general viewing conditions. In the other hand, when the planned receiver receives the paper, through certain prenegotiated manipulations, e.g., by heating as shown in Fig. 1.1, should be performed in order to reveal the secret message/messages. A common example of invisible ink used by secret operation agents during World-War II can be found in this figure.

Certain characteristics of invisible-ink based on steganography skills in the real world are collectively given as follows:

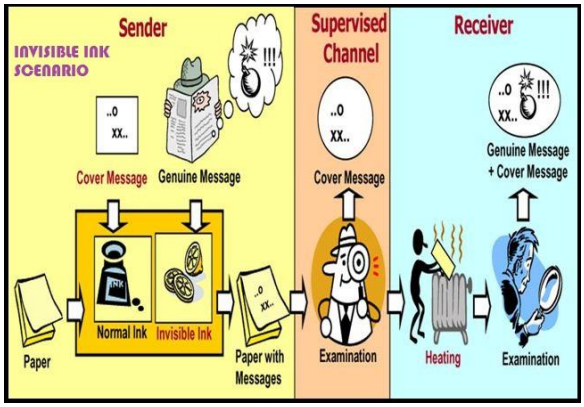

Fig. 1.1 **Real-world scenario using the invisible ink.**

a) Manipulations- Prenegotiated manipulations are crucial steps for the correct extraction of authentic secrets. When certain types of invisible inks are used, the equivalent development methods must be performed by the receiver end on the received paper to extract the hidden message/messages.

b)Results after manipulation- the received paper may be seriously warped due to the matching prenegotiated manipulations, for example the paper may become lumpy after heating. But still extracting the genuine messages will be the real goal, so the visual quality of the paper after the prenegotiated manipulation is often out of anxiety.

c) Cover messages- They play an significant role as smokescreen during delivery of genuine messages. Nevertheless, spaces where left on the paper where still genuine secrets can be invisibly written, because it is usual that a hand-written or printed documents always have blank spaces between words and for the ease of reading.

B. Steganography against Steganalysis

After entering the digital era, digital medias like images or audio clips serve as good cover up objects for carrying secret messages. Therefore, digital data-hiding techniques are adopted to implement steganography systems. In a data-hiding structure, the sender embeds some messages, which can be also symbolized as watermarks for some other applications, into the cover work for generating a perceptually acceptable stegowork. In the receiving end, the receiver extracts the messages from the received stego work. In Digital steganography, a) fidelity- the visual quality of the stego work and b) capacity - the maximally allowable message length are most important implementation measures. On the divergent side, steganalysis is the practice of acting aggressively on the steganographic schemes by either destroying, extracting or detecting the hidden messages. Watchers of the communication channels prefer to implement sufficient steganalysis tools to prevent unexpected communications through the transmitted content. But in general, deciding whether a cover work carries hidden messages is a difficult task. When the channel supervisor has the right to cease any doubtful communication, an accurate steganography detection module suffices for all his needs. Also that the same watcher of the channel may waste his time on applying the same module on potentially unwanted contents, because as said above detecting a message just whether it carries secret messages or not is very difficult to plain eyes. In such a situation, the supervisor should invent multipurpose and effective noises which can be applied to all delivered contents, while designers of steganography systems should consider robustness against potential misrepresentations, as well as prescribed fidelity and capacity requirements. in addition, the watcher of the channel may try to overhear/spy and understand(read between the lines) the secret messages. As a result, cipher (codes, symbols or secret messages) are often applied to the messages sent by the sender to prevent unauthorized reading by unofficial receivers from reading the secret message. Hence these type of covert communications are defined as "the prisoners' problems" and the channel supervisor is therefore denoted as a warden. From the definitions in particular a channel supervisor who can only spy and can do nothing on the communication channels is called as "passive" warden. Conversely, the watcher or supervisor who has the privilege to slightly modify the content which is sent from the sender to the receiver is called as an "active" warden. This paper, focuses more on the passive-warden scenario. Detailed discussions about data-hiding systems can be found In the literature of digital steganography.

C. Plausible Deniability

Plausible deniability is originally a term used in politics. It means the creation of loose and comfortable chains of commands in government, which allow notorious instructions given by high-ranking officials to be denied if these instructions become public. In cryptography, depending on the key used deniable encryption agree to encrypt a message to be decrypted to various meaningful and significant plaintexts i.e information, this way it allows the sender to have plausible deniability. Even if an illegal watcher threatens the sender or the receiver to give up his encryption key it'll show only an alternative image. But in strictly-defined modern cryptography, it is almost impossible to design a cipher text that can be decrypted to several different meaningful plaintexts. In the literature of steganography, plausible deniability means the capability to deliver some genuine message under the cover of other innocent messages. So even if the illegal hacker founds the existence of some hidden messages and compel the sender to reveal the secret message, he can simply turn in one innocuous message and maintain as if that other than this there is no other information is hidden. Hence, Plausible deniability has been proposed to enhance the security of steganography systems and defend current steganalysis. In this paper, instead of diving into details of various plausibly deniable schemes, some high-level discussions about implementing plausibly deniable steganographic systems based on generic watermarking techniques, and the comparisons with the proposed system are provided in the below sections.

2. MOTIVATION OF THE PROJECT

Though security of datas are approached in different ways through super effective key length and watermarking schemes still security has a loop hole and fails in certain factors, it is because on one side when new techniques are found for data security, on the other side hackers are developing an alternative technique to decipher the data on a communication channel. So there is always like when we start building a strong wall for data security illegal tries to break the wall in their own way. Hence relying only on the security key is no longer seems to be helping. That's the reason this project is proposed to take a neat diversion from the dependency of the key to the spread spectrum and invisible ink methods. Again these methods are already proposed but here we are trying to apply these techniques in multiple level so that even the security key is hacked the hacker can have access only to the watermarked image and not the hidden in the resultant image. Hence, only the authorized sender and receiver only can read the original message which motivated this project.

3. LITERATURE SURVEY

The "Digital" Invisible Ink

In this paper, steganography classification based on the "digital" adaptation of invisible ink, is represented as digital invisible ink (DII) is projected. Since we try to put into action a digital version of such invisible-ink system based on existing watermarking schemes, corresponding distinctiveness of invisible ink shall be satisfactorily employed.

1. Hidden messages in a communication channel can be extracted only when the stego work experiences certain prenegotiated manipulations. In consequent discussions, media processing procedures that always cause deformation to the stego work in the prenegotiated manipulations. It should be noted that in our digital implementations, the types and extent of manipulations are carefully controlled and viewed as keys to achieve better security.

2. Only the authorized receiver will know how to extract the secret message/messages intentionally and seriously figure out the watermarked work. But for the channel's unauthorized watcher or non-intended users, the watermarked work is still perceptually similar to the original cover work.

3. In the case of plausibly deniable steganography, the data extracted by the authorized receiver will consist of both a cover message and a genuine message. But still the authorized receiver can easily differentiate between the cover message and the genuine message. because he can also dig out the hidden data i.e., the cover message solely. In some interesting cases, we will show that the cover message can be formulate to help in understanding the hidden messages.

Note that the idea of digital invisible ink data hiding is firstly revealed in and then briefly oppressed in by the authors. In this paper, we thoroughly describe the, implementations, experimental results and motivation of digital-invisible-ink data hiding. The spread-spectrum watermarking and the quantization-based watermarking, which is known as the two major watermarking schemes are embraced to employ the digital invisible ink and respectively discussed further. In addition to this applications, application details, inherent limitations, experimental details of each schemes and the superiority of the digital-invisible-ink methodology are also discussed.

SPREAD- SPECTRUM WATERMARKING ALONG WITH DIGITAL INVISIBLE INK (SS-DII)

It is well known that Spread-spectrum watermarking techniques for all kinds of media, are the well-known data-hiding schemes. Here in this section we can see the modification in the fundamental spread-spectrum approaches to reproduce the invisible-ink steganography in the real-world.

A. Conventional Spread-Spectrum Watermarking

Spread-spectrum watermarking techniques are correlation based schemes. The process of embedding a single message bit using spread-spectrum watermarking schemes and then applying some manipulations to the stego work can be formulated as follows:

$$\hat{c} = \acute{c} + n = c + a \,.\, b \,.w + n$$

where is a vector consisting of components in the cover work, is the corresponding vector in the stego work, and is the c' vector in the distorted stego work c^. Moreover, a is the weighting factor deciding the embedding energy of watermark signals (which is often determined according to perceptual models or heuristic rules).b is the message bit represented as -1 or 1 , and w is the predefined watermark vector, often a pseudo-random chip sequence in common spread-spectrum schemes. Finally,n is the additive noise vector caused by malicious attacks or media processing on the stego work.

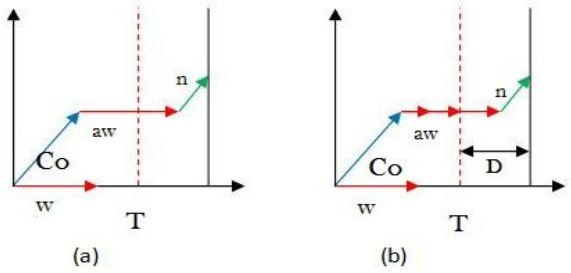

Fig. 3.1 Geometric models of spread-spectrum watermarking: (a) general case and (b) informed-embedding case.

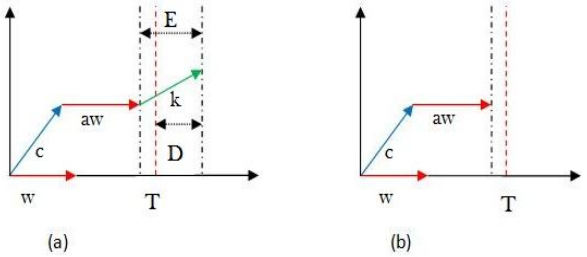

Fig. 3.2 In a DII data-hiding scheme, the detection result depends on whether the prenegotiate manipulations exist (a) or not (b).

Assume that is marked and distorted (i.e., is equal to), the extraction process can be described by

$$w.\tilde{c}=w.c+a.b.w^2+w.n \qquad (2)$$

Both w.c and w.n are close to zero due to the noise-like characteristic of w. If the correlation value $(w.\tilde{c})$ is larger than a positive threshold value T,$\tilde{c}$ can be regarded as hidden with a message 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 $\tilde{c}$ is carrying a message bit of -1. If we simply choose the value of T to be 0, the message bit can be determined according to whether the correlation value is positive or negative. Fig. 2(a) shows the geometric model illustrating the prescribed embedding and detection processes, c, n and w are often regarded as vectors in a multidimensional hyperspace. With an adequately normalized w, the obtained correlation value is in fact the projection of $\hat{c}$ along the direction of w. In an informed-embedding case, i.e., assume the effects of the cover work c and n are known, the weighting factor a can be adjusted to guarantee a successful detection such that:

$$w.c+a.b.w^2+w.n > T+D \qquad (3)$$

where D is a predefined value over the threshold value T . Fig.2(b) illustrates this scenario.

In general-purpose watermarking applications, exactly grasping all possibilities is far from reality. However, it is a totally different story in passive-warden steganography applications where the channel supervisor will not introduce any additional distortions. If both the host-interference caused by and the distortions due to the sender-imposed lossy compression are predictable, detection results can be fully controlled.

The SS-DII System

To implement a digital-invisible-ink data-hiding system using spread-spectrum watermarking, an iterative informed-embedding approach is proposed. Note that, in our implementation, some prenegotiated manipulations, such as lossy compression or content

processing, are incorporated to distort the stego works. Furthermore, a watermark extractor is also included to estimate the effect of prenegotiated manipulations.

More specifically, as shown in Fig 3.1 and 3.2, assume we would like to embed a message sequence $\vec{b}$={b_i|i=1,…,L} into the cover work. Each message bit 'bi' is embedded into a vector 'c_i' consisting of N components selected out of the cover work. In the jth iteration of the embedding process, each 'b_i' will be modulated with an N–component chip sequence 'w_i', scaled according to the weighting factor a_i^j, and then added to'c_i' to produce the stego work vector c_i^j . After message embedding, prenegotiated manipulations will be applied to the stegowork to introduce some distortion , k_i^j and a spread-spectrum watermark extractor is adopted to determine whether the embedded 'bi' can be successfully extracted when k_i^j has been applied to the stego work. Note that a_i^j is iteratively increased until 'b_i' can successfully resist k_i^j. Though the same prenegotiated manipulations are used throughout the whole iterative process, differences between k_i^p and, k_i^q given , p≠ q, are nature results due to the difference between c_i^p and c_i^q. Between 'k_i and 'w_i' lies within the range of [90-90] This fact implies that, inherently, about half 'b_i' will never show the intended invisible-ink behavior.

Securing Messages With Digital Invisible Ink

The effectiveness and feasibility of the SS-DII scheme is weighed up to formulate an application scenario where only the SS-DII techniques decides the protection of secured messages, wherein which it does not engage any sort of additional security modules like ciphers, symbols or passwords. In other hand, in the receiving end i.e., the unauthorized receiver tries to extract the hidden data/ messages directly through the equivalent watermark extractor, in the end he will have only the incorrect messages in his hand. But through prenegotiated manipulations along with the corresponding watermark extractor the hidden secret messages exactly attained.

4. PROPOSED SYSTEM

Difference between the existing and proposed system

In the existing system

1) Known Message Attack (KMA): The attacker is assumed to have access to watermarked signals and the messages embedded in each of those signals. This scenario constitutes the basis for the study of more involved scenarios and provides the main insight into the security problem (influence of the embedding parameters). It is also useful for the study of security in some watermark detection scenarios.

2) Watermarked Only Attack (WOA): The only information available to the attacker are the watermarked signals.

In Proposed System

Spread spectrum methods continue to be widely used, as many embedding functions existing nowadays are based on spreading. Thus, the analysis presented in this paper is expected to provide useful insights in the identification of security weaknesses of current spread spectrum schemes and the design of improved ones. In this regard, we want to remark that spread-spectrum-based embedding functions with improved security features have already been proposed .One of these embedding functions (Natural Watermarking) achieves perfect secrecy of data.

Registration format:

With the rapid development of parallel computing capacities of Registration process, this method alone could not be trusted to ensure security by increasing the key sizes, thus bringing in the information hiding techniques into the scenario. Cryptography scrambles the data to be secured while information hiding embeds the information into files which do not reveal the presence of information. Steganography and water marking are two information hiding techniques.

Watermarking security key:

The information hiding techniques into the scenario, Cryptography scrambles the data to be secured while information hiding embeds the information into files which do not reveal the presence of information. Steganography and water marking are two information hiding techniques. While steganography is used for secretly embedding the sensitive information in files, watermarking is used to implement copyright protection. Steganographic techniques are being widely used these days to increase the security of information. A combination of cryptography and steganography results in very strong cryptosystems.

File splitting & data hiding message:

The main results reveal fundamental limits and bounds on security and provide insight into other properties, such as the impact of the embedding parameters, and the tradeoff between robustness and security. On the practical side, workable estimators of the secret parameters are proposed and theoretically analyzed for a variety of scenarios, providing a comparison with previous approaches, and showing that the security of many schemes used in practice can be fairly low.

5. SYSTEM DESIGN

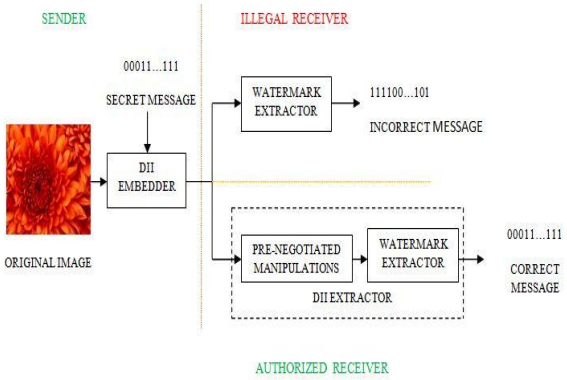

Fig. 5.1 Securing hidden message using the proposed DII scheme.

6. CONCLUSIONS AND FUTURE WORKS

This paper has briefly gone through experiments in models, implementations and applications, of invisible ink-liked data hiding techniques. Without any additional or extra alternation to the original work the Secret messages are embedded and in the other hand, in the receiving end there is no supplementary sensitive component is used for the deployment is required. plausible deniability the major key factor played a vital role in this project and it is combined with The proposed digital-invisible-ink scheme to provide better secrecy. Plausible deniability is actually used in multi level so that the hacker even with the matching key length will be fooled and made distant from the secured data without knowing that it is actually secured through certain manipulations and it is right in his hands. Moreover, the adopted statistical steganalysis scheme cannot differentiate works marked using the DII scheme from the one produced using common watermarking schemes with the cover message only. Budding dangers of delivering secret messages in the cover of legal watermarking

treatment are also pointed out. In the near future, to achieve better robustness against filtering and geometric attacks in the active-warden scenario, exploiting of the capacity issues of digital-invisible-ink schemes is done. Furthermore, we also try to work out ideas or proposals that can provide better concealment of data and even in future we can add up more levels of embedding procedures.

REFERENCES

1. F. L. Bauer, Decrypted Secrets: Methods and Maxims of Cryptology, 2nd ed. Berlin, Germany: Springer, 2000, ch. 1 HUANG.

2. D. Rigden, SOE Syllabus: Lessons in Ungentlemanly Warfare, World War II. East Sussex, U.K.: Gardners, 2004.

3. S. Katzenbeisser and F..A. P. Petitcolas, Eds., Information Hiding Techniques for Steganography and Digital Watermarking. Norwell, MA: Artech House, 2000.

4. By Wilhelm Burger, Mark J. Burge, Principles of Digital Image Processing: Core Algorithms.

5. Ingemar J. Cox, Digital watermarking and steganography, second edition, Elsevier Science Limited, 2008

6. Information Hiding: Steganography and Watermarking-Attacks and By Neil F. Johnson, Zoran Duric, Sushil Jajodia