An Erasable Watermarking Scheme Based on Text Exact Authentication

Xinmin Zhou, Lina Tan, Shu Xu
Institute of Big Data and Internet Innovation, Hunan University of Commerce, Changsha 410205, Hunan, China

Fang Lu *
School of Finance and Economics, Hunan University of Technology, Zhuzhou 412007, Hunan, China
*Corresponding author (E-mail: lufang31@126.com)

Abstract
It is becoming easier and easier to tamper with digital Works in ways that are difficult to detect. The problem of authentication has been well studied. This paper proposes a novel erasable text watermarking scheme for exact authentication, which includes authentication of content and format of Chinese Word documents. In this method, the cover document is divided into two blocks by utilizing the mathematical expression of Chinese characters, and then the hashing values of the text document’s content and format are embedded into the two blocks respectively by setting underlines to Chinese characters and hiding the underlines. In each block, the embedding position is chosen by Chinese character’s strokes and the magic square. Watermark to be authenticated can be extracted without the help of the original watermark and Word document itself. When any modification of the watermarked text document’s content and/or format are made, the Chinese text document will fail to pass the authentication. Experimental results indicate that the proposed scheme is efficient and secure.

Key words: Exact Authentication, Erasable Watermark, Text Watermark, Information Hiding.

1. INTRODUCTION
At present, the importance of authenticity and integrality verification become more apparent and acute. For example, a staff at a military headquarter has always to be sure that the digital media received come from the right people and that the contents are original. In response to these challenges, digital watermarking approaches conveying the authentication information in host multimedia have been proposed in the last decade. There are three main categories of watermarking approaches for multimedia authentication, namely fragile, semi-fragile, and erasable schemes (Cox, Miller, Bloom, et al., 2008). In deciding whether to make the scheme fragile, semi-fragile or erasable, the designer has to take the nature of applications and scenario into account since no single optimal scheme is available for all applications. There are a few watermarking schemes for multimedia authentication in following scenarios. In order to ensure the integrity of database relations, Guo et al. proposed a fragile watermarking scheme for detecting malicious modifications (Guo, Li, Liu, et al., 2006); a new semi-fragile image watermarking method is presented for the automatic authentication and tampering restoration of the content of digital images (Zhu, Ho and Marziliano, 2007); and an erasable watermarking scheme using skipped macro-blocks is addressed (Profrock, Richter, Schlauweg, et al., 2005), which suitable for authentication of H.264 compressed videos.

As for authentication of text documents, some watermarking schemes on binary document image authentication are proposed (Kim and De Queiroz, 2004; Puhan and Ho, 2005), but less on Word documents. Nowadays, many government organizations and enterprises provide more and more important data and other valuable information existing as Word documents through the Internet, and they are increasingly required to publish their data on the Internet (Samarati, 2001). Because the Internet is an open environment, it offers a convenient channel for service providers and users alike, the user can obtain such important information from the Internet. Unfortunately, if malicious tampering of these documents can not be perceived, the modified data can lead to unwanted and fatal wrong decisions and transaction disputes. Therefore, the authentication of Word documents has become a focused issue at present. In some applications, even the minimal distortion to text Word documents might be unacceptable. This has led to a research interest in using erasable watermarks, i.e., watermarks that can be removed from their associated cover Works to obtain exact copies of the original unwatermarked Works (Cox, Miller, Bloom, et al., 2008). Ideally, an erasable watermarking scheme for exact authentication would be able to embed a signature, and restore the watermarked Work to its original state. It is
theoretically impossible to make an erasable mark that can be embedded in digital content, which is the fundamental problem of designing an erasable watermark.

Compared with the work on image, audio and video watermarking, text watermarking has been relatively little focused on in the literature (Borges and Mayer, 2007). There is less research has been done on erasable text watermarking schemes for exact authentication. In fact, the exact authentication of Word documents should deserve more attention in some cases such as detection of hidden information in military communication. However, the researches of text watermarking schemes at present mainly focus on robust text watermarking which are designed for copyright protection. On the other hand, compared with images, Word documents have less redundant information, while there are rich redundant spaces suitable to be modified in images. Furthermore, Chinese semantics and word parsing are more difficult than that of western language; therefore, Chinese text watermarking is more difficult than English text watermarking. Generally speaking, the principle and thought of other multimedia watermarking schemes can not be used in text watermarking directly. Accordingly, there are some challenges for the research of erasable text watermarking.

In this paper a novel erasable watermarking scheme is proposed to provide exact authentication of Chinese Word documents. In the proposed method, through MD5 algorithm, the hashing values of the content and format information of the cover document can be obtained. According to structure types of Chinese characters, the whole Word document is divided into two blocks. By setting underlines to Chinese characters, watermarks dependent on the content and format information of the cover document are embedded into two text blocks on the basis of watermark bits and strokes of Chinese characters. This scheme is capable of providing exact authentication of the Word document with a high probability. Further more, this text watermarking scheme is the blind watermarking technique which the extracting process needs neither the original watermark nor cover document. The main contributions given in this paper are as follows:

(i) Developing a novel erasable text watermarking scheme which can detect any modification of the watermarked Work’s content and format, and analyzing the proposed scheme theoretically and empirically;

(ii) Through deep analysis on Chinese characters, which the complexity is exploited to provide lots of convenience to Chinese text watermarking;

(iii) Chaotic encrypting algorithm, a magic square and the algorithm of blocking text documents are introduced to enhance the security of erasable watermarking scheme.

The rest of this paper is organized as follows: Section 2 gives an overview of the related work. Section 3 will expound the principle and algorithms of the proposed watermarking scheme. The security analysis will be presented in Section 4, and the experiment results will be addressed in Section 5. Finally, Section 6 concludes the paper with summaries.

2. RELATED WORK

The research of text watermarking started from 1993, for the first time, N. F. Maxemchuk et al. of Bell Labs proposed several invisible techniques for encoding information in text documents to protect copyright. In September of 1995, the IEEE Journal on Selected Areas in Communications issue was scheduled to be published, for Secure Electronic Publishing Trial. There were over 1200 registered users in the first month, and every copy of every paper distributed was watermarked and registered with the recipient (Maxemchuk and Low, 1997). In 1999, a landmark paper on text watermarking has been published by Brassil et al. (Brassil, Low and Maxemchuk, 2000), in which the authors described and compared three different methods for watermark embedding into text documents. The authors formulate the problem as determining the capacity of text marking channel with line-shift coding, which the shifts of text lines should be Gaussian distributed with adjacent shifts negatively correlated (Low and Maxemchuk, 2000). In 2001, Atallah et al. of Purdue University proposed several methods of natural language watermarking (Atallah, Raskin, Hempelmann, et al., 2002), which opened up a brand-new and challenging research direction for text watermarking. For text watermarking, we have to distinguish between methods that hide information in the format, which means in the layout and the appearance, and methods that hide information in the content, which means that hide information by linguistic transformations, such as semantic transformations, synonym substitution and syntactic transformations.

Merits and limitations of watermarking methods that hide information in the format of text documents are described and compared as follows. Brassil et al. Brassil et al. proposed three different embedding methods for text documents: line-shift coding; word-shift coding and feature coding(Brassil, Low and Maxemchuk, 2000). In line-shift coding, single lines of the document are shifted upwards or downwards by very small amounts. The information to be hidden is encoded in the way the lines are shifted. Line centroids can be used as references in blind detection. However, the centroids are required to be uniformly spaced, that is not necessarily present in all documents. Similarly, words are shifted horizontally in order to modify the spaces between consecutive words in word-shift coding. Both methods are applicable to the format file of a document or to the bitmap of a page image. The third method, feature coding, slightly modifies features such as the pixel of characters, the length of the end lines in characters etc. Among the three presented methods, line-shift coding is the most robust in the
presence of noise but also most easily defeated. These two last methods can embed more bits in comparison to line-shift coding, but the original document must necessarily be available for non-blind detection and the algorithm of watermarking extraction can be comparatively complicated. Bender et al. proposed open space methods that encode information through manipulations of white space (unused space on the printed page), which exploit inter-sentence spacing, end-of-line spaces, and inter-word spacing in justified text (Bender, Gruhl, Morimoto, et al., 1996). Open space methods are useful as long as the text remains in an ASCII (American Standard Character Interchange) format. In this method, changing the number of trailing spaces has little chance of changing the meaning of a phrase or sentence, and a casual reader is unlikely to take notice of slight modifications to white space. But its robustness is worse and the watermarking capacity is very limited. Some improved watermarking schemes based on word-shift coding are proposed (Huang and Yan, 2001; Kim, Moon and Oh, 2003; Yang and Kot, 2004). Although the described methods can theoretically be defeated, it requires interactive human intervention and is expensive in practice.

Similarly, merits and limitations of watermarking methods that hide information in the content of text documents are presented as follows. Atallah et al (Atallah, Raskin, Hempelmann, et al., 2002) implemented watermark embedding through manipulations of TMR (Text meaning representation), such as grafting, pruning and substitution. In this scheme, the original document is not necessary, but it must be implemented by means of complex semantic analysis technique. This method is more robust and extends its watermarking capacity. Since a computer cannot understand the meaning of a text fully correctly, it is most difficult to improve this text watermarking technique. In a distinct class of algorithms, the schemes embed information into text documents by replacing words with their synonyms, but not by changing the meaning of sentences (Topkara, Topkara and Atallah, 2006). Synonym substitution is the most widely used linguistic transformation for information hiding systems since it is the simplest transformation. Synonym substitution has to take the sense of the word into consideration. In order to preserve the meaning of the sentence the word should be substituted with a synonym in the same sense. A clear advantage of this technique is that it is robust to multiple copying. However, it is language dependent, but not used directly in any language. Even more importantly, words can not always be replaced by their exact synonyms. Hence, the quality of the documents is depreciated by synonym substitution.

Another type of watermarking algorithm is based on syntactic transformations, such as adjunct movement, passivization and clefting (Atallah, Raskin, Crogan, et al., 2001). This method embeds watermark through changing the syntactic structure of a sentence with little effect on its meaning. An improved text watermarking based on syntactic transformations is proposed (Gupta, Pieprzyk and Wang, 2006), in order to reduce distortions caused by modifications made by attackers, the sequence of the paragraphs and sentences in a text document used to embed the watermark is permuted using a secret key, then watermarking bits are embed in the Least Significant Bits of the sentences’ cardinalities by modifying word counts of sentences. Other new embedding methods that hide information in the content of text documents are proposed (Liu and Tsai, 2007; El-Kwae and Cheng, 2002). These algorithms improve the robustness and the capability of resisting attack of watermarking system, but they are not applicable to text documents which contents can not be modified.

As fragile text watermark should be sensitive to alterations, which means that the embedded watermark should not be detectable after the Work is modified in any way. If a very fragile mark is detected in a Work, we can infer that the Work has probably not been altered since the watermark was embedded. However, because every kind of watermark embedding modes has the fatal drawback of itself, the watermarking fragility is difficult to be implemented by hiding information only in the format or content of Word documents. Therefore, according to the analysis of watermarking methods described above, we design a new erasable watermarking scheme based on the content and format information of text documents. In this scheme, watermarks generated are from the hashing values of the content and format of the host document respectively, and watermark embedding is implemented through setting underlines to Chinese characters. The erasable watermarking scheme is designed for exact authentication of Word documents. In this scenario, an attacker will try his best to make modifications to a Word document while keeping the embedded watermarks untouched. The attack is successful if the Word document is modified while the embedded watermarks are still unchanged or the watermark extraction and verification can not detect the alterations. In order to resist tampering or attack, the embedded watermarks of the scheme are designed to be dependent on the content and format information of Word documents, which is sensitive to any modification made to the Word document. If there is any alteration, the watermark extraction and verification can be able to perceive the alterations accurately.

3. THE PROPOSED WATERMARKING SCHEME

In this section, we introduce in detail our proposed erasable watermarking scheme for exact authentication of Chinese Word documents. We define words, sentences and paragraphs of a Chinese Word document as semantic entities. Any semantic entity changing will result in different understanding of text meaning to some extent. Generally, as Chinese characters can not be handled in a computer conveniently like English letters, it is
obvious that research on erasable watermarking of Chinese text documents is more difficult. Text documents are, however, the most difficult to be watermarked, because text manipulations are guided by strict rules in terms of grammar, syntax, semantics, context-based selection of a word from a set of synonymous words, etc; while in the case of other media, there is large amount of redundant information to manipulate. But in text documents, when a watermark is embedded in content of a text document, grammatical rules need to be preserved. Therefore, it is difficult to implement text watermarking algorithms based on content, but there is large amount of formatting information to manipulate for watermark embedding.

Through deep analysis on Chinese characters, we find that it is the complexity of Chinese characters that brings a few advantages to Chinese text watermarking. We have implemented an erasable watermarking scheme for exact authentication of Chinese Word documents by exploiting the features of Chinese characters. In this section we will present thought of blocking text documents, mathematical model and definitions, and algorithms of the watermarking scheme.

3.1. Blocking Text Documents

The Chinese mathematical expression theory can remedy the inadequacy of information of a Chinese character ISN (internal statement number), ensuring that a computer handles Chinese characters in Chinese components whose granularity is much smaller than Chinese characters, which create advantages for the research of text watermarking. The mathematical expression of Chinese characters is a novel mathematical method to express Chinese characters based on deep analysis of knowledge about character structure. In this method, a Chinese character is expressed into a mathematical expression in which the components of Chinese characters act as operands and the position relationships between two components act as operators which satisfy some certain operation laws, just like general math expressions.

Based on the deep statistical analysis, 580 basic components are selected to get the expressions of all the 20902 CJK Chinese characters standardized by UNICODE, and six spatial relations of two components are needed to be defined as the operators in the mathematical expression. These six operators are lr, ud, ld, lu, ru and we which represent respectively the spatial relation of left-right, up-down, left-down, left-upper, right-upper, and whole-enclosed defined strictly (Sun, Chen, Yang, et al., 2002).

The method is simple and suitable for Chinese characters. With this method, Chinese characters can be processed in a computer like English letters to a certain extent. Some applications have been achieved, such as platform-spanning transmission of Chinese information, knowledge mining of character structure and Chinese text watermarking. We can acquire the structure types and the strokes of Chinese characters by the mathematical expression of Chinese characters, the concrete methods are as follows:

Structure types: obtained by the prefix expression of mathematical expression of a Chinese character, the mathematical expression of every Chinese character in UNICODE 3.0 can be converted to the equivalent prefix expression, whose first operator is the structure type of the Chinese character.

Strokes: obtained by counting strokes of basic components of Chinese character and strokes of every basic component have been calculated beforehand.

In this paper, structure types and strokes of Chinese characters are utilized together to improve the robustness of text watermarking algorithm. Structure types of Chinese characters are used to divide the whole document into two blocks. In each block, not only watermarking bit but also Chinese character’s strokes are chose to determine the position selected to embed watermarking. According to the general table of single character frequency of Chinese characters, we have calculated that the frequency of the Chinese characters of left-right body (lr) and hybrid body (we, lu, ld and ru) accounts for 50.08%, and the frequency of the Chinese characters of up-down body (ud) and single body (basic component) accounts for 49.71%. Based on the above statistical results, a host document can be divided into two blocks comparatively uniformly, which is called first block h1 including Chinese characters of left-right body and hybrid body, and second block h2 including Chinese characters of up-down body and single body respectively. Further Statistical results show that the respective frequency of the Chinese characters with odd strokes and even strokes in first block account for 21.65% and 28.43%, the corresponding frequency in second block account for 24.58% and 25.12%. Therefore, selecting the parity of Chinese characters strokes as the controlling parameter is advisable while watermark embedding.

3.2. Mathematical Model And Definitions

We represent the erasable watermarking scheme as EWS, where

\[ EWS=\{H, K, \xi, \zeta, \psi\} \]  \hspace{1cm} (1)

\[ H = \text{a set of host text documents}; \ K = \text{a set of secret keys}. \]

Watermarking embedding \(\xi: H\times K \rightarrow H^{(w)}\) \hspace{1cm} (2)

where \(H^{(w)}\) is a watermarked text document.
Watermarking extraction $\zeta: H^{m\times n} \rightarrow W_e$ (3)

where $W_e$ is a extracted watermark. If the watermarked document does not undergo any malicious attack, then $W_e=W_i$, that is, $\zeta(H, K, K) = W_i$, where $W_i = \{w_i, w_2, \ldots, w_n\}$ is the watermark to be embedded, $\forall i$, $w_i \in \{0, 1\}$, $w_i$ is the $i^{th}$ bit of the watermark.

Watermarking verification $\forall H: H^{m\times n} \times W_e \rightarrow \{\text{true/false}\}$ (4)

The verification is completed by calculating the correlation between $W_e$ and $W_i$.

In order to make the following watermarking algorithms easily understood, some of the definitions are expounded as follows:

**Definition 1** A function block is called blocking function on text document $H$, if for $h \in H$

\[
(h_s, h_f) = \text{Separate}(h)
\]

$h_s$ and $h_f$ denote the content and format information of text document $h$ respectively.

**Definition 2** Algorithm MD5 is used as the hashing function, given a string $s$, which the hashing value is denoted as $\text{Hash}(s)$ of 32-bit hex.

**Definition 3** Given a binary string $str_b$ and the corresponding hex string $str_h$, the conversion relation between them is denoted as follows:

\[
str_h = \text{Hex}(str_b), \quad str_b = \text{Binary}(str_h)
\]

**Definition 4 (Chaotic encrypting function)** A function chaos is called chaotic encrypting function. Optical bistable model

\[
X_{n+1} = A\sin^2(X_n - X_h)
\]

is used as chaotic encrypting algorithm, and then make iterative computations,

\[
\text{if } X > 2*A/3, \quad E_i = 1
\]

\[
\text{else } E_i = 0
\]

where $A=4, X_0=2.5$, the equation is in chaos, $E_i$ denotes the chaotic sequence value. As different $X_0$ will result in complete different chaotic sequence values, here $X_0$ is regarded as the key of the encrypting algorithm. Encrypting or decrypting is completed by making logical operation of Xor between chaotic sequence values and plaintext or ciphertext, which is transformed into the binary form.

**Definition 5** $\Omega = \{C_i | C_i \text{ is a Chinese character in UNICODE 3.0}\}$, i.e., $\Omega$ is the set of all the Chinese characters in UNICODE 3.0, the strokes of $C_i$ is denoted as $S(C_i)$ and the structure type of $C_i$ is denoted as $\text{Str}(C_i)$.

**Definition 6** Given $W_i$ and $h = \{h_s, h_f\}$, $w_i$ is the $i^{th}$ bit of the watermark, $h$ is a set of Chinese characters, where $h = \{C_1, C_2, \ldots, C_n\}$. Let Embed($w_i, C_i$) denote embedding the watermark bit $w_i$ in the position of $C_i$.

**Definition 7** Given the $j^{th}$ bit of watermark $w_j$, and array underline[16]={2,3,4,6,7,9,10,11,20,23,25,26,27,39,43,55}, in which every different element of the array represents the value of different type underlines. $w_j$ is embedded by setting underline to a candidate and hiding it simultaneously, the value of underline type is equal to underline[i], $i := ((j-1) \mod 16) + 1$.

**Definition 8** Suppose that $M$ is an $n$-by-$n$ matrix $M$ consisting of natural numbers. If and only if

\[
\text{i) } \forall k \in \{1, 2, \ldots, n\}, \quad \sum_{i=1}^{n} m_{ik} = \sum_{j=1}^{n} a_{ij} = c \quad (c \text{ is a constant which is only relevant to } n)
\]

\[
\text{ii) } \sum_{i=j}^{m} m_{ij} = \sum_{i+j=1}^{n} m_{ij} = c
\]

Then $M$ is called a magic square. Specially, the matrix $M$ is called normal magic square of $n$-order if its matrix elements consist of the consecutive integers $1, 2, \ldots n^2$.

**Definition 9** Let $C_i$, hiding the $j^{th}$ bit of watermark, i.e. $w_j$,

\[
\text{if } S(C_i) \mod 2 = 1, \quad w_j = 1,
\]

\[
\text{else } w_j = 0.
\]
Definition 10 (Similarity function) Let \( C \) be a nonempty set. A function \( \text{sim} : C^2 \rightarrow (-\infty, 1] \) is called similarity function on \( C \), if for \( x, y \in C \)
\[
\text{sim}(x, y) = 1 \iff x = y
\]
for \( x \neq y \), \( \text{sim}(x, y) < 1 \)

In the case of watermarking verification the correlation between original watermark \( W_i \) and extracted watermark \( W_e \) can be calculated by using the similarity function. If \( \text{sim}(W_e, W_i) = 1 \), then the watermarking verification result is true and the verification of text document is passed.

3.3. Watermark Algorithms

In this Section, we will describe the algorithms of watermarking scheme in detail. In our scheme, the watermark is embedded by setting underlines to Chinese characters which are embedding candidates, and hiding the underlines simultaneously. According to the mathematical model of the proposed watermarking scheme, the watermarking algorithms is composed of three parts primarily, that is algorithms of watermark embedding, watermark extracting and verification, which are described in algorithm 1, algorithm 3 and algorithm 4, algorithm 2 is used for blocking text documents.

In order to make the following watermarking algorithms easily understood, let \( \text{length}(W) \) denote the bit number of \( W \), \( \text{length}(h) \) the number of Chinese characters in a document \( h \), and \( \text{length}(h, j) \) the number of Chinese characters in the \( j \)th line of \( h \). Let \( \text{Order}(p) \) denote the least odd number which is not less than the square root of \( p \), where \( p \) is a positive integer.

Algorithm 1: \( \zeta (h, k) \)
// algorithm \( \zeta \) is designed for watermark embedding
\[
\begin{align*}
\text{Input:} & \text{ a cover document } h, \text{ the key } k. \\
\text{Output:} & \text{ a watermarked text document } h^{(w)}. \\
1: & (h_1, h_2) = \text{Block}(h) \ // \text{See Algorithm 2} \\
2: & (h_c, h_f) = \text{Separate}(h) \ // \text{See Definition 1} \\
3: & (m_c, m_f) = \text{Hash}(h_c, h_f) \ // \text{See Definition 2} \\
4: & (b_c, b_f) = \text{Hex}(m_c, m_f) \ // \text{See Definition 3} \\
5: & W_1 = \text{Chaos}(b_c, k) \ // \text{See Definition 4} \\
6: & W_2 = \text{Chaos}(b_f, k) \\
7: & \text{for } i=1 \text{ to } 2 \text{ do} \\
8: & \quad n=\text{length}(W_i) \\
9: & \quad m=\text{length}(h_i) \\
10: & \quad \text{pos}=1 \\
11: & \quad \text{for } j=1 \text{ to } n \text{ do} \\
12: & \quad \quad \text{for } k=\text{pos} \text{ to } m \text{ do} \\
13: & \quad \quad \quad \text{if } (w_j = x \text{ and } S(C_k) \mod 2 = x) \ // x \in \{0, 1\} \\
14: & \quad \quad \quad \text{Embed}(w_j, C_k) \ // \text{See Definition 5, 6, 7} \\
15: & \quad \quad \quad \text{pos}=\text{pos}+1 \\
16: & \quad \quad \text{exit the “for” iteration} \\
17: & \quad \text{end if} \\
18: & \quad \text{end for} \\
19: & \text{end for} \\
\end{align*}
\]

In algorithm 1, the watermarks used for authentication are generated according to the cover document \( h \) and the key \( k \), and the watermark \( W_1 \) and \( W_2 \) are independent on the content and format information of the cover document respectively. Watermark embedding is completed by setting underlines to Chinese characters in two text blocks on the basis of watermark bits and strokes of Chinese characters.

Algorithm 2: \( \text{Block}(h) \)
// algorithm \( \text{Block} \) is designed for blocking text documents
\[
\begin{align*}
\text{Input:} & \text{ a text document } h. \\
\text{Output:} & h_p, h_s. \\
1: & \text{the total number of lines in } h \rightarrow l \\
2: & n = \text{Order}(l) \\
3: & \text{Generating a magic square } M \text{ with } n\text{-order} \\
\quad \text{ // According to Definition 8} \\
4: & \text{for } i=1 \text{ to } n \text{ do} \\
5: & \quad \text{for } j=1 \text{ to } n \text{ do} \\
\end{align*}
\]
In algorithm 2, the two text blocks and the magic square are utilized for scrambling watermark in order to enhance the security of the proposed watermarking scheme, and function \textit{Order} is used to select a rational order of the magic square in order to make full use of lines of the cover document for embedding the watermark.

Algorithm 3: \(\tilde{\zeta}(h^{w}, k)\)
// algorithm \(\tilde{\zeta}\) is designed for watermark Extracting
\textbf{Input}: a watermarked text document \(h^{w}\) and the key \(k\).
\textbf{Output}: watermark extracting result \(W_{1}, W_{2}\)
1: \((h_{1}^{w}, h_{2}^{w}) = \text{Block}(h^{w})\) // See Algorithm 2
2: \(\text{for } i=1 \text{ to } 2 \text{ do}\)
3: \(n = \text{length}(h_{i}^{w})\)
4: \(W_{i} = ""\)
5: \(\text{for } j=1 \text{ to } n \text{ do}\)
6: \(\text{if } C_{j} \text{ hiding a bit of watermark in } h_{i}^{w}\)
7: \(\text{extract the watermark bit and concatenate } W_{i}\)
8: \(\text{else}\)
9: \(i = i+1\)
10: \(\text{end if}\)
11: \(\text{end for}\)
12: \(\text{end for}\)

In algorithm 3, watermark extracting can be regarded as the reverse of watermark embedding simply. It’s important to note that before watermark extracting the watermarked document should be divided into two blocks according to the blocking principle of watermark embedding. The extracted watermarks are used for watermark authentication of algorithm 4.

Algorithm 4: \(\psi(h^{w}, W_{1}, W_{2})\)
// algorithm \(\psi\) is designed for watermark verification
\textbf{Input}: a watermarked Work \(h^{w}\), \(W_{1}\) and \(W_{2}\)
\textbf{Output}: watermark verification result \(\Theta\)
1: Obtaining the restored document \(h^{'}\) by cancelling underlines of watermark embedding candidates in \(h^{w}\)
2: \((h_{1}^{'}, h_{2}^{'}) = \text{Separate}(h^{'}))\)
3: \((m_{1}, m_{2}) = \text{Hash}(h_{1}^{'}, h_{2}^{'})\)
4: \((b_{1}, b_{2}) = \text{Hex}(m_{1}, m_{2})\)
5: \(W_{1}^{'}, W_{2}^{'}, = \text{Chaos}(b_{1}^{'}, k)\)
6: \(W_{2}^{'} = \text{Chaos}(b_{2}^{'}, k)\)
7: \(\text{if } \text{sim}(W_{1}, W_{1}^{'})=1 \text{ and } \text{sim}(W_{2}, W_{2}^{'})=1\)
8: \(\Theta = \text{true}\)
9: \(\text{else}\)
10: \(\Theta = \text{false}\)
11: \(\text{end if}\)
In algorithm 4, If and only if the extracting watermarks $W_1$ and $W_2$ match perfectly the regenerated watermark $W'_1$ and $W'_2$ respectively, the text document can be able to pass the exact authentication. Before watermark authentication, it is the prerequisite to acquire the restored document on the basis of watermark embedding rules.

4. SECURITY ANALYSIS

The security of a watermark refers to its ability to resist intentional tampering or hostile attack, which becomes a significant issue when someone is motivated to prevent a watermark from serving its intended purpose. Watermarks can be attacked in a variety of different ways, and each application requires its own type of security.

The proposed scheme is designed for exact authentication of Chinese Word documents, and the most basic task of exact authentication is to verify that a Work has not been altered at all since it left a trusted party. If even a single bit has been changed, the Work is regarded as inauthentic. By insisting on a perfect copy, we avoid any need to design algorithms that can differentiate between acceptable and unacceptable alterations. Generally, any modification will be often referred to as vicious attack. Based on this background, we will discuss analyzing on attacks and errors of the watermarking system as follows.

4.1. Analyzing Attacks

In the proposed scheme, if the attacker does not known what the watermark means or has not the key, unauthorized watermark embedding will destroy the content or format of the authenticated text document, which will result in the fail of authentication. As two different Works can not contain the same watermark in our scheme, the attack of unauthorized detection can not prevent the watermark from serving its intended purpose. In this scenario, the primary purpose of an attacker is to tamper the watermarked Work or watermark in order to defraud the receivers of their trust by passing the authentication of text documents. Obviously, even if the watermark is removed without any modification to content of the watermarked text document, the attacker is unable to obtain the intended purpose.

As the watermark is carried in the formatting information, hence, retyping, reformating or reproducing attacks will change these formatting attributes, which will result in the watermark destroyed and the authentication failed. At the same time, any semantic entity changing such as semantic entity addition, deletion, swapping, shuffling, etc., will result in different content and format of text document to some extent, and their hashing values will be completely different from that of the original. Under these scenarios, the extracted watermark is impossibly consistent with the embedded watermark, and the authentication of text document will be failed too. Hence, this scheme is totally secure against formatting attacks and semantic entity changing attacks. Chaotic encrypting algorithm lies at the core of our scheme as it is used to generate chaotic sequences for encrypting the watermarks. It makes use of chaotic system properties such as sensitive to initial condition; it will result in the entirely different chaotic sequence, even if there is $10^9$ difference to the original key. As long as the attacker does know nothing of the key of the chaotic encrypting algorithm, it is impossible to fake the watermarked document. Accordingly, the proposed scheme is able to meet the Kerckhoff Principle of cryptography completely.

4.2. Analyzing Errors

Errors are inevitable in even the best-designed watermarking systems. The proposed scheme is a blind detection algorithm, which detector does not require any information related to the original Work and original watermark. Nonetheless, in non-blind watermarking scheme, watermark detector determines the presence of watermark through calculating the similarity between extracted watermark and original watermark. False positive and false negative errors are coupled and impacted by the setting of the threshold, i.e. the setting of the similarity mentioned above. In our proposed scheme, the relativity between false positive errors and false negative errors is reduced effectively by the blind detection algorithm. According to strokes of Chinese characters, watermark bits are embedded by setting underlines with a certain embedding periodicity, and the embedded watermarks are related to the content and format of host text document, when the extracted watermarks from the two text blocks are consistent with the embedded watermarks respectively, the authentication is successful, else failed. By this kind of distinctive authentication mode, the probability of message errors is reduced effectively.

5. EXPERIMENTAL RESULTS

In order to prove the validity of the algorithm, let us give some examples of the watermarking system. As there is no public testing document for text watermarking scheme, here some famous essays of Mr. Zhu Ziqing are regarded as the testing Word documents. The text blocking results are presented in the following table 1, which indicates that the cover documents are divided into two blocks comparatively uniformly according to algorithm 2, and table 2 gives the total numbers of Chinese characters with odd or even strokes in the block of
h₁ and h₂ respectively, which shows that choosing the parity of Chinese characters strokes as the controlling parameter while watermark embedding is advisable.

<table>
<thead>
<tr>
<th>paper</th>
<th>title</th>
<th>hₙ</th>
<th>h₁,n</th>
<th>h₂,n</th>
</tr>
</thead>
<tbody>
<tr>
<td>P₁</td>
<td>The Transient Days</td>
<td>542</td>
<td>270</td>
<td>272</td>
</tr>
<tr>
<td>P₂</td>
<td>Moonlight over the Lotus Pond</td>
<td>1179</td>
<td>563</td>
<td>616</td>
</tr>
<tr>
<td>P₃</td>
<td>Retreating Figure</td>
<td>1141</td>
<td>519</td>
<td>622</td>
</tr>
<tr>
<td>P₄</td>
<td>Qinhuai River in the Oaring Sound and Light Shadow</td>
<td>4927</td>
<td>2529</td>
<td>2398</td>
</tr>
<tr>
<td>P₅</td>
<td>Woman</td>
<td>3162</td>
<td>1478</td>
<td>1684</td>
</tr>
</tbody>
</table>

In table 1, hₙ denotes the total numbers of Chinese characters in the whole text document, h₁,n denotes the total number of Chinese characters in the block of h₁. Obviously, hₙ = h₁,n + h₂,n.

**Table 2.** The total numbers of Chinese characters with odd or even strokes in each block

<table>
<thead>
<tr>
<th>paper</th>
<th>h₁,odd</th>
<th>h₁,even</th>
<th>h₂,odd</th>
<th>h₂,even</th>
</tr>
</thead>
<tbody>
<tr>
<td>P₁</td>
<td>122</td>
<td>148</td>
<td>162</td>
<td>110</td>
</tr>
<tr>
<td>P₂</td>
<td>253</td>
<td>310</td>
<td>337</td>
<td>279</td>
</tr>
<tr>
<td>P₃</td>
<td>242</td>
<td>277</td>
<td>339</td>
<td>283</td>
</tr>
<tr>
<td>P₄</td>
<td>1028</td>
<td>1501</td>
<td>1338</td>
<td>1060</td>
</tr>
<tr>
<td>P₅</td>
<td>619</td>
<td>859</td>
<td>893</td>
<td>791</td>
</tr>
</tbody>
</table>

In table 2, h₁,odd and h₁,even denote the total numbers of Chinese characters with odd and even strokes in the block of h₁ respectively. As the statistical samples are reduced, the results of table 1 and table 2 are different from the results that are calculated according to the general table of single character frequency of Chinese characters. But this does not affect designing of the watermark system.

In order to examine and certify the security of the watermarking scheme, Moonlight over the Lotus Pond of Mr. Zhu Ziqing’s famous essays is regarded as the original cover document. As the total number of lines in this cover text is 35, so the selecting order of the magic square is 7 according to Algorithm 3 mentioned above. In this case, according to Algorithm 4, the following magic square M is used for scrambling the watermark. There are 14 elements of M, which values are more than 35, and these elements are not exploited for scrambling the watermark.

\[
M = \begin{bmatrix}
30 & 39 & 48 & 1 & 10 & 19 & 28 \\
38 & 47 & 7 & 9 & 18 & 27 & 29 \\
46 & 6 & 8 & 17 & 26 & 35 & 37 \\
5 & 14 & 16 & 25 & 34 & 36 & 45 \\
13 & 15 & 24 & 33 & 42 & 44 & 4 \\
21 & 23 & 32 & 41 & 43 & 3 & 12 \\
22 & 31 & 40 & 49 & 2 & 11 & 20
\end{bmatrix}
\]

To the testing Word document P₂, the distribution maps of Strokes in h₁, h₂ are shown in Figure 1 and Figure 2, respectively.
The hashing value of the content of the cover text generated by MD5 algorithm is b4b837b49a02a72fd c1c76672bebd89b, and the corresponding encrypting results with different keys are displayed in table 3, which indicates that the results of chaotic encrypting algorithm is very sensitive to the initial condition.

<table>
<thead>
<tr>
<th>Key</th>
<th>Encrypting values of the hashing value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key=3.14</td>
<td>ed47c9b42a0905808fe38dd8d30b9dde</td>
</tr>
<tr>
<td>Key=3.141</td>
<td>e9606834c5fd7cd03d0804d92c682766</td>
</tr>
<tr>
<td>Key=3.1415</td>
<td>e8e7c85a5fd632c1de8987f8141d00</td>
</tr>
<tr>
<td>Key=3.14156</td>
<td>e8b8c84d500a1d0221b8a592aee4364</td>
</tr>
<tr>
<td>Key=3.141565</td>
<td>e8b3c84c25219b282253899704fc7b64</td>
</tr>
</tbody>
</table>

Even if there is $10^{-6}$ difference to the original key, it will result in the entirely different encrypting result. Accordingly, the proposed scheme is able to meet the Kerckhoff Principle of cryptography completely, and the security of the proposed scheme is verified further. According the experimental results mentioned above, even if the attacker obtains the original text document, as he or she does know nothing of the order of the magic square and the key of the chaotic encrypting algorithm, it is impossible to fake the watermarked document for the attacker. The experimental results are consistent with our security analysis.

6. CONCLUSIONS

A novel erasable watermarking scheme for exact authentication of Chinese Word documents is proposed in this paper. This scheme is able to embed watermark, restore the watermarked Work to its original state, and have a very low false positive probability. Watermarks generated by the content and format information of text cover document are embedded in the two blocks respectively by setting underlines to Chinese characters, and the watermark extracting needs neither original cover document nor original watermark. The characteristics of this scheme is presented as follows: (i) structure types and strokes of Chinese characters are exploited to block
text documents and to select candidates of embedding position respectively; (ii) in order to improve security of the scheme, chaotic sequences are used to encrypt the watermark, and algorithms of blocking text document and generating magic square are utilized for scrambling the watermark; (iii) any modification of the content and format for watermarked text document can be detected.

Acknowledgements

This work was supported by 13CJY007 (National Social Science Fund Projects of China), I2YJAZH216 (Ministry of Education, Humanities and Social Sciences Research Projects), 15B070 (Outstanding Youth Project Of Hunan Education Department), 2012FJJ3058 (Science and Technology Project of Hunan Province) and 2011ZK3045 (Soft Science Project of Hunan Provincial Science and Technology Department).

REFERENCES


Samarati P.(2001)”Protecting respondents identities in microdata release”, IEEE Transactions on Knowledge and Data Engineering, 13(6), pp.1010-1027.

