A SPECTRUM METHOD FOR NATURAL LANGUAGE TEXT WATERMARKING TECHNIQUE

Dr. Hana'a M. Salman

Department of Computer Science & Information System, Technology Univ., Baghdad, Iraq,
salmanhana2007@yahoo.com

ABSTRACT

Natural language text watermarking, means embedding the watermark into a text document, using the natural language components as a carrier, in such a way that, modifications are imperceptible to the readers and the embedded information is robust against possible attacks.

The watermark embedding scheme can either embed the watermark directly into host data or to a transformed version of the host data.

In this paper a transform watermark embedding scheme is used for watermarking natural language text is proposal by using the spectrum method. Also explore various ways of natural language text watermarking. The results show that, the proposal technique is a successful one in implementing methods like, natural language text watermarking using spectrum transformation

Keywords: *Natural Language Watermarking, Spectrum Method, Transform Method.*

1. INTRODUCTION

Internet is being increasingly used as the platform for distribution of digital multimedia content. The inherent flexibility of Internet facilitates users to transact with one another to create, distribute, store, peruse, subscribe, enhance, modify and trade digital content in various forms like text documents, databases, e-books, still images, audio, video, computer software and games [1].

Even with the proliferation of image and video data, text data still forms the bulk of Internet tract and other forms of data that encounter everyday.

Most magazines, newspapers, scientific journals, and conferences provide articles in digital format. While this is improving the ways readers can search and access information, it also brings about author concerns about how their work is distributed and reused. This grows the concerns about protection and enforcement of intellectual property rights of the digital content involved in the transaction. In addition, unauthorized replication and manipulation of digital content is relatively trivial and can be done using inexpensive tools, unlike the traditional analog multimedia content. A solution is rise through the use of digital watermarking [1].

Digital watermarking is a process of embedding unobtrusive marks or labels into digital content. These embedded marks are typically imperceptible that can later be detected or extracted [1].

Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the watermark remains in the content in its original form and does not prevent a user from listening to, viewing, examining, or manipulating the content.

Also, unlike the idea of steganography, where the method of hiding the message may be secret and the message itself is secret, in watermarking, typically the watermark embedding process is known and the message (except for the use of a secret key) does not have to be secret.

In steganography, usually the message itself is of value and must be protected through clever hiding techniques and the "vessel" for hiding the message is not of value. In watermarking, the effective coupling of message to the "vessel," which is the digital content, is of value and the protection of the content is crucial.

Watermarking is the direct embedding of additional information into the original content or host signal. Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal. In some instances, the amount of information that can be hidden and detected reliably is important [2].

Applications for digital watermarking include copyright protection, fingerprinting, authentication, copy control, tamper detection, and data hiding applications such as broadcast monitoring [2].

The Application of watermarks determines its requirements, and hence, the used technique for implementation. For instance, a straightforward way to provide an imperceptible watermark is to embed the watermark signal into the perceptually insignificant portion of the host data. However, this makes the watermark vulnerable to attack because it is fairly easy to remove or alter the watermark without affecting the host signal.

To provide a robust watermark, a good strategy is to embed the watermark signal into the significant portion of the host signal. This portion of the host data is highly sensitive to alterations, however, and may produce very audible or visible distortions in the host data [2].

The watermark embedding scheme can either embed the watermark directly into the host data or to a transformed version of the host data. The cover signal is generally a still image, audio clip, video sequence or a

text document in digital format. Digital watermarking technique is appealing, since it provides many features "Imperceptibility, Robustness, Inseparability, and Security" and does not require out-of-band data as in other mechanisms. Various types of watermarking techniques "Robust & Fragile Watermarking, Visible & Transparent Watermarking, Public & Private Watermarking, Asymmetric & Symmetric Watermarking, Asymmetric & Symmetric Watermarking, and Steganographic & Non-Steganographic Watermarking", each of the different types mentioned below have different applications.

Digital watermarking is one of the key technologies that can be used for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication and facilitating content authentication.

The objective of this paper is to proposal a natural language text watermarking technique using spectrum method, and reviews the current state of the art in natural language watermarking, which aims to embed information in text documents. The proposal natural language watermarking technique is different from all the natural language watermarking technique, that uses structure of the sentence constituents in natural language text or all others techniques, which modify the appearance of text elements, such as lines, words, or characters. Text watermarking is achieved by altering the text format or fonts, such as modifying inter-word and inter-letter spacing in text. Watermarks inserted by most of these systems are not robust against attacks such as scanning the document and performing optical character recognition or re-formatting of the document file.

The organization of the paper is as follows: In Section 2, the unique difficulties in natural language Watermarking caused by the structure of language are introduced in Section 3. A survey of current state of the art in natural language watermarking In Section 4, The proposal technique with a test, in Section 5, followed by conclusions in Section 6

2. DIFFICULTIES IN NATURAL LANGUAGE WATERMARKING

The goals of watermarking in natural language are: The embedding of information by modifying original data in a discreet manner, such that the modifications are imperceptible when the watermarked data is consumed and the embedded information is robust against possible attacks.

On the other hand, language has a discrete and syntactical nature that makes such techniques more difficult to apply. Specifically, language, and consequently its text representation, has two important properties [3]:

1. Sentences have a combinatorial syntax and semantics. That is, structurally complex (molecular) representations are systematically constructed using structurally simple (atomic) constituents, and the semantic content of a sentence is a function of the semantic content of its atomic constituents together with its syntactic/formal structure.
2. The operations on sentences are causally sensitive to the syntactic/formal structure of representations defined by this combinatorial syntax.

The atomic/syntactical nature of language brings about unique challenges for natural language watermarking. For example, deriving an analog of least significant bit (LSB) embedding that modifies text locally, i.e., based on words, without making perceptually significant changes to sentence structure is a hard problem. This is due to the fact that even small local changes in a sentence can change its semantics and/or make it ungrammatical. The only current local modification techniques used are the synonym substitution methods in natural language steganography. These approaches are unsuitable for natural language watermarking since they are not robust to attacks [3].

3. THE PREVIOUS WORK ON NATURAL LANGUAGE TEXT WATERMARKING

Work in natural language text watermarking goes in two main directions as a result to the natural, and difficulties of the text: using text layout and format modification, using text it self. The later technique uses the natural language processing techniques and tools for watermark embedded. A review to the previous work done in natural language watermarking is presented in bellow subsections.

3.1. TEXT LAYOUT AND FORMAT MODIFICATIONS

Most of this work is based on hiding the watermark information into the layout and formatting of the document directly. In, the authors develop document watermarking schemes based on line shifts, word shifts as well as slight modifications to the characters. These techniques are focused on watermarking the binary-valued text regions of a document.

Watermark detection consists of post-processing steps to try to remove noise and correct for skew. These techniques are quite effective against some common attacks such as multigenerational photocopying. The authors point out that optical character recognition can remove the layout information and, for such schemes, remove the watermark information.

Figure (1) illustrates an example from of word shift coding: (a) shows where the space has been added before the word “for,” and (b) contains the un-watermarked and watermarked versions in their natural state to illustrate that the word shift is not noticeable.

Figure (2) shows an example from on character alteration for watermark embedding: In (a), no coding has been applied. In (b), feature coding has been applied to select characters. In (c), the feature coding has been exaggerated to show feature alterations [2].

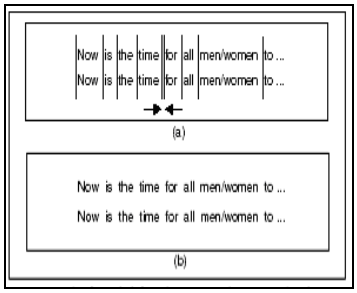

Figure (1): Example from of word shift coding

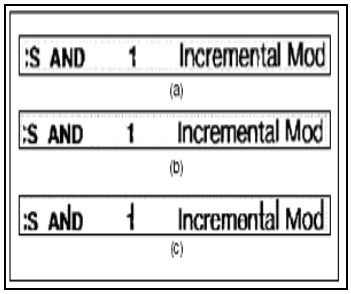

Figure (2): Example from on character alteration

2.2. USING TEXT IT SELF

There are two types of these techniques: Technique which, capable of embedding the watermark in the text itself, and Technique which, capable of embedding the watermark in the transform of text. Both the above technique uses the natural language processing technique and tools.

Primitive methods, such as inserting spelling and/or punctuation peculiarities and/or deliberate errors and/or synonym substitutions while still being used, turn out to be not very effective, besides degrading the text [4].

The idea of employing the semantics and syntax of text for inserting watermarks was first proposed by Atallah et al. in 2000, where the quadratic residues to the ASCII number corresponding to each word of the text, thus making it carry a bit of the watermark and necessitating lexical synonym substitutions " of word or even of phrases" [4].

In later Atallah et al. have proposed two algorithms that embed information in the tree structure of the text rather than using lexical substitution these techniques aim to modify the structural properties of intermediate representations of sentences, built using natural language processing tools. In other words, the watermark is not directly embedded to the text, as is done in lexical substitution, but to the parsed representation of sentences. Utilizing the intermediate representation makes these algorithms more robust to attacks compared with lexical substitution systems. The difference between the two proposed algorithms is that the first one modifies syntactic parse trees of the cover text sentences for embedding while the second one uses semantic tree representations. A syntactic tree is a representation of various parts of a sentence that has been syntactically parsed [3].

A better approach to natural language watermarking is to analyze the global semantic/syntactical structure of the sentence to be modified and then apply transformations that preserve its meaning and grammaticality. According to the transformational grammar (TG) theory of Chomsky, multiple sentences may be derived from the same underlying form by linguistic transformations. For example, the sentences "Ned loves Jody" and "Jody is loved by Ned" convey the same meaning although one is active and the other is passive. According to the TG theory these two sentences are derived from the same underlying form. The underlying form is known as the deep structure and the syntactic structure derived from the deep structure using syntactic transformations is known as the surface structure [3].

Numerous of transforms that are apply not directly to sentences as a whole but to their constituent phrase structures which can be obtained using sentence parsers. Natural language watermarking techniques that embed information in the underlying structure of a sentence will be more robust than those that modify the surface representation of the sentence. There are two commonly used approaches from the machine translation field that are useful to natural language watermarking. One is parsing sentences in text into an intermediate representation, transforming this parse structure into a corresponding parse in target style using predetermined transfer rules, and realizing this parse as a sentence using natural language generation methods. Another approach is to use an Interlingua, a language-neutral canonical form which can represent all sentences that mean the "same" thing in the same way regardless of the stylistic conventions of text. Translation is done by parsing the sentence into the Interlingua and later performing generation to the target style using this representation [3].

4. THE PROPOSAL NATURAL WATERMARK TEXT TECHNIQUE

Natural language text watermarking, is a way of embedding the watermark into a text document, using the natural language mechanisms as a carrier, in such a way that, alterations are imperceptible to the readers and the embedded information is robust against possible attacks. All the previous mentioned methods for watermarking techniques embed the watermark in either the modified layout or format of a text or use text itself with addition of natural language processing and tools. By tacking into consideration the difficulties of natural language text, and needs for finding a way to use spectral methods in natural language text. The proposal technique for natural language text watermarking using the spectrum method is implemented. In this section, the proposal natural language watermark technique for using the spectrum is introduced in subsection 4.1, and a test example for the proposal technique is introduced in subsection 4.2.

4.1 ALGORITHM FOR THE PROPOSAL NATURAL LANGUAGE TECHNIQUE

With idea of using spectral method as a means for natural language txt watermarking technique, to embed a watermark into the natural language txt, by using

random number generator as a secret key for determination of words to carries the watermark followed by applying FFT to the determined words. The proposal technique is implemented using matlab ver7 as a programming language the algorithms of random number generator, embedding and detecting is restricted in the bellow sub sections.

4.1.1 RANDOM NUMBER GENERATOR

Input: (p) prime number, (k) bits number of the watermark, period length, ($l = n$), a, b, r_0

Output: ($r_0, r_1, ..., r_{k-1}$)

Process:

Step1: Initialization: Input r_0, a, b, n and k , $j \leftarrow 1$

Step2: Compute $r_j \leftarrow (ar_{j-1} + b)(\text{mod}\, n)$

Step3: $r_i = r_i (\text{mod}\ numberofletter\ \text{int}\ heusedlanguage)$, and print r_j

Step4: increase j: $j \leftarrow j + 1$, If $j \geq k$, then go to step 5, else go to step 2

Step 5: End

4.1.2 PROPOSAL EMBEDDING ALGORITHM

Input: watermark, text file

Output: Stego-cover carrier text.

Process:

Step1: Convert the input watermark into bits ($mbit_i$).

Step 2: Use a random number generator which initialized by a prime number (p) to generate (k) numbers ($r_0, r_1, ..., r_{k-1}$)

Step 3: Repeat until the end of cover "txt" file

Step3.1: $A(w_i)$ is the ASCII number corresponding to the word of the text in the position, $r_i (\text{mod}\, p)$

Step3.2: $fft(A(w_i))$ is the result of Applying the Fast Fourier Transform to $A(w_i)$

Step 3.3: $real(fft(A(w_i)))$ is the real part of $fft(A(w_i))$

Step3.4: E_i is the result of embedding, $mbit_i$ into the LSBs of $real(fft(A(w_i)))$

Step3.5: $ifft(E_i)$ is the result of applying the Inverse Fast Fourier Transform to the E_i

Step3.6: $Ch(E_i)$ is character of E_i

Step 4: End

4.1.2 PROPOSAL DETECTING ALGORITHM

Input: Stego-cover carrier text.

Output: watermark

Process:

Step1: Use a random number generator which initialized by a prime number (p) to generate (k) numbers ($r_0, r_1, ..., r_{k-1}$)

Step2: Do until the end of stego-cover file

Step2.1: $A(S_i)$ is the ASCII number corresponding to the word of the stego-cover, in the position $r_i (\text{mod}\, p)$

Step2.2: $mbit_i$ is the LSB of $A(S_i)$

Step2.3: Convert each seven ($mbit_i$) into a letters "the watermark letters which represents its words"

Step3: End

4.2 TEST EXAMPLE

The above algorithms for the proposal watermark technique is tested where, the watermark is {holder}, and this paper as a cover-carrier. In bellow subsection is the results of implementations.

4.2.1 PROPOSAL EMBEDDING ALGORITHM

Input: {holder}, this paper is used as a cover-carrier

Output: the watermark paper

Process:

Step 1: Convert the input secret text information into bits ($mbit_i$).

{holder} $\rightarrow$ {1101000, 1101111, 1101100, 1100100, 1100101, 1110010}

Step 2: Use a random number generator which initialized by a prime number (5) to generate (42) random numbers ($r_0, r_1, ..., r_{k-1}$)

{r0=5, a=11, b=73, n=1399, k=42} $\rightarrow$ {5, 128, 82,975, 1005, 1335,768,127,71,854,1073,684, 602, 1099,970, 950,730,1108,1069,640,118,1371,1164,286,421,507,54, 667,415,441, 727, 1075, 706,844,963, 873, 1282,185, 709, 877, 1326,669}

Step 3: Repeat until the end of cover "txt" file

Step3.1: $A(w_i)$ is the ASCII number corresponding to the word in the position, $r_i (\text{mod}\, p)$

$\{ A(w_1) \} \rightarrow$ {87 97 116 101 114 109 97 114 107 105 110 103}

Step3.2: $fft(A(w_i))$ is the result of Applying the FFT to first letter of $A(w_i)$

$\{ fft(A(w_1)) \} \rightarrow$ {1.2600, 97 116 101 114 109 97 114 107 105 110 103 }

Step3.3: $real(fft(A(w_i)))$ is the real part of $fft(A(w_i))$

$\{real(fft(A(w_i)))\} \rightarrow$ {1260, 97 116 101 114 109 97 114 107 105 110 103}

Step3.4: E_i is the result of embedding, $mbit_i(0)$ into the LSBs of $real(fft(A(w_i)))$

$\{E_1\} \rightarrow$ {1260, 97 116 101 114 109 97 114 107 105 110 103}

Step3.5: $ifft(E_i)$ is the result of applying the Inverse Fast Fourier Transform to the E_i

$\{ifft(E_1)\} \rightarrow$ {87 97 116 101 114 109 97 114 107 105 110 103}

Step3.6: $Ch(E_i)$ is character of E_i

$\{Ch(E_1)\} \rightarrow$ {Watermarking}

Step 4: End

4.2.2 PROPOSAL DETECTING ALGORITHM

Input: the stego_carrier
Output: {holder}

Process:
Step1: Use a random number generator which initialized by a prime number (5) to generate (42) random numbers $(r_0, r_1, ..., r_{k-1})$

{r0=5, a=11, b=73, n=1399, k=42} → {5, 128, 82,768, 127,71,854,1073, 84,602,1099,970,950,730,1108,1069, 640,118,1371,1164,286,421,507,54,667,415,441, 727, 1075,706,844,963,873,1282,185,709,877,1326,669}

Step 2: Repeat until the end of stego-cover file

Step2.1: $A(S_i)$ *is the ASCII number corresponding to the word of the stego-cover, in the position* $r_i \pmod p$

$\{A(S_i)\} \rightarrow$ {87 97 116 101 114 109 97 114 107 105 110 103}

Step2.2: $mbit_i$ is the LSB of $A(S_i)$

{0} → {87 97 116 101 114 109 97 114 107 105 110 103}

Step2.3: Convert each seven $(mbit_i)$ into a letters "the watermark letters which represents its words"

{1101000, 1101111, 1101100, 1100100, 1100101, 1110010} → {Holder}

Step3: End

5. SUMMARY AND CONCLUSIONS

The proposal natural language text watermarking technique using spectrum method is used for intellectual property rights of digital text content. All the previous methods for natural language text watermarking, either attempts to alter the appearance of text elements, such as lines, words, characters, or attempts to alter the semantic and/or syntactic structure of sentences. Also natural language watermarking differs from image, video, or even software watermarking in that the watermark is embedded in the text, and is much harder to embed. Otherwise, the same principles are applied: the watermark should be robust, unpredictable to anybody but the author/owner of the text, and easily produced by the watermarking software.

In the proposal method a text which represents cover-carrier is spilt into words. A random number generator is used as secret key for determine the selected words for the watermark embedding positions. The FFT is applied to the ASCII number corresponding to each selected word, followed by extracting its real part. The watermark bits are embedding in the LSB's of the extracted real part. Then the IFFT is applied to the result.

The result txt of the embedding process is identical to the input one. Also only the user who knows the secret key can determined the watermark. All the methods that applied for images can be applied for natural language text such as, LSB's, DCT, and FFT. For the used random number generation the input prime number, a, b, should be chosen carefully.

REFERENCES

[1] Chaelynne M. Wolak, "Digital Watermarking", *School of Computer and Information Sciences Nova Southeastern University*, October 2000.

[2] Christine I. Podilchuk, and Edward J. Delp, "Digital watermarking: algorithms and Techniques", *IEEE Signal Processing Magazine*, JULY 2001.

[3] Mercan T. , Edward J. and Taskiran E. , "Natural Language Watermarking", *Purdue University, West Lafayette, Indiana*, 47907.

[4] M. Atallah, C. McDonough, S. Nirenburg, and V. Raskin, "Natural Language Processing for Information Assurance and Security: An Overview and Implementations," *Proceedings 9th ACM/SIGSAC New Security Paradigms Workshop*, September, 2000, Cork, Ireland, pp. 51–65.