L-021

電子透かしを用いた著作権侵害防止システム

A Digital Watermark System for Preventing Piracy

礒部 博行　　吉冨 康成
Hiroyuki Isobe　　Yasunari Yoshitomi

1．緒言

著作権保護技術には直接的防止と間接的防止の二種類があり、端末指定などの利用制限を施し、料金回収に重きをおくものが直接的防止であり、コンテンツの普及促進と著作権保護の両立を図るものが間接的防止である。本報では電子透かしを用いた間接的防止システムを提案する。

デジタルコンテンツの著作権を保護するため電子透かし技術が注目され、様々な研究が行われている[1]。しかし電子文書を対象とする電子透かしの研究開発は少ない。文字コードは１ビットでも変わるとその文字の意味を保持出来ない。このため、文書を画像として取り扱った電子透かしが研究されてきた[2]。著者らは、冗長性を付与することによる、文書を対象とした透かし埋め込みの方法を提案した[3]。本報では、既報[3]を発展させた著作権侵害防止システムについて述べる。

2．システム概要

システムの概要を図１に示す。本システムは透かし埋め込み暗号化部、表示部、ネット検索部で構成される。透かし埋め込み暗号化部は、配信する多様なコンテンツに電子透かしとして著作権情報などを埋め込むと共に、ファイルを暗号化する機能を有する。透かしを埋め込まれたコンテンツを暗号化しているため、表示部を用いて複号化し、透かしを検出して、閲覧を可能にする。配信されたコンテンツが不正掲載された場合、ネット検索部を用いて不正掲載を発見する。

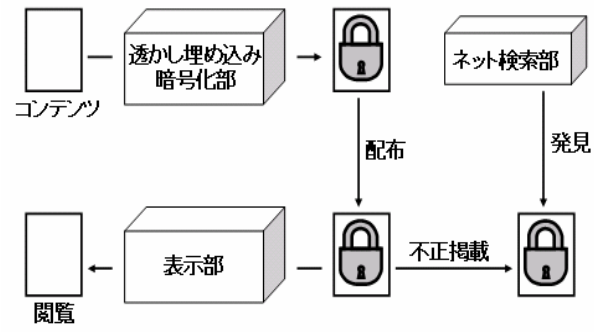

図.1　システムの概要

3．電子透かし埋め込み法

電子透かしの埋め込みは、通常、データの冗長性を利用して行われるため、冗長性の少ないコンテンツへの透かし埋め込みは困難である。文字コードには冗長性がないため、透かし埋め込みが困難だとされている。本法では、ビットを付加し、そのビット列を利用することで電子透かし埋め込みを可能にした（図２）。

付加するビットはバイナリーコード３４バイトに対して３４バイトとする。

4．暗号化

図３に透かし埋め込み暗号化部の概要を示す。暗号化には置換と秘密鍵との排他的論理和を用いる。暗号化するファイルをバイナリーとして先頭から３４バイトずつ読み込んでいく。これに対し透かし情報は３４バイトの文字列とする。置換と排他的論理和を施す単位は３２ビットとし、２バイトのバイナリーコードと２バイトの透かし情報を要素数３２の配列に格納し、置換、秘密鍵との排他的論理和を施す。このようにして得られた暗号コードをファイル保存する。作成されたファイルは暗号化されているため、復号と透かし検出を行い、冗長ビットを除いて表示する。

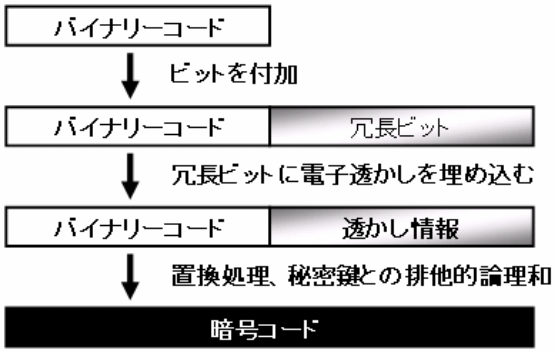

図.2　電子透かし埋め込みと暗号化の処理フロー

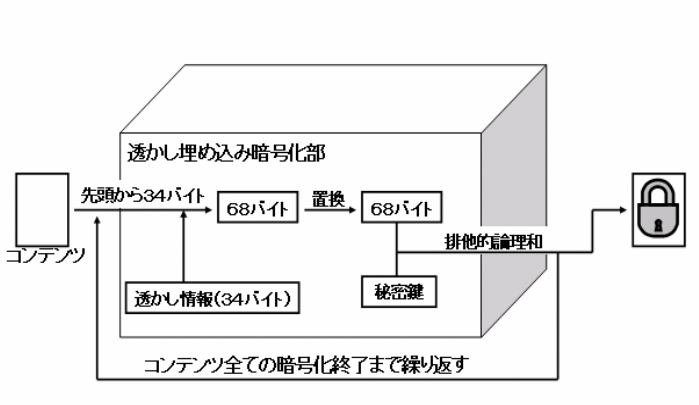

図.3　透かし埋め込み暗号化部

5．表示部

図４に表示部の概要を示す。表示部では、暗号化されたファイルを復号化し、透かし情報を抽出した後、平文を表示させる。本システムは多様な形式のファイルを対象とするため、ファイルの形式に対応したアプリケーションを利用して表示を行う。

6．ユーザー権限の設定

コンテンツの閲覧に関して、ユーザーによってその権限を制限する必要がある。印刷の制限や別名保存の禁止、コピー＆ペーストの禁止などがこれにあたる。これらのセキュリティ設定も既存のアプリケーションを利用する（図５）。以下、Microsoft Word （ doc ファイル）を例に、説明する。

Microsoft office 2003 から搭載された機能に IRM がある。これは Information Rights Management の略称で、コンテンツのセキュリティをサポートする機能である。配布するファイルが Microsoft office のファイルである場合、セキュリティ制御にはこの IRM を利用する。Microsoft Word では、IRM により以下の三段階のセキュリティ設定を施すことが可能である。

レベル１：フルコントロール
レベル２：コンテンツの表示、変更、コピーは可能
　　印刷は不可能
レベル３：表示のみ可能

Word ファイルを配布する場合、ユーザーに応じてこれらのセキュリティ設定を行ったファイルに電子透かしを埋め込み暗号化したものを配布する。

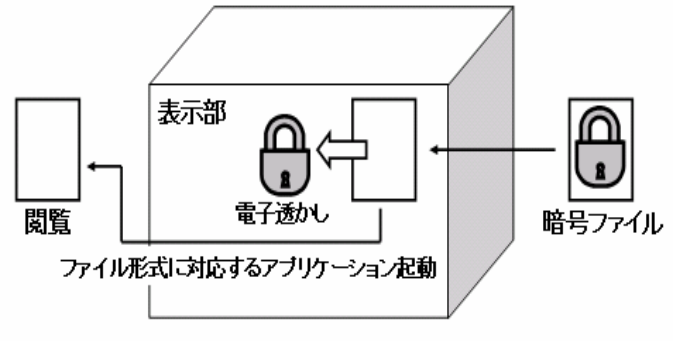

図.4　表示部

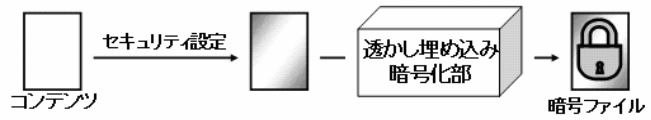

図.5　セキュリティ設定

7．対応するファイル形式

表示に既存アプリケーションを用いているため、セキュリティ設定の機能が付属していることが求められる。利用できるファイル形式は doc、xls、ppt、pdf である。セキュリティの設定を既存のアプリケーションに依存しない方法の実現は今後の課題である。

8．ネット検索部

悪意ある第三者によるコンテンツのインターネット上の不正掲載を発見するためにネット検索部を用いる。

検索部は起点となる URL の HTML 文書からリンク情報をキューに格納していくと同時に、指定した属性のファイルをダウンロードしていく。ダウンロードしたファイルに対し、透かし検出を行う。リンクを辿っていく深さの設定も可能である。

9．適用例

電子透かしとして「著作権　礒部博行」を埋め込んで暗号化したファイル“ test.doc ”をウェブページにリンクし、ネット検索部によりファイルを取得し、透かしを検出する実験を行った。

index.html を起点ページに設定し、test1.html、test2.html、test3.html へのリンクを貼った。test1.html には test2.html と test3.html へのリンクを貼り、test2.html には test3.html へのリンクを貼った。ファイルは test3.html にリンクした（図６）。またそれぞれの html ファイルは各々異なったサーバ上に置いた。

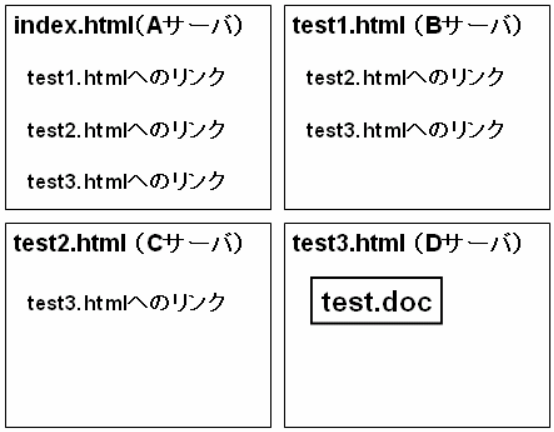

図.6　実験環境

結果、正常にファイルをダウンロードし、透かし情報を検出することが出来た。

10．結言

本報では、コンテンツにビットを付加し、そこへ電子透かしを埋め込む方法を用いることで、電子透かしを用いた間接的な著作権侵害防止システムを構築した。

本研究では、暗号化に置換と秘密鍵との排他的論理和を用いているが、今後はより強固な暗号化法の適用を検討する。

[参考文献]
[1]画像電子学会 編：電子透かし技術、東京電機大学出版局、(2004).
[2]松井甲子雄：文書画像への電子透かし、画像電子学会誌、vol.31、pp609-615(2002).
[3]礒部博行、吉冨康成：電子透かし埋め込み機能を有する文書エディタの開発、電子情報通信学会総合大会講演論文集、pp.183、(2006).