修士論文要旨

電子透かしパリティを用いた著作権侵害防止システム

（知能情報システム学）　礒部 博行

１．緒言

インターネットの急速な普及によって、コンピュータネットワークという情報を流通させる新しい手段が登場した。デジタルコンテンツの長所は、迅速にかつ大量に複製ができ劣化しない点や、瞬時に遠くへ、また同時に多数へ容易に伝達できる点である。これにより近年では、音楽や書籍をデジタルコンテンツとして、オンライン配信する方式が一般的になりつつある。しかしデジタルコンテンツの長所である、複製が容易である点が、逆に違法コピーなどの著作権侵害を助長することになっている。こういったオンライン配信が一般的になるにつれ、配信するコンテンツの著作権の保護が非常に重要になっている。

デジタルコンテンツの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る。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、これに対して、コンテンツの普及促進と著作権保護の両立を図る間接的防止法もあり、その一つの手段として電子透かしが用いられている。本報では電子透かしの概念を拡張した間接的防止システムを提案する。

２．電子透かし

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]。これは、オリジナルデータの情報をわずかに変化され、著作権情報などのデータを透かしとして埋め込み、その埋め込まれたデータを流通させる技術である。音楽や画像を対象とした研究開発は、すでに実用化のレベルまで達しているが、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、パリティビットのような冗長性を付与することにより、文書を対象とした透かし埋め込みの方法を提案した[3]。パリティビットとは、コンピュータの通信において、与えられた二進数に対して全体の奇偶性を保つために与えられる一桁の二進数(つまり 0 か 1)であり、最も単純な誤り検出符号である。このようにその情報自体に影響を与えない冗長性のあるビット列を透かしを埋め込むために付加し、情報自体に冗長性を持たせた。この方式は「情報に内存する冗長性などの属性を利用する」というこれまでの電子透かしに関する既成概念におさまらない。既報の研究[3]ではこの方法を用い、電子透かし埋め込み機能を有する、テキスト形式のファイルを対象としたエディタを開発した。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。

３．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は暗号化されているため、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こ

とが出来る。

4．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）。付加したビット列を「電子透かしパリティビット列」と呼ぶことにする。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。

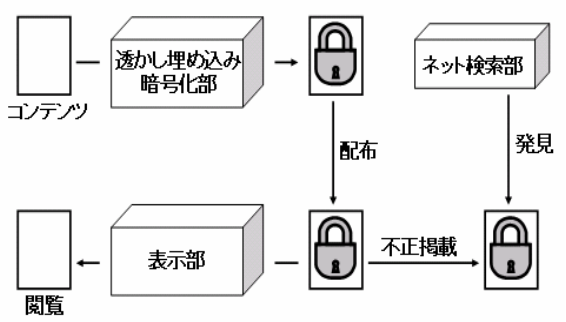

図.1　システムの概要

5．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 Triple　DES 暗号[4]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を３４バイトの文字列とする。Triple DES を施す単位は６４ビットとし、４バイトのバイナリーコードと４バイトの透かし情報を一つの単位そして Triple DES を施していく。これから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。

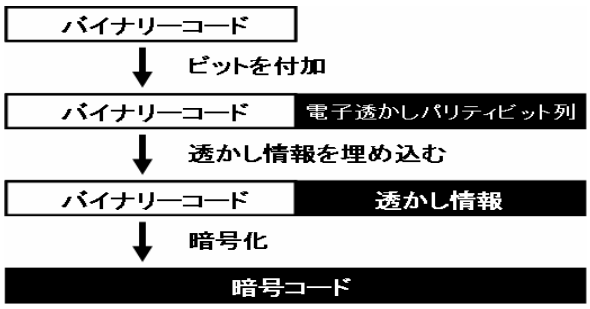

図.2　電子透かし埋め込みと暗号化処理フロー

6．Triple DES について

DES では平文の６４ビットブロックに対して演算を行う。最初の並べ替えの後、ブロックは右と左の３２ビットずつに分けられる。そして１６回にわたる同じ演算操作が行われる。この演算操作一回分を関数 f で表し、データは鍵と組み合わされる。１６回目のラウンドが終わったら、左右の各半分は結合され、最終的な並べ替え（最初の並べ替えを逆にする）が行われてアルゴリズム終了となる。

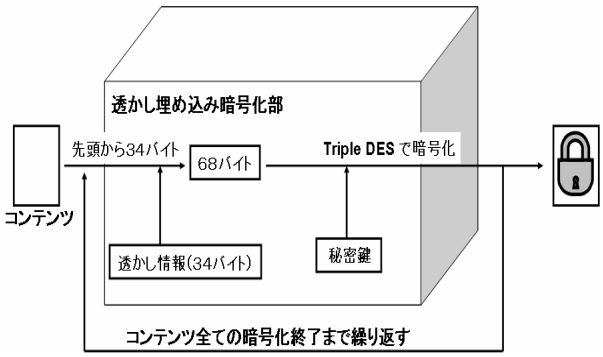

図.3　透かし埋め込み暗号化部

各ラウンドで、鍵ビットはシフトされ、鍵の５６ビットから４８ビットが選ばれる。データの右半分が拡大並べ替えによって４８ビットに拡大され、シフトして並び替えられた４８ビットの鍵と排他的論理和で組み合わされ、S ボックス置換により３２ビットが出力され、この結果を P ボックス置換する。この４つの演算操作が関数 f を構成する。関数 f の出力は、左半分の結果と排他的論理和によって組み合わされ、この演算結果が新しい右半分になる。もとの右半分が新し

い左半分となる。この操作が 16 回繰り返され、DES のラウンドとなる。DES の１ラウンドの概要を図４に示す。Bi を i 回目の繰り返しの結果とし、Li と Ri が Bi のそれぞれ左半分と右半分とし、Ki を i ラウンド目の 48 ビット鍵だとし、f を置換と並べ替えと鍵との排他的論理和をすべて行う関数とすると、1 ラウンドは次のように表せる。

Li = Ri-1

Ri = Li-1 $\oplus$ f(Ri-1 , Ki)

Triple DES はこの DES を３回施す暗号化法である。鍵Ａで暗号化したものを、鍵Ｂで複号化し、さらに鍵Ｃで暗号化したものを出力とする。復号の際は鍵Ｃで複号化したものを、鍵Ｂで暗号化し、鍵Ａで複号化する。

ファイルに透かし情報として「著作権　礒部　博行」を埋め込んで暗号化した例を図 5～6 に示す。

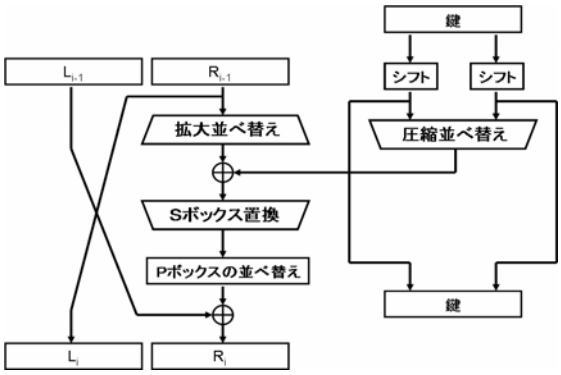

図.４　DES の１ラウンド[4]

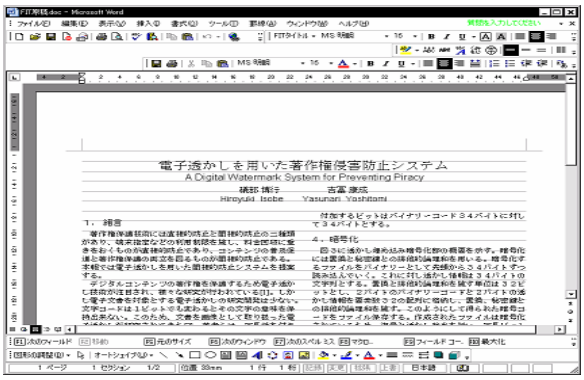

図.５　暗号化前のファイル（Word）

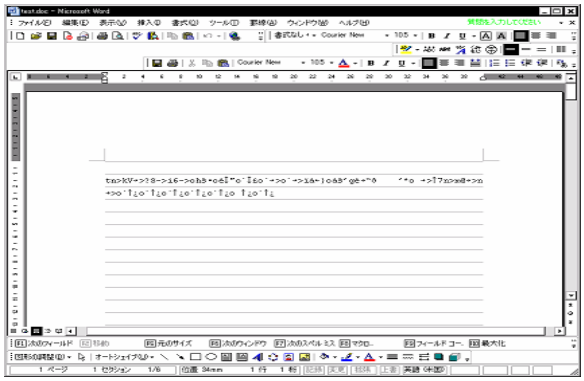

図.６　暗号化後のファイル（Word）

7 ． 表示部

図７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。

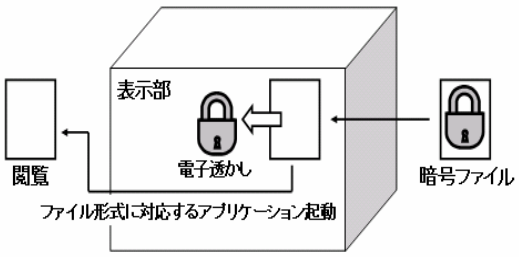

図.7　表示部

8 ． 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 8)。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：表示、変更、コピー可能、印刷不可能
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。

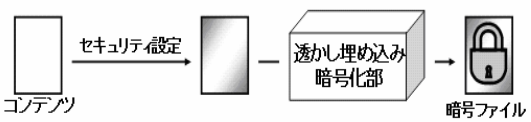

図.8　セキュリティ設定

9 ． 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。このため現在利用できるファイル形式は doc、xls、ppt、pdf である。既存のアプリケーションにセキュリティの設定を依存しない方法の実現は今後の課題である。

10 ． 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。

11 ． 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。またそれぞれの html ファイルは学内の各々異なったサーバ上に置いた。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。次に、同じファイル” test.doc ”を学外のサーバ上に置き、クローラする実験を行った。起点ＵＲＬを Yahoo　JAPAN 内の”http://dir.yahoo.co.jp/Regional/Japanese_Regional/Japanese_Regions/Kinki/Osaka/Entertainment/Music/Jazz/Artists/”にし、そこから二階層下のページに対象のファイルをリンクした。結果、クローラページ数 429、A タグチェック数 11490、ダウンロードファイル数 2 となり、対象のファイルのダウンロード及び透かし検出を正常に行うことが出来た。

12 ． 結言

コンテンツにビットを付加し、そこへ透かし情報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。

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).
[4]Bruce Schneier : 暗号技術大全、ソフトバンクパブリッシング株式会社、(2003).