意味保存型の情報ハイディング —日本語文書への適用—

中川 裕志* 三瓶 光司† 松本 勉‡ 村瀬 一朗§

1 はじめに

最近、注目されている情報ハイディングは，元データの品質を落とすことなくそこに情報を隠蔽しておき，必要に応じてそれを抽出する技術である．この情報ハイディングは，主として画像，音声データに対する分野で研究が進んでいる．一方，テキストデータに対するものは事例が少なく，現在有効な手法が模索，研究されている．本稿では，我々が開発した、ある言語表現を意味を変えずに別の表現の置換による情報ハイディング方式を提案する．また，今回開発したシステムの評価についても報告する．

なお、類似の技術である暗号と比較すると、暗号は情報の内容を隠す技術であるのに対して、情報ハイディングは情報の存在そのものを隠す技術である。

2 意味保存の情報ハイディング

2.1 基本的アイデア

一般に同一の内容であっても複数の表現が存在することを利用する情報ハイディングについて検討する．例えば，「意味を変えない置き換え」という文に対しては，「意味を変化させない置き換え」，「意味を変えない置換」，「意味を変化させない置換」といった，同一の意味を持つ文が存在する．仮に，「変えない」と「置き換え」がビット情報０を，「変化させない」と「置換」がビット情報１に対応しているとすれば，これら意味の同一な４つの文はそれぞれ，００，１０，０１，１１という情報を表わしていることになる．このような表現の置換を文書全体に対して行えば，文書の品質が損なわれず，かつ，存在を検出されにくい秘匿情報が埋め込まれたテキストが生成できる．

2.2 表現の置換

2.2.1 一般的な置換

我々が普段使っている言語には，同一の内容を表現するものであっても，多種多様な表現が存在する．前にあげた，「意味を変えない置き換え」のような，各語を同一の意味を持つ語で置き換えるようなものもあれば，語順を変えるもの，全く違う構文，語で同一の内容を表現するものなど様々である．我々のシステムの対象となるものは文書であるので，まず文書における表現の置き換えとして以下の方法について考察する．

- 並列句の順番の置き換え
- 受動態から能動態へ，能動態から受動態へ
- 同義語，類義語の利用
- 送り仮名，仮名⇔漢字等の表記揺れを利用する
- 冗長である部分を付加，削除する

上記のもののうち，はじめの２つは正確な構文解析または意味解析が必要である．これらの処理は，処理時間がかかる上に曖昧さが残ってしまうため，現在のところでは有効な手法であるとは言えない．また，これら構文解析を用いる置き換えの手法は，文節や文を単位とするので，同義語等を用いた場合と比べ隠蔽できる情報量が少ない．したがって我々のシステムでは，文の構造を変えるのではなく，語や語句の置き換えによって情報を隠蔽する方式をとることにする．

2.2.2 品詞の種類による特徴

置換の対象となる品詞の種類によって，同義語への置き換えは，さらに細かく分類することができる．例えば，普通名詞であれば置き換えの際，語の活用について考慮する必要はないが，複合名詞化しているものは，単純に置き換えると文法が崩れる恐れがある．また，動詞は活用形を考慮して置き換えねばならない．これら品詞の種別による表現の置き換えの特徴を示す．

○ 名詞 (サ変名詞[1]を除く)
前方および後方に名詞が連接する場合を除き，文法的制限はない場合が多い．しかし意味的に完全に等しい語が存在する場合は少なく，特定の条件下において同じ意味を持つ場合や，一方がもう一方を包括する意味を持つことが多いため，一方向の変換になることが多い．例としては「文書」と「テキスト」．また，一般的に用いられる名詞であっても，特定の分野においては特殊な意味を持つ場合があるため注意が必要である．例えば，「表示」は計算機分野ではディスプレイへの表示であり「掲示」や「表現」とは置き換えられない．

○ サ変名詞
サ変名詞単体で文中に出現する場合は普通の名詞と同様の特徴をもつが，「サ変名詞＋する」の場合には動詞として振る舞うため，この場合は動詞の置換と同様，「する」の部分の活用形を考慮した置換を行わねばならない．また，「～を＋サ変名詞＋する＋こと」のようにサ変名詞を含む名詞句が存在する場合は，この部分を「～の＋サ変名詞」とする置き換えが可能である．

○ 動詞

*東京大学情報基盤センター，
†横浜国立大学大学院工学研究科電子情報工学専攻，
‡横浜国立大学大学院工学研究科人工環境システム学専攻，
§株式会社三菱総合研究所，

[1]後方に“する”が続くことで動詞を形成する名詞．“置換”など．

動詞の置換に当たってもっとも考慮しなければならないことは，活用形の変化である．例えば,「できる」という語とそれに対する置換候補「可能だ[2]」を考えた場合，前者は終止形，連体形とも「できる」であるが，後者は終止形が「可能だ」，連体形が「可能な」となる．このように置換対象とその置換候補では必ずしも活用形が一致するわけではないので注意が必要である．
また，サ変名詞が名詞句を形成する場合と同様,「～を＋動詞＋こと」は，これと同様の意味を持つ名詞を用いて,「～の＋名詞」とすることが可能である．

2.2.3 置換条件の設定

表現の置換において，最も考慮しなければならないことは，意味および文法性を損なわないことである．そこで，形態素解析システム茶筌 [?] を用い，これらのことを実現するために，置換可能な際の条件をあらかじめ設定するという方式をとる．
一般に，置き換えられた表現に近い語ほど，置き換えによって受ける影響が大きい．我々はこのことを考慮し，置換の対象となる表現の周囲の語によって置換可能かどうかの判定を行うような条件を設けた．形態素解析によって得られる情報は，品詞の種別やその活用形であるため，条件を構成する要素として，置換の対象となる語からの距離(形態素数)と，語そのもの，品詞名を選択した．条件は論理式に近い形式で記述され，辞書に登録される．条件は基本的に,「位置特定子」+「==または!=」+「品詞識別子または文字列」のように記述される．位置特定子とは図1に表わしたものであり，置き換え可能かどうかを判定される語を Self，それ以前に出現する語を Self から近い順に Pre1, Pre2, …, Pre5, Self 以降に出現する語を近い順に Post1, Post2, …, Post5 といった名前をつけたものである．また，品詞識別子とは，名詞，動詞，形容詞等にそれぞれ別名をつけたものであり，これらであれば，Noun, Verb, Adj という風になる．また，複数の条件を ||, &&でつなげることもできる．例えば「直前が名詞でなく，直後が動詞でないならば置き換え可能」という条件を記述すると，
(Pre1!=Noun)&&(Post1!=Verb)　となる．

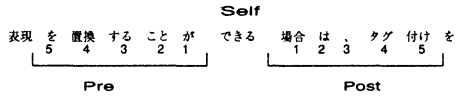

図 1: 位置特定子

2.3 システム概要

まず、以下の二つの用語を定義しておく．

カバーテキスト 秘匿情報を埋め込む対象となるテキスト

ステゴテキスト カバーテキストに秘匿情報を埋め込んで変換したテキスト

本システムの概要は図2のようになっている．処理の流れを以下に述べる．

- カバーテキスト C を形態素解析によって各形態素に分解する．
- 文書変換辞書 D の構造は図 2に示すように，置換対象となる語と，それに対する置換候補，置換の際の条件を保持する．
- 形態素解析されたテキスト C と，辞書 D の登録内容との比較を行い，D 中に存在する表現があれば，置換条件による判定を行う．置き換えが可能であった場合は，置き換えが可能である語と共に，それに対する候補もタグ付けがなされテキスト C ' として出力される．

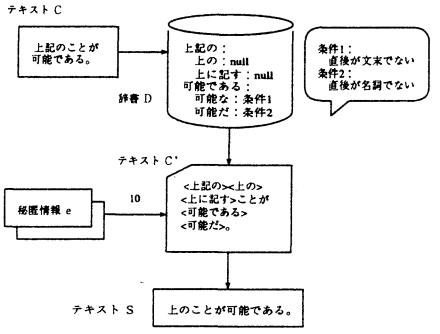

図 2: 辞書の構造

- テキスト C' は HTML 形式に変換する専用のフィルタをかけることで，どのように置き換えられるかが Web ブラウザで確認できるようになっており，C' 中の置き換えに不適切な部分があった場合，人手でそれを修正することが可能である．
- 秘匿情報 e はバイナリストリングに変換され，そのバイナリストリングと C' のタグ情報にしたがって表現の置換が行われる．その結果生成されるのがステゴテキスト S である．
- 秘匿情報の抽出はテキスト C' とテキスト S の比較によって行われる．比較によってどの個所が置き換わっているかを特定し，情報隠蔽の際に適応した情報埋め込みパターンを用いて情報の抽出を行う．

図 3に秘匿情報が埋め込まれたステゴテキストの例を示す．

3 実証実験

本システムの有効性を実証するため，文書作成に携わる業務をしている被験者複数名に対して，以下の 2 種類の実験を行った．

- カバーテキストと，それから生成されたステゴテキストの 2 つの文書を比較し，その 2 つの間で日本語として文法的，意味的に等しいかを検討してもらう．(以下，比較実験と呼ぶ．)
- ステゴテキストのみを査読させ，その中で使用されている表現が，日本語として正しく，かつ専門文書としての内容に即しているかを検討してもらう．(以下，査読実験と呼ぶ．)

ネットワーク基盤の発達等 [によって]，電子的にやり取りされる情報量が目覚ましく増加している．それに伴い，電子化されたコンテンツに対する著作権保護が大きな問題となっている．[そのような] 問題を解決する一つの方法として注目，研究されているのが情報ハイディングである．しかし，[これまで] の情報ハイディングは，画像，音声などに対するものがほとんどであり，テキストを対象にしたものでも，文字間や行間なを微妙に変化させて情報の隠蔽を行うなど，実質的には画像的な扱いをするものがほとんどであった．

図 3: 生成されたステゴテキストの例

以降では各実験の詳細について述べる．

3.1 比較実験

3.1.1 実験概要

比較実験は，生成されたステゴテキストが，もとのカバーテキストと同一の意味を持っているかを検証することを目的とする．文書の種類やサイズの，辞書の内容による影響についても調査するため，カバーテキストとして，5KB 前後のサイズをもつソフトウェアのマニュアル，使用許諾文書をそれぞれ 2 種類ずつと，25KB，50KB のサイズのマニュアルを用いた．文書変換辞書は，一般的な文書に適応するための辞書 (以下，一般辞書)，対象となるカバーテキスト中の専門用語も置換の対象とするよう，特定のカバーテキスト用にカスタマイズされた辞書 (以下，専門辞書)，一般辞書の登録内容を削除して置換対象を減らした辞書の 3 種類を用意した．これらを組み合わせ，12 種類のステゴテキストを生成した．

表 1: 実験に使用したステゴテキスト

ステゴテキスト名	カバーテキスト名	使用した辞書
MS1-t	Manual-Small-1	Technical
MS1-c1	Manual-Small-1	Common1
MS2-t	Manual-Small-2	Technical
MS2-c1	Manual-Small-2	Common1
LS1-t	Licence-Small-1	Technical
LS1-c1	Licence-Small-1	Common1
LS2-t	Licence-Small-2	Technical
LS2-c1	Licence-Small-2	Common1
MM1-c1	Manual-Middle-1	Common1
MM2-c1	Manual-Middle-2	Common1
ML1-c1	Manual-Large-1	Common1
ML2-c1	Manual-Large-2	Common1
MM1-c2	Manual-Middle-1	Common2
MM2-c2	Manual-Middle-2	Common2

カバーテキスト名：文書種別 — サイズ — 識別子
文書種別：Manual=マニュアル，Licenece=使用許諾文書
文書サイズ：Small=5KB，Middle=25KB，Large=50KB
辞書名：Common1=一般辞書，Technical=専門辞書
Common2=登録内容の少ない一般辞書

表 1に示すステゴテキストに対し，各 2 人の被験者にカバーテキスト—ステゴテキストの比較を行ってもらった．制限時間などの制限事項は特に設定しなかった．

表 2: 比較実験の結果

[1]	[2]	[3]	[4]	[5]	[6]	[7]
MS1-t	50	48	23	1 0	4.3 % 0 %	3 5
MS1-c1	17	17	10	0 0	0 % 0 %	4 5
MS2-t	310	304	123	22 39	17.9 % 31.7 %	5 4
MS2-c1	37	32	16	3 4	18.8 % 25.0 %	5 2
LS1-t	76	50	30	1 0	3.3 % 0 %	5 5
LS1-c1	52	48	26	0 0	0 % 0 %	5 5
LS2-t	154	153	86	4 9	4.7 % 10.5 %	5 4
LS2-c1	39	32	15	0 8	0 % 53.3 %	5 1
MM1-c1	147	144	79	4 2	5.1 % 2.5 %	3 5
MM2-c1	154	152	83	8 15	9.6 % 18.1 %	5 5
ML1-c1	318	312	142	7 4	4.9 % 2.8 %	3 5
ML2-c1	229	224	120	16 19	13.3 % 15.8 %	5 4
MM1-c2	75	73	39	1 0	2.6 % 0.0 %	4 5
MM2-c2	79	72	42	5 8	11.9 % 19.0 %	5 5

[1]：ステゴテキスト名　[2]：置換可能個所　[3]：置換個所
[4]：不一致個所　[5]：不一致指摘個所　[6]：不一致指摘率
[7]：全体評価
(5：意味はほぼ同じ 3:全体の文意は同じ 1:同じ意味ではない)

3.1.2 実験結果

表 2に示される比較実験の結果について考察する．

- カバーテキストの種類
一般的な表現の置き換えによって，単純に文章としての意味を保存するという観点からは，使用許諾文書の方がマニュアルより，隠蔽情報量，生成されたステゴテキストの質の両方において優れていると言える．

- 辞書の登録内容
辞書の登録内容は，専門用語等，対象となる文書独特のものであっても置き換えるように登録してあったほうがよいと言える．

- 置換個所数
カバーテキストの長さに比例的であるが，単位長さあたりの置換個所数は使用する辞書の品質，カバーテキストの品質等によって変わってくる．

3.2 査読実験

3.2.1 実験概要

査読実験は，ステゴテキスト単体でみた場合，日本語の品質が維持され，かつ専門分野における文

表 3: 査読実験の結果

[1]	[2]	[3]	[4]	[5]	[6]
MS1-t	50	48	26	5 / 12 3 / 3	19.2 % 11.5 %
MS1-c1	17	17	10	4 / 14 0 / 0	40.0 % 0 %
MS2-t	310	304	151	83 / 98 13 / 20	55.0 % 8.6 %
MS2-c1	37	32	17	6 / 12 8 / 10	35.3 % 35.3 %
LS1-t	76	74	39	8 / 10 11 / 14	20.5 % 28.2 %
LS1-c1	52	48	26	1 / 3 2 / 5	3.8 % 7.7 %
LS2-t	154	153	67	9 / 12 28 / 34	13.4 % 41.8 %
LS2-c1	39	32	14	2 / 2 4 / 9	14.3 % 28.6 %
MM1-c1	147	144	71	48 / 52 2 / 6	67.6 % 2.8 %
MM2-c1	154	152	79	2 / 3 35 / 64	2.5 % 44.3 %
ML1-c1	318	312	164	91 / 118 4 / 7	55.5 % 2.4 %
ML2-c1	229	224	117	2 / 2 27 / 153	20.5 % 28.2 %
MM1-c2	75	73	28	18 / 19 0 / 0	64.3 % 0.0 %
MM2-c2	79	72	33	0 / 0 13 / 51	0.0 % 39.4 %

[1]: ステゴテキスト名　[2]: 置換可能個所
[3]: 置換個所　[4]: 不一致個所数
[5]: 問題指摘個所数 (変更分)/問題個所数 (全体) [6]: 問題指摘率

書としての正当性を保持しているかどうかを検証するための実験ある．比較実験で用いたカバーテキスト—辞書の組み合わせと同じ組合わせを用い，埋め込みデータだけを変えステゴテキストを生成した．それらのステゴテキストに対し，各文書あたり 2 人づつ文書の正当性を評価してもらった．

3.2.2 実験結果

表 3と 4に査読実験の結果を示す．

比較実験の結果と比べ，全体的に問題指摘個所が増加していることがあげられる．単純に，本実験の問題指摘率と比較実験の不一致指摘率を比較すると，全体の平均値で 14%程，専門辞書を用いたもの，一般辞書を用いたものはそれぞれ，18%，13%程度づつ値が増加している．これは，比較実験において，日本語としては意味が同一であると判定されたものでも，専門的な分野の文書としてみた場合には，意味が異なってくることによる．

また，表 3を見ると実際に置換えた個所以外にも，問題が指摘されている個所が多い．この原因として，置換えにより文脈の解釈が曖昧になる可能性があげられる．比較実験の際には，比較するカバーテキストがあったため，あらかじめ文脈はわかっていた．しかし，査読実験の場合には，基準となる文書がないため，文脈の解釈の仕方は査読者に委ねられる．複数存在する解釈のうち，カバーテキストと違う意味で解釈をすると，その後方などで意味のつながりが切れ，そこを問題点として指摘されることが起こりえる．マニュアルなどで，置換え個所以外での問題点の指摘が多いのは，マニュアルの方が使用許諾文書に比べ，前に述べたことを踏まえた上で次のことを述べると言った意味的な依存関係が多く存在するためであると考えられる．

表 3: 査読実験の結果 (主観的評価)

文書名	専門文書としての評価	日本語としての評価	総合評価
MS1-t	3 - 5	2 - 5	2 - 5
MS1-c1	3 - 5	3 - 5	3- 5
MS2-t	1 - 3	2 - 4	2 - 3
MS2-c1	3 - 3	3 - 3	4 - 3
LS1-t	4 - 3	5 - 4	4 - 3
LS1-c1	4 - 4	5 - 5	4 - 4
LS2-t	3 - 1	4 - 2	3 - 1
LS2-c1	5 - 4	5 - 4	5 - 4
MM1-c1	2 - 5	2 - 5	2 - 5
MM1-c1	5 - 2	5 - 3	5 - 2
ML1-c1	3 - 5	3 - 5	3 - 5
ML2-c1	3 - 3	3 - 4	3 - 3
MM1-c2	2 - 5	3 - 5	3 - 5
MM2-c2	5 - 2	5 - 2	5 - 2

5：意味はほぼ同じ 3:全体の文意は同じ 1:同じ意味ではない
なお，各欄の a - b は 1 人目が a，2 人目が b という評価をしたことを表す．

表 4に示す査読者側による全体評価は，比較実験に比べ問題指摘率が多い分，全体的に低下している．特に専門辞書を用いたものについては，比較実験の際には平均で 4.5 という非常に高い値であったのだが，査読実験においては 2.9 とかなり低下している．比較実験の結果に対する考察の際、専門用語も置換えの対象とした方が良いとの結果になったが，これは日本語としての意味の同一性だけを考慮した立場から導き出されたものであり，元のデータの品質を低下させないという情報ハイディングの前提に立つと，専門用語は置換えの対象としない方がよいということになる．

4 まとめ

我々が提案する意味を変えない置換えによる情報ハイディング方式は，評価実験などから，意味を保存し置換えることに成功していると言える．しかし，専門用語などの扱いなどによっては文書の品質が低下することがあるため，この扱いに対する研究が今後の課題となる．

5 謝辞

本研究は情報処理振興事業協会 (IPA) の情報セキュリティ関連事業 (平成 11 年度) 援助により行われました．本研究を進めるにあたって，御助言，御協力頂いた NTT ソフトウェアの若月秀氏，ジャストシステムの宮城裕氏に感謝致します．同じく御協力頂いた三菱総合研究所の川口修司氏，柏木健志氏に感謝致します．