秘密分散法を応用したソフトウェア電子透かし
—分散情報としてのバースマークの利用—

棚瀬 真臣 † 真野芳久 ‡
南山大学 数理情報研究科 数理情報専攻 † 南山大学 数理情報学部 情報通信学科 ‡

1 はじめに

近年、ソフトウェアにおける著作権侵害が大きな問題となっており、プロテクション技術が重要となってきている。ソフトウェアの盗用を防ぐことを目的としたプロテクション技術の例として、電子透かしとバースマークがある。

バースマークは、ソフトウェアから抽出した特徴あるいは、その特徴の一致をもってソフトウェア盗用の可能性を識別する技術である。電子透かしは、デジタルコンテンツ中に特定の情報を埋め込む技術のことであり、特にソフトウェアに対する電子透かしをソフトウェア電子透かしと呼ぶ。しかし、ソフトウェア電子透かしには、画像などへの電子透かしよりも電子透かしが発見されやすい、電子透かしを埋め込むことでソフトウェアの処理時間やサイズが大きくなる、などの欠点がある。以降はソフトウェア電子透かしを単に透かしと呼ぶ。

本研究では透かし情報の表現方法に着目し、秘密分散法を用いて 1 つのソフトウェアに数個の透かしを埋め込む状況でのサイズ増加量を改善する方法として、バースマークを利用する方法を提案する。

2 透かしへの秘密分散法の応用

本章では、秘密分散法を透かしに応用する方法を述べる。透かしに秘密分散法を用いることで、透かし情報を解読することが難しくなる。

2.1 秘密分散法

秘密分散法は、Shamir[1] と Blakley[2] によって、それぞれ独自に発表された暗号化方法である。秘密分散法では、秘密情報を複数の分散情報に分散する。また、決められた数片の分散情報を集めないと秘密情報は復元されない。

特に、秘密情報 S の分散情報 $W_1, W_2, ..., W_n$ が次の 2 条件を満たすとき (k, n) 完全秘密分散法という。

- 任意の k 個の分散情報から S が正しく復元できる。
- 任意の $k-1$ 個以下の分散情報からは S の情報が全く得られない。

(k, n) 完全秘密分散法において、任意の分散情報 W_j の情報量 $|W_j|$ は、秘密情報 S の情報量 $|S|$ に対して $|W_j| \geq |S|$ となることが知られている。

2.2 基本的なアイデアの概要

透かしではこれまで図 1 に示す埋め込み (Embed) 抽出 (Recognize) モデルが一般的に用いられている。

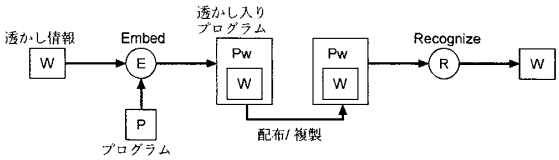

図 1 従来の透かし埋め込み抽出モデル

本研究では、秘密分散法を透かしに応用し図 2 に示すモデルを用いる。透かし埋め込みでは、まず秘密情報 S を n 個の分散情報 $W_1, W_2, ..., W_n$ に分散する。それらの分散情報を、透かし埋め込み機能 E でプログラム P に埋め込み、透かし入りプログラム P_w を生成する。また、P_w から透かし抽出機能 R で k 個の分散情報 $W_{j_1}, W_{j_2}, ..., W_{j_k}$ を抽出し、S を復元する。

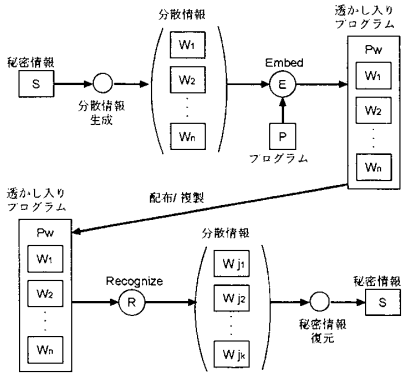

図 2 秘密分散法を応用した透かし埋め込み抽出モデル

ここで、プログラムサイズが埋め込み情報量の h 倍増えるとすると、透かしを n 個埋め込む場合のプログラムサイズの増加量は、「$n \times h \times$ 埋め込み情報量」となる。しかし、(k, n) 完全秘密分散法において、$|W_j| \geq |S|$ となることが知られている。結果として、分散情報 W_j を n 個埋め込んだ場合のプログラムサイズの増加量は $h \sum |W_j| \geq hn|S|$ となりサイズ増加量が増える。

3 分散情報としてのバースマーク

図 2 のモデルを使う場合のサイズ増加量を改善するために、透かしの一部を対象プログラムのバースマークで置き換える方法を述べる。

Software Watermarks based on Secret Sharing Scheme – Birthmarks used as Shares–
† TANASE, Masaomi: Gra. Program in Math. Sciences and Inf. Eng., Nanzan Univ. ‡ MANO, Yoshihisa: Dept. of Inf. and Telecomm. Eng., Nanzan Univ.

3.1 提案方法の概要

図3に示すように、1個の透かし W_i をバースマーク $BM(P)$ で置き換えるとする。$BM(P)$ で置き換えられた W_i は透かしとして埋め込む必要はなくなる。また、W_i の抽出はバースマークを抽出する。

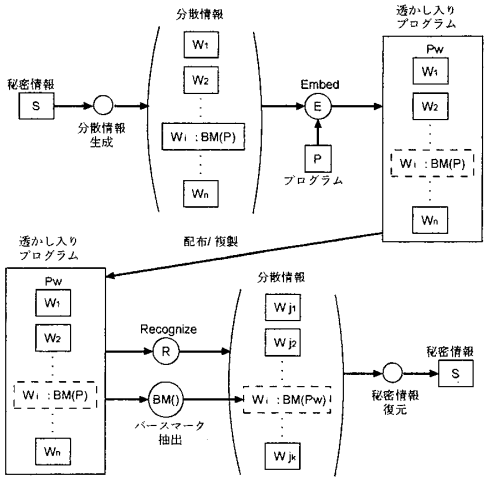

図 3 バースマーク利用の透かし埋め込み抽出モデル

問題点として、透かしを埋め込むことでバースマークが変わる可能性があることが挙げられる。透かし埋め込みの際はプログラム P から抽出したバースマーク $BM(P)$ を分散情報 W_i として用いるのに対して、透かし抽出の際は、透かし入りプログラム P_w から抽出したバースマーク $BM(P_w)$ を W_i として用いているため、$BM(P) = BM(P_w) = W_i$ である必要がある。バースマークを変えないで透かしを埋め込む簡単な方法として、透かしの埋め込み場所とバースマークの抽出場所を変える方法が挙げられる。

3.2 藤井らの (k,n) しきい値法 [3] を用いた構成法

藤井らの (k,n) しきい値法は、生成行列 G と、ベクトル U(秘密情報 S と乱数成分 R からなる) を用いた行列計算と排他的論理和で分散情報 W を生成する。

提案方法では、S と分散情報の一部として使うバースマーク $BM(P)$ から決まる R' を R の代用情報として用いる。この R' を用いて分散情報を生成することで、他の分散情報が定まる。また、本方法は $k-1$ 個のバースマークを分散情報として使うことが可能であり、サイズ増加量は最善で $h\{n-(k-1)\}|W_i|$ となる。

3.2.1 $(2,3)$ しきい値法での構成

秘密情報 S と代用情報 R' からなるベクトル U、および生成行列 G から分散情報 W_1 =$BM(P)$ となるような分散情報 W_1, W_2, W_3 を生成するとする。

$$(W_1, W_2, W_3) = (R', S)G$$

ここで仮に $W_1 = 101011, S = 111000$ として、分散情報 W_1 を生成する処理 $W_1 = UG_1$ から R' を求める。

また、W_1, S, R' はそれぞれ2個 $(n-1$ 個) に分割され、E は 2×2 $(n-1\times n-1)$ の単位行列となる。

$$(101,011) = (R'_1, R'_2, 111, 000)\left[\frac{E}{E}\right]$$

$$(101,011) = (R'_1, R'_2)\left[\ E\ \right] \oplus (111,000)\left[\ E\ \right]$$

$$(R'_1, R'_2) = (101,011) \oplus (111,000)$$

$$(R'_1, R'_2) = (010,011)$$

となり、S と分散情報 W_1 から R' が決まる。このようにして求めた R' を用いて分散情報を生成することで、分散情報 W_2, W_3 が定まる。

3.2.2 (k,n) しきい値法での構成

$k-1$ 個の分散情報 W、秘密情報 S と代用情報 R' からなるベクトル U、生成行列 G を以下のように定める。

$$W = (W_{i_1}, ..., W_{i_{k-1}}) = (BM_{i_1}(P), ..., BM_{i_{k-1}}(P))$$

$$U = (R'_{1,1}, ..., R'_{k-1,n-1}, S_1, ..., S_{n-1})$$

$$G = (G_{i_1}, .., G_{i_{k-1}})$$

分散情報を生成する処理は $W = UG$ と表すことができる。G の S に関係する部分を G_s、R' に関係する部分を G_r とすると

$$W = UG = U\left[\frac{G_r}{G_s}\right]$$

$$W = (R'_{1,1}, ..., R'_{k-1,n-1})G_r \oplus (S_1, ..., S_{n-1})G_s$$

$$W \oplus (S_1, ..., S_{n-1})G_s = (R'_{1,1}, ..., R'_{k-1,n-1})G_r$$

とすることができる。$W \oplus (S_1, ..., S_{n-1})G_s = W_s$ と表し、G_r の逆行列 ${G_r}^{-1}$ を求めると

$$W_s = (R'_{1,1}, ..., R'_{k-1,n-1})G_r$$

$$W_s {G_r}^{-1} = (R'_{1,1}, ..., R'_{k-1,n-1})$$

となり、S と $k-1$ 個の分散情報 W から R' が定まる。また、このようにして求めた R' を用いて分散情報を生成することで、他の分散情報が定まる。

4 おわりに

今後の課題として、3章で記した方法の (k,L,n) ランプ型秘密分散法への拡張、$BM(P)$ =$BM(P_w) = W_i$ を満たす透かしの埋め込み方法の考察が挙げられる。

参考文献

[1] A.Shamir, "How to Share a Secret," C.ACM, Vol.22, No.11, pp.612-613, 1979.

[2] G.Blakley, "Safeguarding Cryptographic Keys," Proc.AFIPS, Vol.48, pp.313-317, 1979.

[3] 藤井ら, "排他的論理和を用いた (k,n) しきい値法の構成法," ISEC2007-5, pp.31-38.