社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－AVM－52（5）
2006／3／3

画像情報のデータ量削減型階層秘密分散法に関する検討

橋本 真幸† 南 順之‡ 松尾 賢治† 小池 淳†

†株式会社 KDDI 研究所 〒356-8502 埼玉県ふじみ野市大原 2-1-15
‡東京理科大学工学研究科電気工学専攻〒162-8601 東京都新宿区神楽坂 1-3
E-mail: †{masayuki, matsuo, koike}@kddilabs.jp, ‡yori-373@tsm.kddilabs.jp

あらまし 本論文では，画像情報の秘密分散法の利便性を高めるためにこれまでに提案された階層型秘密分散方式において，安全性を保ったまま分散情報（シェア）のデータ量を削減する方式を提案する．階層型秘密分散方式では，秘密分散法の本来の特長であるシェアの損失や漏洩に対する強度をもつだけでなく，JPEG 2000 の階層構造を利用することにより，合成するシェアの数に応じて階層的に画像情報を公開することが可能である．しかし，シェアの作成に(k, n)しきい値秘密分散法を用いていたため，シェアのデータ量が元の秘密情報と同じになり，データ蓄積容量の面で問題があった．本論文では，(k, L, n)しきい値秘密分散法を用いることによりデータ量の削減を図る（方式１）．しかし，(k, L, n)しきい値秘密分散法は，しきい値の数に満たない数のシェアからでも秘密情報が復元されてしまう可能性があり，方式１では安全性の面で問題がある．そこで，JPEG 2000 の階層構造における各階層を重要部分とそれ以外に分割し，画像情報を再生する上で重要でない部分に対してのみ(k, L, n)しきい値秘密分散法を用いる方式（方式２）を提案し，その有効性を示す．

キーワード JPEG 2000，秘密分散法，コンテンツレベルセキュリティ

A Study on Data-Size-Reduction Methods for Hierarchical Secret Image Sharing Method

Masayuki HASHIMOTO† Yoriyuki MINAMI‡ Kenji MATSUO† and Atsushi KOIKE†

† Visual Communication Laboratory, KDDI R&D Laboratories Inc.
2-1-15 Ohara, Fujimino-Shi, Saitama, 356-8502, Japan
‡ Department of Electrical Engineering, Faculty of Engineering, Tokyo University of Science
1-3 Kagurazaka, Shinjuku-Ku, Tokyo, 162-8601, Japan
E-mail: †{masayuki, matsuo, koike}@kddilabs.jp, ‡yori-373@tsm.kddilabs.jp

Abstract This paper proposes the data reduction methods for the hierarchical secret image sharing scheme(HSIS). The HSIS has the security level against the loss or leak of the image content using the (k, n)-threshold secret sharing method. HSIS can also disclose image contents hierarchically using JPEG 2000(J2K)'s hierarchical code stream syntax.

However, HSIS has a problem with storage size: the data size of each share is same as that of the J2K image. Therefore, in this paper, we propose the data-size reduction method (Method 1) for the HSIS using the (k, L, n)-threshold secret sharing method, which generates smaller shares than the (k, n) method.

The (k, L, n) method has the problem with security because there is a possibility that the original data is unexpectedly reconstructed by a smaller number of share than the threshold number, k. Therefore, our second proposed method(Method 2) uses the (k, L, n) method for the parts of coded data which is not significant in the decoded image. In this paper, we show that the Method 2 reduces the data size of shares keeping the security level of the image content.

Keyword JPEG 2000, Secret Searing Scheme, Contents level security

1. はじめに

ブロードバンドネットワークの普及に伴いコンテンツ配信に対する注目が高まっている．コンテンツを販売することにより利益を得るビジネスを確立するためにはコンテンツに対するセキュリティは必須の技術である．またコンテンツに対するセキュリティ技術の普及を考えた場合，セキュリティ強度だけではなく機能性や使いやすさのなどの要素も重要になってくる．

秘密情報を保護し，安全に保管するための方法として秘密分散法[1]-[3]を用いた分散蓄積技術が注目され

ている．一般に良く知られている秘密分散法として(k, n)しきい値秘密分散法（以降，「(k, n)法」）[1]がある．(k, n)法は，（k-1）個までのシェアが漏洩しても元の秘密情報は復元できないため情報漏えいに対して安全であり，（n-k）個までシェアが紛失しても元の情報を復元できるため，情報の紛失に対して安全である．セキュリティの度合いを上げるためには k の値を大きくすることが望ましいが，その情報にアクセスするためには，いかなる場合でも k 個以上のシェアを集めて合成する必要があり，単に画像の概要を低解像度で閲覧したい場合など，セキュリティレベルを落としても良い利用場面などでは利便性に問題が生じる可能性がある．

そこで，筆者らはこれまでに，合成するシェアの数により再生する画像品質を階層的に制御できる階層型秘密分散方式（以降，従来方式）を提案した．そこでは，JPEG 2000（J2K）[4][5]を用いた階層符号化手法と(k, n)法を組み合わせて用いている．しかし，(k, n)法では，シェアのデータ量が元の J2K ファイルサイズと等しくなるため，セキュリティ強度を上げるためにシェアを大量に作成した場合，蓄積容量のが問題が発生する．

本論文では，従来方式におけるシェアのデータ量を削減するため，（k, n）法の代わりにシェアデータ量を小さくできる（k, L, n）しきい値秘密分散法（以降，「(k, L, n)法」）を用いる方式を提案する（方式１）．しかし，(k, L, n)法は，しきい値の数に満たない数のシェアからでも秘密情報が復元されてしまう可能性があり，安全性の面で問題がある．そこで，各レイヤを保護レイヤと通常レイヤに分割し，最上位レイヤおよびそれ以外のレイヤの保護レイヤに対しては，セキュリティ強度の高い(k, n)法を適用し，通常レイヤに対してはデータ圧縮性能の高い（k, L, n）法を適用する方式を提案する（方式２）．

以降本論文では，第 2 節で従来方式およびこれを構成する秘密分散法と J2K について説明する．第 3 節で方式１，第 4 節で方式２をそれぞれ提案し，特性を評価する．

2. 階層型秘密分散方式（従来方式）

2.1. 秘密分散法

秘密分散共有法を使った情報の分散蓄積方法は図１に示すように画像情報を複数の分散情報（シェア）に分散して蓄積しておき，そのうち幾つかを合成することにより元の画像情報が得られるというものである．この方式により情報を分散して蓄積しておくことで，一部のシェアが紛失した場合でもオリジナルの画像情報の再現性が補償でき，一部のシェアが漏洩したとしてもオリジナルの情報が秘匿されるという，強固なコンテンツレベルでのセキュリティが実現される．

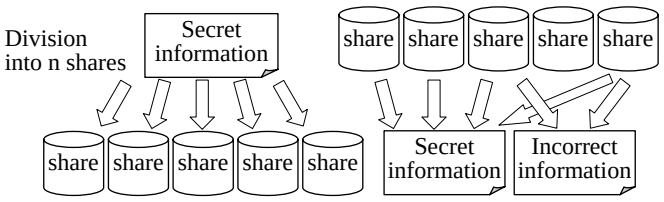


図 1　秘密分散法

一般に良く知られている Shamir の(k, n)法では，分散関数と呼ばれる(k-1)次の多項式を用いて秘密情報を分散符号化する．分散関数の一般形は秘密情報 S，乱数項 r_i(1 ≦ i ≦ k-1)および素数 p により次のように表現される．

$$f(x) = S + r_1 x + \cdots + r_{k-1} x^{k-1} (\mathrm{mod}\ p) \qquad (1)$$

分散情報 W_i は上記の分散関数に任意の i(i<p)を代入し，W_i=f(i)として計算される．分散関数 f(x)は，(k-1)次の多項式であることから，k 個の分散情報を集めれば，分散関数自体を復元でき，したがって秘密情報 S の復元が可能となる．一般に，秘密分散情報 S は k 個の分散情報を表す連立方程式を解くことにより復元されるが，秘密分散法では以下の Lagrange の補間公式が用いられることが多い．

$$S = f(0) = \sum_{i=1}^{k} c_j W_i, \; which\ c_j = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x_j}{x_j - x_i} \qquad (2)$$

2.2. 階層的符号化方式 JPEG 2000

2.2.1. JPEG 2000 の符号化アルゴリズム

画像情報を階層的に表現する符号化手法のひとつに J2K がある．図 2 に J2K 符号化の流れを示す．符号化対象画像は１つ以上のタイルと呼ばれる矩形領域に分割され，タイルごとに符号化処理される．これにより符号化データ上において特定画像領域へのランダムアクセスが容易になる．

次に，タイル化された画像はウェーブレット変換により，縦横それぞれの方向の画素値の変化の周波数成分に応じてサブバンド分解される．ウェーブレット変換は縦横両方ともが低周波数成分を持つサブバンドに対して繰り返し行われる．

サブバンドはさらに小さな矩形であるコードブロックごとにビットプレーン符号化される．図 3 にビットレーン符号化の概念図を示す．基本的には各ビットプレーンに対して 3 つのパスが生成される．それぞれのパスは算術符号化される．

復号する際に読み込むビット量に応じて段階的に復号画像の画質（量子化精度）を向上させることが出来るように，符号化時に画質に同程度寄与するパスの

集合をひとつのレイヤにまとめることができる.

2.2.2. JPEG 2000 符号列構文

符号データは，パケットと呼ばれるデータセグメント単位でまとめられる．それぞれのパケットは，必ずある特定タイルのある特定ウェーブレット分解レベルにおけるある特定レイヤの符号を含む．パケットを伝送する順序によって,再生画像の品質(解像度レベル，量子化精度，再生領域など）を制御することが可能である．本論文では，より柔軟に再生画像品質を制御することが可能な SNR スケーラブルモードに関して議論することとする．このタイプではあるレイヤに含まれるすべてのパケットが連続してあらわれる．より上位のレイヤのデータほどより前にあらわれる．このタイプのパケットの並びを図 4(a)に示す.

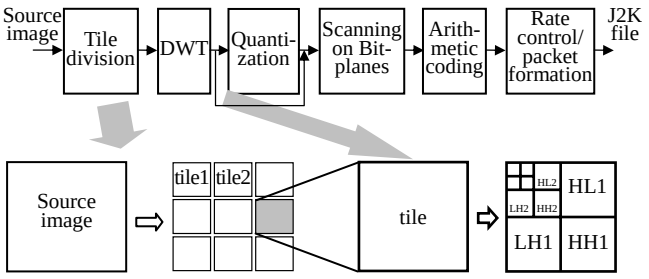


図 2　JPEG 2000 符号化処理

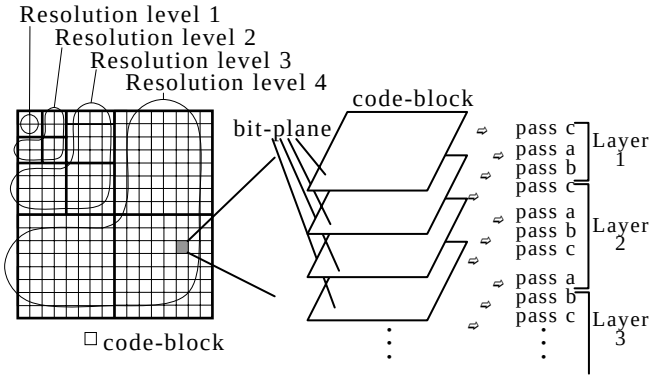


図 3　符号化におけるコードブロックとパス

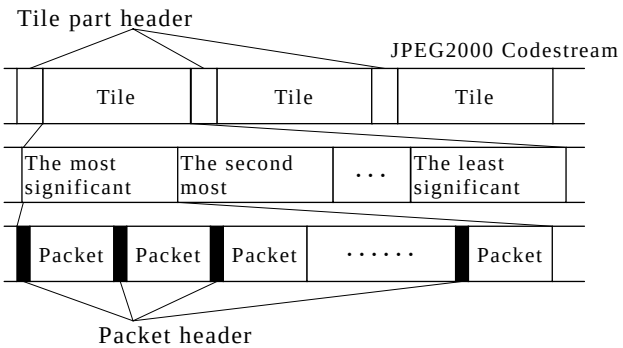


図 4(a)　JPEG 2000 符号列構文
(SNR スケーラブルモード)

2.3. 階層型秘密分散方式(従来方式)

2.3.1. 階層型秘密分散方式フレームワーク

図 5 に提案方式の処理の流れを示す．まず秘密情報は符号化され通常の J2K 符号列が作成される．次に，シェア作成部において，その符号列をもとに秘密分散法を用いて J2K シェア情報が作成される．ここで，階層的機能を実現するため，それぞれのレイヤごとに k の値が決定される.

画像を再生する際にはいくつかの J2K シェア情報が合成される．まず J2K 符号列が復元され，その符号列を復号して画像が再生される．提案方式においては，合成するシェア情報の数が，再生画像の再生画像品質に影響を与える.

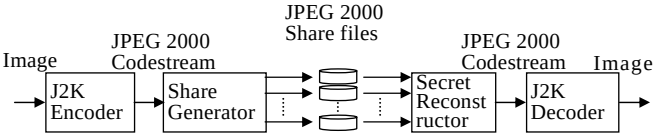


図 5　階層型秘密分散方式のフレームワーク

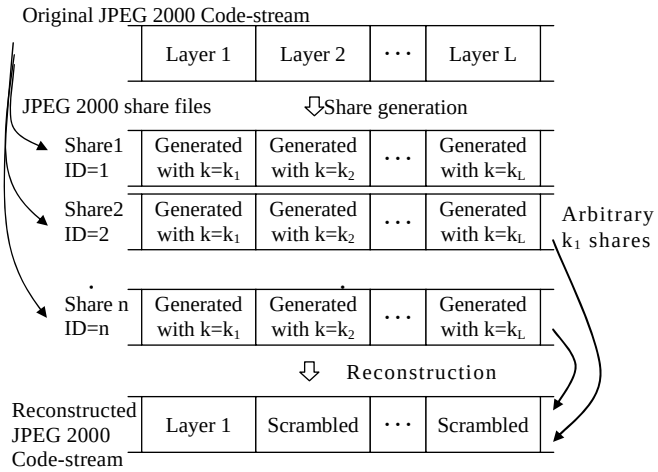


図 6　シェア情報生成と JPEG 2000 符号列の復元

2.3.2. シェア情報生成処理

図 6 に従来方式でのシェア情報生成と J2K 符号列復元の様子を示す．まず，原画像を階層化 J2K（SNR スケーラブルモード）で符号化し，符号列を生成する．シェア作成部では，それぞれのパケットの情報から秘密分散法を用いて n 個の分散を作成する．ここで，式(1)(2)で使われる x としてシェア ID を定義する．それぞれのシェア ID の値はそれぞれの JP2 シェア情報のコメントタグ（自由に内容を記載できるスペース）に書き込む．後述の実験ではすべて M を 8 とした.

ここでは，どのレイヤに含まれるパケットかによって k の値が決められる．つまり，あるレイヤごとにそこに含まれるパケットに関しては特定の同一の k で分散処理を行う．この際，優先度の高い階層ほど小さな

k の値を用いる．例えば，多くの J2K シェア情報を合成するほど，正しく復元されるレイヤの数を増やしたい場合を考えると，シェア情報生成部においてレイヤ i に対して次のように k の値を設定して秘密分散処理を行う．

$$k_1 \le k_2 \le \cdots \le k_L \qquad (3)$$

ここで k_i はレイヤ i の秘密分散処理に用いる k の値を示し，L は J2K 符号列中のレイヤの個数を示す．

また，JP2 シェア情報は，もとの JP2 符号列のパケットデータを置き換えただけのものなので，JP2 符号列構文に完全に準拠している．そのため，JP2 シェア情報を JP2 復号器で復号処理することが可能である．この場合，当然のことながら，分散処理されたタイルの部分はスクランブルされて再生される．また復号器の実装によっては，符号中にマーカコードが発生すると，復号処理に問題が発生する場合があるため，分散情報中にマーカコードが発生しないようにするのが望ましいが，ここでは他の論文（[6]など）に議論を譲る．

2.3.3. 再生処理

次に合成処理を示す．m 個の JP2 シェア情報を集めたとする．シェア情報のヘッダはコメントタグを除いては，すべて同一であるため，任意のひとつのヘッダを用いて JP2 シェア情報を解析できる．

すべてのシェア情報とコメントタグに埋め込まれた各シェア情報の ID から式(2)を用いてパケットデータを復元する．もし $k_i \leqq m < k_{i+1}$ の場合には式(3)より m は k_j (j=1, 2, …, i)より大きい．従って，上位のレイヤから数えて i 個のレイヤが正しく復元される．その後，通常の J2K 復号器により，復元された符号列が再生される．もし前段のパケット復元処理においていくつかのレイヤが正しく復元されていなかった場合，再生画像はノイズを含んだ画像となる．合成するシェアの数 m が増えると正しく再生されるレイヤの数が増え，再生画像のノイズ成分が減少し画質が改善する．

2.4. 従来方式の特性

ここでは方式の有効性を検証する．J2K 符号化器において 2 つのレイヤを含む通常の可逆ビットストリームを生成する．この際，最上位レイヤに 0.005 bit/pixel(bpp)を割り当て，残りのビットはすべて 2 番目のレイヤに割り当てる.（可逆符号化による符号化ビットレートは 4.496 bpp であった.）そして，上位 i 番目のレイヤの秘密分散処理に用いる k の値を k_i と定義し，シェア情報生成部において$(k_1, k_2) = (5, 6)$，n = 20 として秘密分散処理を行った．

図 7 (a)にあるひとつの J2K シェア情報から再生した画像を示す(m = 1)．図 7(b)および(c)にそれぞれ m = 5 および 6 の場合の再生画像を示す．図 7 (a)からは原画像は判別できないのに対し，図 7(b), (c)では m が大きくなるに従って再生画像中のノイズが少なくなることがわかる．これは，多くのシェア情報が合成されることにより，より多くのレイヤが正しく復元されるためである．本実験の場合 m =6 以上では原画像が完全に再生される．以上の結果より，合成するシェアの数 m により再生するレイヤ数が制御でき，それにより再生画像の品質を制御できることがわかった.（今回の評価では 2 段階の画質制御）

3. 提案方式 1

提案方式 1 では，従来方式における(k, n)法の代わりにデータ量削減のため(k, L, n)法を用いる．本節では 3.1 節において (k, L, n)しきい値秘密について説明した後，3.2 節において方式を提案する．3.3 節，3.4 節ではそれぞれデータ量の削減効果とセキュリティレベルの低下について説明する．

3.1. (k, L, n)法

一般に(k, L, n)しきい値法では，秘密情報 S を L 数の部分秘密情報 S_i (i = 1, …, L).に分割する．シェアデータ $W = [w_1 \ \cdots \ w_n]^{\mathrm{T}}$ は次の式により作成される．

$$W = G\,A \pmod p \qquad (3)$$

ここで，

$$G = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{k-1} \\ 1 & x2 & x_2^2 & \cdots & x_2^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{k-1} \end{bmatrix},$$

$$A = [S_1 \ \cdots \ S_L \ \ r_1 \ \cdots \ r_{k-L}]^T$$

である．x_i (i = 1, …, n) はシェア ID を示す．また r_i (i = 1, …, k-L)は乱数である．k はしきい値，p は素数を示す．

m 個のシェアから元の秘密情報を合成する際には，次の式により秘密情報が得られる．

$$A_m = G_m^{-1} W_m \pmod p,$$

ここで，

$$A_m = \begin{cases} [\,S_1 \ \cdots \ S_m]^T & (m \le L) \\ [\,S_1 \ \cdots \ S_L \ \ r_1 \ \cdots \ r_{m-L}]^T & (m > L) \end{cases}$$

$$W_m = [\,w_{I_1} \ \cdots \ w_{I_m}]^T,$$

$$G_m = \begin{bmatrix} 1 & x_{I_1} & x_{I_1}^2 & \cdots & x_{I_1}^{m-1} \\ 1 & x_{I_2} & x_{I_2}^2 & \cdots & x_{I_2}^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_{I_m} & x_{I_m}^2 & \cdots & x_{I_m}^{m-1} \end{bmatrix}$$

なお，I_i は i 番目のシェアの ID である $(i=1,\cdots,m)$．

3.2. 方式

方式 1 では，従来方式のシェアデータ量を削減するため，単純に(k, n)しきい値秘密分散方式の部分を(k, L, n)しきい値秘密分散方式に置き換えただけたものである．S_i のデータサイズは S のデータサイズの $1/L$ である．ここで S_i の大きさを 8 ビットとすると，S の大きさは $8L$ ビットとなる．p の値を 257 に設定する．作成されたシェア情報 w_i $(i = 1,\cdots, n)$のうち一つでも 256 あるいは 257 であった場合は，異なる乱数を用いてもう一度シェア情報を作り直す．これにより w_i は必ず 0～255 の間の値をとるため 8 ビットで表現できる．つまり，w_i のサイズと S_i のサイズを同じにすることが出来る．

連続した $8L$ ビットずつを J2K のコードストリームから順次取り出し，秘密情報 S として用いると，8 ビットのシェアが n 個できるため，合計 $8n$ ビットのシェアが生成される．(k, n)法を用いた場合だと $8L$ ビットの S からは，$8L$ ビットのシェアが n 個生成されるため，合計で $8Ln$ ビットのシェアが作成される．よって，(k, L, n)法を用いることにより，シェアのデータ量を $1/L$ にすることができる．

3.3. データ量削減効果

表 1 に方式 1 のシェア情報ファイル 1 つあたりのデータ量を示す．評価に使用した画像は 2048×2048 画素グレースケール画像である．2.4 節と同様に 2 つのレイヤを含む可逆 J2K 画像を作成し，第 1 レイヤ P_1 および第 2 レイヤ P_2 の k の値はそれぞれ $k_1 = 5$, $k_2 = 6$ とした．シェアの数 n は 20 とした．同表中の HSIS の記述は従来方式を示す．表 1 よりシェアのサイズは従来方式に比べて約 1/4 になっていることがわかる．これは前節にも説明したとおり， L 分割（L=4）した部分秘密情報 Si と同じサイズのシェアが作成されるためである．以上より(k, L, n)法を使った方式 1 の，データ削減効果が確認された．

3.4. セキュリティの低下

(k, L, n)法では，しきい値 k に満たない数のシェアから部分秘密情報が再生されてしまう場合があることが知られている．ここでは，確率的にどの程度，この漏洩が発生するかについて検証する．

ひとつ以上の部分秘密情報が完全に復元される場合 20 個のうち m 個のシェアを取るすべての組み合わせで合成処理を行い，一つ以上の部分秘密情報が復元される確率を計算機シミュレーションにより求めた．結果は乱数項の影響をうけるので，異なる乱数パターンを用いて 10 回測定を行った．表 2 および表 3 はそれぞれ k = 5, k = 6 の場合の復元確率である．両表とも L = 2, 3 および 4 の場合を示す．

本来，m < k では，部分秘密情報は復元されるべきではないが，表 2 および表 3 より，k=5 の場合 m=4 において，k=6 の場合 m=5 において，部分秘密情報が復元されていることがわかる．これより，(k, L, n)法を単純に用いた方式 1 では，秘密情報漏洩の危険性があることがわかる．そこで，次節により安全性を改善した新しい方式を提案する．

4. 提案方式 2

4.1. 方式

一般に J2K のコードストリームが 2 つ以上のレイヤに分かれていて，最上位レイヤ（MSL）がスクランブルされている場合，再生画像からは画像情報を全く読み取れないことが期待できる．なぜなら，再生画像の各画素の上位ビットの値がランダム化されるからである．そこで方式 2 では MSL に対しては安全性の高い(k, n)法を利用し，それ以外のレイヤに対してはデータ削減効果の高い(k, L, n)法を用いることとする．

しかし，階層型秘密分散方式においては「半開示」の状態が存在する．つまり上位のいくつかのレイヤは正常に復元され，残りのレイヤがスクランブルされた状態である．この場合，MSL 以外にはセキュリティ強度の低い(k, L, n) 法を用いていると，まだ正常に復号されるべきではないレイヤが漏洩してしまう危険性があり，これにより，半開示画像の画質が期待以上に改善してしまうおそれがある．そこで，方式 2 では，MSL 以外の各レイヤ P_i をさらに 2 つのレイヤ P_{i0} と P_{i1} に分割する．P_{i0} を上位のレイヤとし，保護レイヤと呼ぶ．保護レイヤには安全性の高い(k, n) 法を適用し，通常レイヤ P_{i1} にはデータ削減効果の高い(k, L, n)法を用いる．これにより，(k, L, n)法を用いているすべての通常レイヤが漏洩したとしても，保護レイヤは漏洩しないため，各レイヤは高い安全性で保護されていることになる．

4.2. セキュリティ性能評価

4.2.1. 画像全体に対するセキュリティ

方式 2 では MSL に対しては(k, n) 法を用いるため，それ以外のレイヤがすべて復元された場合でも画像情報は開示されないものと期待できる．MSL に割り当てるビットレート B_1 について検討した結果，3.3 節で用いた評価画像の場合は，$B_1 = 0.005$ bpp 以上であれば画像情報は安全であることを確認した．図 8 に $B_1 = 0.005$ bpp とし，MSL 以外のレイヤがすべて漏洩した最悪の

ケースの画像を示す．この場合でも画像情報は漏洩していないことが確認できる．

4.2.2. 半開示画像に対するセキュリティ

MSL のビットレート B_1 = 0.005 bpp，第 2 レイヤ P_2 のビットレート B_2 = 4.491 bpp として，3.3 節と同様のパラメータで方式 2 の階層型秘密分散を行った．P_2 の保護レイヤ P_{21} のビットレート B_{21} が 0.001 bpp と 0.1 bpp の場合について，P_{21} 以外のレイヤがすべて漏洩した場合の画像を図 9(a), 図 9(b)にそれぞれ示す. 図 9(a)では画像はほどんと開示されてしまっている．一方図 9(b)では，本来の半開示画像（図 7(b)）とほぼ同等の画質であり，半開示画像に対する安全性が確保されたことがわかる. MSL や保護レイヤへの割り当てビット量の最適化は今後の課題とする．

4.3. データ量削減効果

表 1 に方式 2 のデータ削減効果を示す．同表より，方式 2 においては従来方式に比べシェアのデータ量を 26.9%にまで削減できることがわかる．これは方式 1 のデータ削減効果に比べると若干効果が小さい．これは，保護レイヤに対してはデータ削減効果の見込めない(k, n) 法を用いているためである．

5. まとめ

本論文では，画像情報の秘密分散法の利便性を高めるためにこれまでに提案された階層型秘密分散方式において，安全性を保ったままシェアのデータ量を削減する方式を提案する．まず，単純に(k, L, n)法を用いることによりデータ量の削減を図る方式 1 を提案した．しかし，(k, L, n)法は，しきい値の数に満たない数のシェアからでも秘密情報が復元されてしまう可能性があり，方式 1 では安全性の面で問題があることが確認された．そこで，JPEG 2000 の階層構造における各階層を重要部分とそれ以外に分割し，画像情報を再生する上で重要でない部分に対してのみ(k, L, n)法を用いる方式 2 を提案した.その結果,安全性を確保したまま，シェアのサイズを従来方式に比べ 26.9%にまで削減できることがわかった．

文　献

[1] A. Shamir, "How to share a secret", In Communications of the ACM, vol.22, no.11, pp.612-613, November 1979.

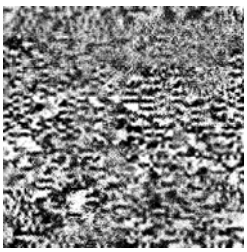
[2] G. R. Blakley, "Safeguarding cryptographic keys", Proc. AFIPS 1979 National Computer Conf., vol.48, pp.313-317, September 1979.

[3] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes", J. of Cryptology, vol.4, no.2, pp.123-134, 1991.

[4] ISO/IEC 15444-1, “Information technology – JPEG2000 image coding system – Part 1: Core coding system,” ISO/IEC JTC 1/SC 29/WG1, Jan.2001.

[5] D.S. Taubman, “High performance scalable image compression with EBCOT,” IEEE Trans. Image Proc., vol.3 no.5, pp.1158-1170, July 2000.

[6] H. Kiya, et. al., “Partial-scrambling of images encoded using JPEG2000 without generating marker codes”, IEEE International Conference on Image Processing (ICIP2003), volume 3, pp. Ⅲ205-8, Sept. 2003.



(a) Reconstructed image. m = 1. (PSNR 6.8dB)

(b) Reconstructed image m = 5. (PSNR 11.4dB)

(c) Reconstructed image. m = 6.(Lossless)

図 7　従来方式の再生画像

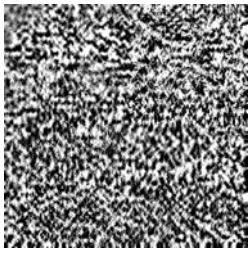


図 8　MSL 以外が漏洩した画像（PSNR 7.3dB）

(a) B_{21}=0.001bpp (PSNR 20.1dB)

(b) B_{21}=0.1bpp (PSNR 11.9dB)

図 9　方式 2 において保護レイヤ以外のレイヤが漏洩した画像

表 1　シェア情報ファイルのデータ量

		Data size (K Byte)	HSIS's share size (%)
Conv. HSIS		2357	100.0
Method 1 (L=4)		593	25.2
Method 2 (L=4)	B_{21}=0.001bpp	595	25.2
	B_{21}=0.100bpp	634	26.9

表 2　1 つ以上の部分秘密情報が復元される確率 (k = 5)

		m						
		1	2	3	4	5	6	7
L	2	0	0	0	0.25	100	100	100
	3	0	0	0	0.29	100	100	100
	4	0	0	0	0.54	100	100	100

表 3　1 つ以上の部分秘密情報が復元される確率 (k = 6)

		m						
		1	2	3	4	5	6	7
L	2	0	0	0	0	0.45	100	100
	3	0	0	0	0	1.05	100	100
	4	0	0	0	0	1.65	100	100