1E-04

観賞価値を有した画像への秘密分散法の提案

公文　裕太‡　　山田　隆行‡

高知工業高等専門学校‡

1　はじめに

これまでセキュリティ技術の基本となっていた暗号化技術に暗号化がある．この暗号化には鍵が必要であり，鍵配送問題や鍵の管理が必要となる．また，量子コンピュータの実用化が進むことで，計算量を安全性の根拠とする暗号の安全性は揺らいでしまうこともあり，近年，秘密分散方式が注目されている．

画像への秘密分散として，視覚復元型秘密分散法があるが，分散された画像は，無意味なランダムパターンとなるか，別の絵柄となるように画素の配置を行う必要があるため，観賞的価値が無く，視覚特性を利用する方法のため，埋め込める情報も画像に限られる．

本論文では，さまざまなデジタル情報を分散することができ，かつ分散された各々の画像の鑑賞的価値を損なうことのない秘密分散法を提案する．これにより，分散された画像の視認性と管理効率の向上が期待できる．

2　従来の方法

秘密鍵分散は 1979 年に Adi Shamir と George Blakley らによって独立に提唱された概念で，一つの情報（秘密）を複数に分割して管理する技術である．元の情報の復元には，分割後の情報をすべて集めない限り元の情報を復元不可能であるという特徴がある．

この概念を画像に応用した方式に視覚復元型秘密分散法がある．この方法は，情報の復元を人間の視覚によって行うもので，暗号化により生成された画像形式の分散情報を透明フィルムに印刷し，複数の透明フィルムを重ね合わせることにより浮かび上がる情報を視覚的に得ることにより行う．

しかしながら，この方法では，分散された画像は，無意味なランダムパターンとなるか，別の絵柄となるように画素の配置を行う必要があるため，画像の観賞的価値は無くなってしまう．このため，分散された画像は視覚的に区別がつかず，複数の分散画像の管理は困難である．

そこで本論文では，次章で述べるShamir の秘密分散法を利用して，分散された画像の鑑賞的価値を有した秘密分散法を提案する．

A Proposal of Image Secret Sharing with Worth Seeing
Yuta Kumon‡ and Takayuki Yamada‡
National Institute of Technology, Kochi College‡

3　提案手法

3.1　Shamir の秘密分散法[1]

(k, n)閾値法を実現する方法としてよく使用されるものは多項式補間である．この方法は，(k−1)次曲線上の k 個の点の座標が判明すれば曲線を表す多項式が一意に定まるという性質を利用している．しかしこの方法では，3 次曲線以上の曲線の場合に計算結果が小数で表されることがある．その際，計算結果を整数にする必要があるために小数点以下を切り捨て，または，四捨五入する必要がある．その結果，暗号化と復号化で値が一致しなくなる．それでは，完全性を確保することが出来ない．また，画像の画素は 0 から 255 までの整数値で扱う必要がある．

そこで，本論文では，k=n とした Shamir の(k, n)閾値法を用いる．

k=n の場合の(k, n)閾値法では，一般的に任意の有限体上での暗号化と復号化の式として，それぞれ①式と②式が知られている．

$$V_n = \left(S - \sum_{k=1}^{n-1} V_k\right) mod\ N \qquad ①$$

$$S = \sum_{k=1}^{n} V_k\ mod\ N \qquad ②$$

ここで，nはシェアする人数である．Sは秘密にしたい情報（秘密情報）である．$V_1 \sim V_{n-1}$は S の範囲でランダムな値である．NはSの取り得る値の数である．

3.2　観賞価値を有した画像への秘密分散方法

提案手法では，任意の情報に対し Shamir の秘密分散法を利用して情報を分散する．このとき，分散させる情報は電子透かしとして埋め込む．Shamir の秘密鍵分散法では，$V_1 \sim V_{n-1}$はランダムな値を選ぶ必要あるが，提案手法では，$V_1 \sim V_{n-m}$は任意の原画像の画素値のビット情報を利用し，残り$V_{n-m+1} \sim V_n$のm枚を透かしとして画像に埋め込む．これにより，画像選択の自由度があるだ

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.

けでなく，分散された画像は高画質なものを作成することができる．

この分散手順と復元手順を図 1，図 2 に示す．

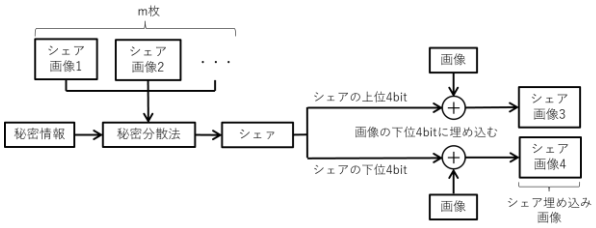


図 1 分散手順

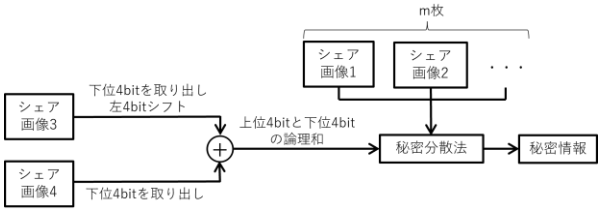


図２　復元手順

4. 検証実験

提案手法により分散が行えることを検証する．実験条件は，$n = 4$ とし，用いる画像は 256×256 サイズの 256 諧調グレースケール画像とする．実験では，秘密情報として画像とテキストファイルの 2 つを設定して実施した．

4.1. 画像の秘密分散

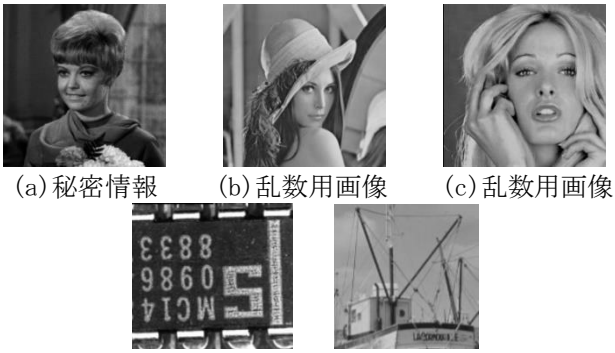
実験に用いた画像はそれぞれ，図 3(a)は秘密情報，(b)と(c)は乱数として用いる画像，(d)と(e)は埋め込む画像である．以上の画像を用いて分散を行った結果を図 4(a)，(b)に示す．また，復号で得られた復元秘密情報を図 4(c)に示す．秘密情報と復号秘密情報を比較すると一致する．

4.2. テキストファイルの秘密分散

実験に用いた画像は図 3(b)，(c)，(e)である．秘密情報は，ls コマンドのマニュアルであり，形式としてはテキストファイルである．図 3(b)，(c)は乱数として用いる画像，(d)，(e)は埋め込む画像である．秘密情報と復号秘密情報を比較すると一致する．

5. 考察

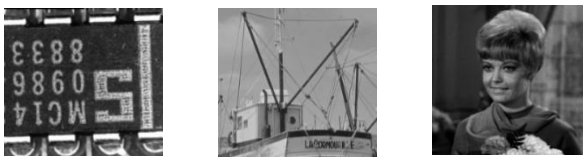
実験結果から，分散・復号が行えているため，本提案手法を用いての分散・復号が行えたと判断できる．また，埋め込んだ画像の画質劣化を確認するために，画像の品質尺度として PSNR を利用し，③式により求めた結果を表 1 に示す．



(a)秘密情報　(b)乱数用画像　(c)乱数用画像

(d)透かし画像　(e)透かし画像

図 3　実験画像



(a) 埋め込み画像　(b)埋め込み画像　(c)復元画像

図 4　実験結果

$$PSNR = 20\log_{10}\frac{255}{\sqrt{\sum_{i=1}^{M}\sum_{i=1}^{N}(orig_{ij} - emb_{ij})^2 / MN}} \quad ③$$

表 1　画像の PSNR

原画像と透かし画像	PSNR
図 3(d)と図 4(a)	6.822156
図 3(e)と図 4(b)	5.247982

表 1 の結果より，PSNR の値は小さいことが確認できる．よって、画質劣化は小さいと判断できる．また，視覚的にも原画像と透かし画像との差異は確認することが困難である．

これにより，分散後でも観賞価値を有した状態であると判断できる．

6 おわりに

本研究では，観賞価値を有した画像への秘密分散法を提案した．これにより，従来の方法と比較し，分散された画像の視認性と管理効率の向上が期待できる．また，観賞価値を有した状態で情報の分散を行えることを確認できた．

本論文では，グレースケール画像を対象としたが，今後，カラー画像や動画像への応用を考えている．

参考文献

[1] Adi Shamir, ”How to share a secret”, Communications of the ACM Volume22, 612-613

Copyright ©2022 Information Processing Society of Japan.
All Rights Reserved.