# 自己真正性証明可能なディジタル画像文書による偽造防止手法の検討

# A Study on A Self-Authentic Fogery-Protective Image Document System

丸田　英徳 †，野崎　剛一 †
Hidenori Maruta†, Koichi Nozaki†

† 長崎大学　総合情報処理センター
† Information Science Center, Nagasaki University

**概 要**

ディジタル文書が普及するにつれて，それらの真正性や偽造等の防止などの技術の必要性が高まっている．一般的には，ディジタル署名・暗号化等の手法が普及しつつあるが，従来の人間の目による確認と比較する場合，その利用環境下次第では，なじみにくい側面がある．本提案では，デジタル画像文書に対し，近年発展している画像処理手法であるステガノグラフィを用いた真正性・偽造防止等のセキュリティについて考察を行った．

*Keywords* :

デジタル画像文書，情報ハイディング，認証技術，真正性

## 1　はじめに

近年のデジタル技術の急速な進歩・浸透に伴い，ディジタルコンテンツに対するセキュリティが重要視されてきている．デジタルコンテンツのセキュリティのなかでも，ディジタルコンテンツの真正性・偽造防止に関する研究は広い応用分野への適用が可能であり，その必要性は明らかである．

従来，ディジタルコンテンツのセキュリティは基本的には暗号化によりコンテンツを保護し，真正ディジタル署名により真正性を証明するのが一般的であり，さまざまなアルゴリズムが提案され，またそのいくつかは様々な分野で実際利用されている [1].

一方で，実社会におけるアナログデータ（書類や免許証など）による証明システムをみると，従来のディジタルコンテンツのセキュリティ関連手法のみでは対応できない，あるいはユーザにとってなじみにくい側面がある．例えば全くのオフライン環境下での認証，あるいは人間による人物個人の認証時等である．

そこで本稿では，情報ハイディング技術 [2][3] を用いた”直感的な”自己真正性証明型のデジタルコンテンツ技術についての検討を行う．近年の情報ハイディング技術の進歩，携行型の身分証や端末等への IC チップの搭載などで，ディジタルデータを利用できるケースも増えている．本稿では、取り扱う対象をディジタル画像文書 [4] の中でも特にディジタル画像身分証に限定し，情報ハイディング技術として，ステガノグラフィを用いて，偽造防止・自己証明機能を有するディジタル画像身分証システムの構築を目的とし，その基礎的な検討を行った．

## 2　概要

本セクションでは，はじめに本稿で取り扱う対象となるディジタル画像身分証を定義し，次に提案するシステムについて述べ，最後に簡単な攻撃に対する評価を行う．

### 2.1　ディジタル画像身分証システム

本稿で取り扱うディジタル画像身分証システムとは，以下の機能を有するディジタル画像文書による個人等の証明手法とする．

1. （$D_1$）ディジタル画像文書に含まれる（写真・文字データ）により，人間により個人の認証が可能である．
2. （$D_2$）ディジタル画像文書（画像データ）自身で、偽造を判別できる（あるいは自己の真性を証明できる）

一般的な多値画像の特徴として，画像をビットプレーンに分解した場合，上位ビットプレーンに視覚的に有益な情報を含み，下位ビットプレーンの 2 値画像のビット列はランダム性が高いことが知られている [3]．本稿では，ディジタル画像文書の画像フォーマットして，カラービットマップ (24bit/pixel) でのステガノグラフィを用いる．(e.g. [2]) $D_1$，$D_2$ を満たすため，多値画像データの下位ビットプレーンを上位ビットプレーンに置換し，置換後のデータをディジタル画像身分証とする（図 1）．このとき $D_1$ を満たすためには，用いる画像が現行の身分証明書に近い見た目を持ち，多層化後見た目を著しく劣化させないことが求められ，また，$D_2$ の自己証明には多層化された情報を用いる．

図 1: 階層構造をもつディジタル画像身分証

## 2.2 提案手法

下位ビットプレーンのランダム性を利用した情報ハイディングでは，カバー画像として SIDBA 等の標準画像を用いて評価することがことが多い．しかし $D_1$ により，現行の身分証明書 (ID) に近いカバー画像を用いるほうがよい．そこで本稿では評価のため，標準カバー画像として SIDBA の *Mandrill*(256×256，図 2 左)，ID カバー画像として，*ID*(320×216，図 2 右) を用いることにする．


図 2: 評価用画像（左:*Mandrill*，右:*ID*）

これらの画像について，下位ビットプレーン (2 値画像）のランダム性を BPCS ステガノグラフィ [5] で用いられている複雑さの尺度を用いる．この尺度とは，0 と 1 からなる 2 値画像の境界線 $k$ により決まる．この $k$ とは，最近傍の定義を 4 連結としたとき，画素の変わり目を縦方向・横方向でそれぞれ足し合わせたものである．$m \times m$ 画素からなる 2 値画像の場合「複雑さ $\alpha$」は，次式で定義される．

$$\alpha = \frac{k}{2m(m-1)} \qquad (0 \leq \alpha \leq 1,\ k \text{ は 2 値画像境界線の長さ},\ m \times m \text{ 画像})$$

本稿では $m = 8$ とした．その結果が，図 3 である．それぞれ，*Mandrill*，*ID* の $R$ チャネル 8 ビットプレーン目についての $\alpha$ のヒストグラムとなる．このヒストグラムの傾向は $G, B$ 各チャネルの下位ビットプレーンでも同様の結果となった．これより，*ID* のような画像の特徴として，*Mandrill* のような標準的に用いられるカバー画像と比較して，下位ビットプレーンにおいても，ランダム性が比較的高くないことが分かる．また，*Mandrill*,*ID* の $R$ チャネルの輝度分布は図 4 のようになる．$G, B$ チャネルについても同様の傾向がみられ，図 2 からも明らかなように，*ID* については，輝度分布が白（ないし黒）に偏っている．

そこで本稿では，(単純ではあるが）多層構造を，

- 各画素の $R, G, B$ 各チャネルについて，上位 4 ビットを取り出し下位 4 ビットと入れ替える

ことで生成する．これは，下位ビットプレーンの視覚的影響の少なさと，*ID* のような画像の上記のような特徴をとりいれた手法となる．真正性は，各画素の上位 4 ビット下位 4 ビットの比較で可能となる．これにより，*ID* より生

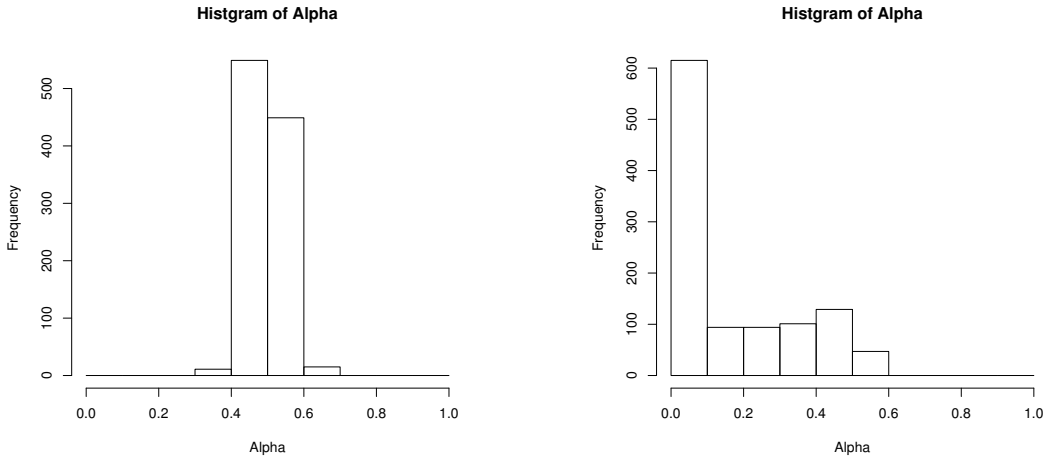


図 3: $\alpha$ の出現頻度（左:*Mandrill*, 右:*ID*）

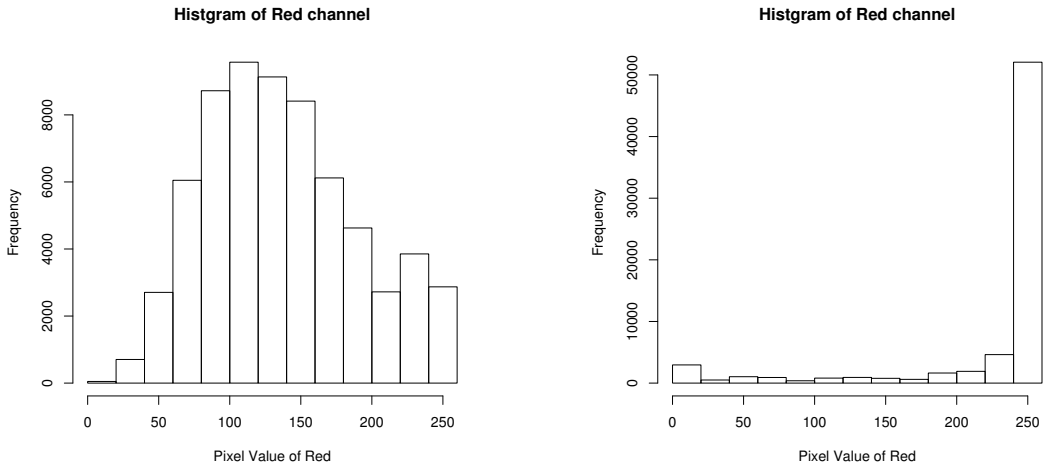


図 4: 画素値の出現頻度 ($R$ チャネル)（左:*Mandrill*, 右:*ID*）


図 5: 生成されたディジタル画像身分証（左）とそこから抽出される秘匿画像 (右)

成されたディジタル画像身分証とそこから取り出される隠匿された画像は，図 5 となり，図 2 右の元画像 $ID$ と図 5 左のディジタル画像身分証との平均二乗誤差は，$R, G, B$ それぞれ $(\Delta R, \Delta G, \Delta B) = (14.6537, 10.3889, 11.3668)$ である．

### 2.3　実験結果

攻撃耐性の評価として，ディジタル画像身分証の顔写真部分を同一人物の別画像と置き換え，秘匿画像を取り出した例を示す．提案手法では隠匿されたデータは全データの 50%にあたり，画素の操作が行われた部分の変化については，明らかに改ざんされたことが分かる．


図 6: 攻撃されたディジタル画像身分証（左）とそこから抽出される秘匿画像 (右)

## 3　今後の課題

カバー画像と比較して大きな容量のデータを埋め込み，画像を多層構造に変換することで，画素の操作に対してビットマップ構造が ” もろい ” ことを利用した，$D_1$，$D_2$ を満たすディジタル画像身分証について検討した．提案のような単純な埋め込み手法では，データを偽造される可能性は高い．しかしながら，人間に与える視覚的影響 $D_1$ を満たすような手法には，既存のディジタル署名などにない，” 直感的 ” な真正性の証明を可能にするという優位性がある．よって今後は，カバー画像に対する埋め込みデータの容量に限界があるため，上の性質を満たしつつさらに複雑な埋め込み手法を検討し，攻撃耐性を高める工夫が必要である．

## 参考文献

[1] 岡本龍明，山本博資，現代暗号，産業図書，1997

[2] 画像電子学会編，電子透かし技術，東京電気大学出版局，2004

[3] 松井甲子雄，電子透かしの基礎，森北出版，1998

[4] 野崎剛一，河口英二，Richard Eason，” 偽造防止機能を有するディジタル証明文書システム ”，大学情報システム環境研究，Vol. 7，pp21–28，2004

[5] 新見道治，野田秀樹，川口英二，” 複雑さによる領域分割を利用した大容量画像深層暗号化 ”，信学論 (D-II)，Vol. 81-D-II，No. 6，pp1132–1140，1998