Vol.2022-DPS-190 No.44
Vol.2022-CSEC-96 No.44
2022/3/11

知覚ハッシュを用いた署名による顔写真付き証明書検証手法

細井 隆秀[1,a)]　宇田 隆哉[1,b)]

概要：近年，文書の電子化が進んでおり，電子化した際に文書の真正性や偽造検出を行える技術が求められる．文書は物理的なものと電子的なものの 2 つに大別される．電子的な文書においては真正性の検証は MD5 などの暗号学的ハッシュ関数が一般的に用いられ，電子的な文書を対象とする既存研究では，暗号学的ハッシュ関数を用いたものや電子文書のファイル自体にディジタル署名を用いたものや OCR を用いたものが存在している．しかしこれらの電子的な文書を対象とした手法は，ランダムノイズ等の要因により 2 度と同じデータを得ることができないため，物理的な文書に対して用いることができない．これらの技術に対して物理的な文書に対しては知覚ハッシュを用いたものが存在する．知覚ハッシュを用いた場合ノイズによる影響を無視して同一のハッシュ値を得ることが可能であり，既存研究においてはその有効性の確認や OCR を組み合わせた手法の提案などがなされている．そこで本研究では，知覚ハッシュおよび OCR，ECDSA ならびに QR コードを用い，物理的に発行された顔写真付き証明書を対象とする真正性検証手法を提案する．スキャンした物理的な文書の知覚ハッシュ値を取得するとともに，OCR を用いて読み取った文の暗号学的ハッシュ値を求め，署名を行った上で QR コードに格納し証明書へ添付する．真正性検証時には QR コードから知覚ハッシュ値を取り出し，検証対象の知覚ハッシュ値と比較する．評価結果として本研究の設定下では同一証明書の識別成功率は 100%であり，偽造証明書の識別においても偽造検知成功率は 100%という結果を得た．一方で，本研究の設定以外の状況での運用を想定した評価を行った際には誤識別してしまう場合が確認された．

Verification Method of Certification Card with Photo by Signature with Perceptual Hash

1. はじめに

近年においては文書の電子化が進んでおり，それに伴い文書の真正性の検証や偽造防止の技術が求められている．電子的な文書に対しては MD5 や SHA256 などの暗号学的ハッシュ関数を用いた真正性の検証が一般的である．暗号学的ハッシュ関数は少しでも情報が変化していた場合，出力値において大きな変化が現れるという性質を持つ．その性質を用いて検証対象のデータが元のデータと変化がないことを検証し，変化がないことを改ざん等の処理が行われていないものとして扱うことで真正性の検証を行っている．

しかし最初からデータとして存在する電子文書に対し物理的に発行された文書は電子化時のランダムノイズ等の要因により，電子文書において用いられている真正性検証技術や偽造防止の技術を用いることができない．

そこで本論文では知覚ハッシュ関数及び OCR，ECDSA 並びに QR コードを用いた，物理的に発行された顔画像付き証明書を対象とした，悪意ある攻撃者による偽造攻撃を防ぐ検証手法を提案する．

2. 関連研究

2.1 知覚ハッシュ関数を用いた検証手法

Putro はスキャンした文書の画像データに対して，知覚ハッシュ関数を用いて真正性の検証を行っている [1]．文書には，画像，テキスト，図付きや写真付きのテキスト，証明書が用いられ，原本のハッシュ値と完全に同一だったものは 60 枚中 3 枚，同一ではないが正しく検証できたものは 95%であった．

Athichitsakul らは物理的に印刷された文書に対する，ラドン変換並びにウェーブレット変換，高速フーリエ変換を用いた検証手法を提案した [2]．彼らは印刷物の外観をキャ

[1] 東京工科大学
東京都八王子市片倉町 1404-1, 192–0982
[a)] c0118244a8@edu.teu.ac.jp
[b)] uda@stf.teu.ac.jp

© 2022 Information Processing Society of Japan

プチャすることによる文書の整合性を検証の目的としており，提案されたアルゴリズムは，テキストや画像編集などに対する変更に対して堅牢としながら，ノイズや複製などの意図しない要因による変化に対しても影響を受けないとしている．

いずれの研究も改竄耐性が考慮されていないことが問題であり，証明書の検証に用いる場合には，正当なものは正しく検証できる一方，改竄されたものは正しく検証できてはならない．いずれの研究の手法も，文書全体に 1 つの知覚ハッシュ関数を適用しているが，改竄を考慮して変化に敏感であるべき場所とそうでない場所をわける必要があると考えられる．さらに，いずれの研究においても，文書の変更はデジタルの環境で閉じられており，実際に印刷された文書をスキャンしたものに対する評価ではないことも問題である．

なお，Putro らは，後続研究として OCR の技術と知覚ハッシュ関数を組み合わせた複合式検証手法を提案している [3]．この研究ではスキャンデータを用いて評価が行われており，PCP（Print， Copy and Paste）攻撃，Imitation 攻撃，REI（Reversed Engineered Imitation）攻撃，SEP（Scan， Edit and Paste）攻撃に対する耐性検証も行われている．ただし，これらは我々が想定する攻撃とは異なるものである．

2.2 既存の文書検証手法

河内らは顔写真入り許可証に対して，顔写真部位に透かしを埋め込むことで偽造防止の提案を行った [4]．彼らは顔写真より特徴 ID を選出し，抽出データに対して電子署名を行い顔写真自体に透かしとして埋め込んでいる．これにより，QR コードのなどのスペースを別途必要とせず，既存の証明書の顔写真を彼らの手法のものに置き換えられる．しかし，河内らの手法では特徴 ID 選出時に顔写真の位置ずれが生じると，抽出データが大きく変化してしまい求められる検証用データが得られない問題が存在している．

Gonzalez らは電子チップが付属していない ID カードの改ざん検出のためのアーキテクチャを提案した [5]．彼らの提案手法は顔写真付き許可証が写真の送付などリモートで提出された際に，その証明書が本物であるか，また提出されたものが改ざんされたものであるかについて検証を行うものである．局所的なノイズや画像を再保存する際のノイズなどを特徴とした深層学習を用いて，改竄を検知している．評価では，97%以上という高い精度でクラス分けに成功していたが，想定する改竄ごとに多量のデータが必要であること，想定されない改竄には対応できないことが問題である．

Sajan らは送信者の身元と文書の内容の完全性を検証する手法として，OPDS（On Paper Digital Signature）と呼ばれる固有のディジタル署名を提案した [6]．そのディジタル署名は，無作為かつ特異的に選択された文章内の単語から作成されている．しかし，彼らの手法は OCR の認識エラーに対する問題があるのと，そもそも画像に対応できない．

3. 提案手法

3.1 提案概要

本手法は悪意ある攻撃者による偽造攻撃を防ぐ証明書署名システムとして，顔画像付きの証明書の真正性の検証を目的とする．まず，スキャンデータに対してトリミングを行い，証明書のみを抜き出す．続けて証明書全体から顔画像部分のトリミングを行い，顔画像部分と証明書全体の 2 種類のデータを用意する．用意したデータに対してそれぞれ知覚ハッシュ関数を用いてハッシュ値を取得する．証明書に記載されている文字列については OCR を用いて取得し，ハッシュ値へ変換する．また，取得したハッシュ値を結合しディジタル署名を行い，得られた署名及び原本のハッシュ値を QR コードに格納し証明書へ添付を行う．証明書の真正性を検証する際には QR コードに格納されているハッシュ値と新たに知覚ハッシュ関数を用いて得た顔画像部分及び証明書全体のハミング距離が閾値を超えていない場合，その文書の真正性が保たれているとするものである．加えて格納されている原本証明書のハッシュ値の真正性は，同様に格納されている署名を用いて検証することとする．

なお本提案手法における要件は以下の通りである．

要件 1電子化された物理的な証明書のノイズ耐性
要件 2証明書記載の重要度が高い文字列の取得手法
要件 3原本データに対する署名
要件 4署名を証明書とともに保管できる手法
要件 5偽造証明書の検知手法

要件 1 について，物理的に発行された文書のスキャン画像は，ノイズなどの外的要因により変化する．よって，ノイズがあっても真正性が保たれる手法が必要である．要件 2 について，証明書の真正性の検証を行うためには，証明書記載の文字列についても原本と同一であることを確認する必要がある．要件 3 について，文書の真正性を検証する際には，改竄を検出するディジタル署名が必要である．要件 4 について，オフライン検証を行うためには，署名は証明書と一体化されて保管される必要がある．要件 5 について，正しい証明書が正しいと検証できるだけでなく，偽造された証明書が正しく検証されないしくみが求められる．

3.2 証明書の構造

本提案手法が対象とする証明書の構造を以下の**図 1** を用いて説明する．

図 1 に示した通り証明書は黒色の枠線で囲み，顔画像は証明書の左上に QR コードは右上に配置しそれぞれ余

© 2022 Information Processing Society of Japan

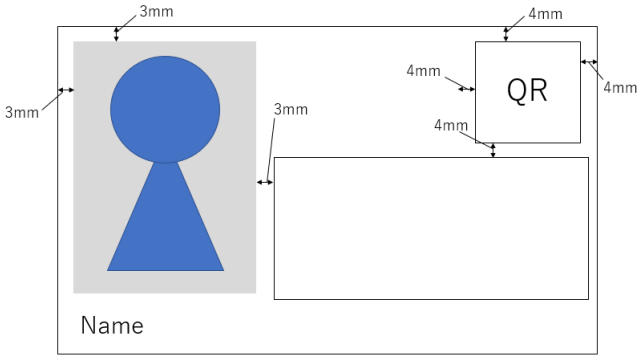

図 1 本論文が対象とする証明書の模式図

白を 3mm と 4mm 持たせるものとする．なお余白部分には他の情報を被せないものとする．証明書自体の大きさは ISO/IEC 7810 に準じた 85.6 × 53.4mm とし，顔写真の大きさは 30 × 40mm，QR コードは 14 × 14mm とする．顔画像の下に Name を設置し，Name の右横に任意の氏名を記載するものとする．また黒枠を設置し枠内には任意の文字列を記載するものとし改変は行われないものとする．文字列のフォントについては OCR-B を用い，US-ASCII かつ大きさを 50 ポイントとした．任意で設定するものを除いて，これらの仕様は本手法が対象とする証明書において全て一定であり不変であるものとする．

3.3 証明書の画像取得

スキャナを用いて物理的な証明書から顔画像部分と証明書全体の 2 種類の電子データを得る．画像処理には OpenCV を用いる．証明書全体の画像に関しては，ハッシュ値に影響を与えないよう，余白を除去する．顔画像部分を別途抽出するのは，顔画像の偽造による変化を敏感に検知するためである．本論文の証明書では，顔画像部分の位置が厳密に決められているため，位置を指定して抽出を行う．

3.3.1 重要度の高い文字列記載部分の抽出

抽出した証明書全体部分より重要度の高い文字列記載部分の抽出を行う．これは証明書の重要度の高い文字列が記載されている部分の抽出を行うことで，OCR による認識の精度の向上を目的とする．本論文の証明書では，重要度の高い文字列の位置が厳密に決められているため，位置を指定して抽出を行う．

3.4 抽出された画像からの知覚ハッシュ値の取得

3.1 節で述べた要件 1 を解決するため，本論文では証明書の画像データよりハッシュ値を取得する際に知覚ハッシュ関数を用いる．知覚ハッシュ関数は暗号学的ハッシュ関数とは異なり，画像のピクセルの関連性を保ったままハッシュ値へと変換することが可能である．本論文では知覚ハッシュ関数の 1 種である phash を用いる．

phash の計算の手順としては以下の通りである．画像をグレースケールに変更し画像サイズを 32 × 32 へのリサイズを行う．リサイズされた画像の 2 次元配列の行成分に対して離散コサイン変換を行い，列に離散コサイン変換を行う．画像を $f_{i,j}$ とし得られる DCT 係数を $F_{k,l}$ とした場合の計算を式 1 に示す．

$$F_{k,l} = 2\sum_{j=0}^{N-1}\left[2\sum_{i=0}^{N-1} f_{i,j}\cos\left\{\frac{\pi}{N}(i+\frac{1}{2}k)\right\}\right]\cos\left\{\frac{\pi}{N}(j+\frac{1}{2}l)\right\} \tag{1}$$

また得られた DCT 係数より低周波成分部分をトリミングする．離散コサイン変換の DCT 係数において低周波数成分は求めた DCT 係数の 1〜8 行目並びに 1〜8 列目に集約しているため，DCT 係数の 1〜8 行目なおかつ 1〜8 列目を抽出する．必要となる低周波成分部分 $L_{k,l}$ は $L_{k,l} = F_{k,l}$ $(k = 0, ..., 7$ ， $l = 0, ..., 7)$ のように表せる．

また得られた低周波成分の中央値を計算し，低周波成分の各成分と中央値との比較を行う．中央値を求めるにあたって，8 × 8 の 2 次元配列である低周波成分 $L_{i,j}$ を 1 次元配列に平坦化する．具体的には 2 次元配列の行を，行の順序に従い 1 次元の形に連接させていくものとする．また平坦化させた 1 次元配列を小さい順に並べ替えたものを L' とすると，中央値 $Q_{\frac{1}{2}}(L')$ は式 2 より求められる．

$$Q_{1/2}(L') = \frac{1}{2}(L'_{\frac{n}{2}} + L'_{\frac{n}{2}+1})(n = 64) \tag{2}$$

求めた低周波成分の中央値 $Q_{1/2}(L')$ よりも低周波成分 $L_{i,j}$ の各要素の値が大きい場合 1 を，小さい場合には 0 を 2 次元配列 $D_{k,l}$ へと代入する．次に，求めた 2 次元配列 $D_{k,l}$ を 1 次元配列に平坦化する．具体的には 2 次元配列の行を，行の順序に従い 1 次元の形に連接させていくものとする．得られた 0 と 1 の配列を 2 ビットの配列としたものを 16 進数の文字列に変換したものが知覚ハッシュ関数が出力するハッシュ値である．

また登録時においてはハッシュ値を取得する前にダミーの QR コードを証明書へ正規の QR コードと同位置に貼り付ける．検証時には証明書上に QR コードが存在しているため外見上の変化が生じてしまい，ハッシュ値に影響を及ぼしてしまうため登録時のハッシュ値取得の際にダミーの QR コードを証明書へ貼り付けることで，外見的変化によるハッシュ値への影響を防ぐ．貼り付けるダミーの QR コードについては，以下の 3.6 節にて説明する正規の QR コードの仕様と全く同じかつ，ダミーとして 0 で正規の QR コードに格納される情報と同じ長さにパディングした数値を格納するものとする．

取得するハッシュ値は，証明書全体及び顔画像部分のそれぞれである．これは証明書全体の真正性を検証するだけでなく，顔画像部分については敏感に変化を検知するためである．

© 2022 Information Processing Society of Japan

3.5 証明書記載の文字列の取得とハッシュ値への変換

3.1 節で述べた要件 2 を満たすため，OCR を用いて文字列を取得し，ハッシュ値への変換を行う．重要度の高い文字列の記載部分の画像は 3.3.1 項の処理にて抽出が行われているため，この画像に対して OCR を行うことで文字列の取得を行う．氏名は本人確認において重要でないと考えられるため，氏名部分は処理対象から除外した．なお取得した文字列から，空白並びに改行は削除する．空白や改行が削除された文字列から，SHA256 を用いてハッシュ値を求める．

3.6 ハッシュ値の署名

3.1 節で述べた要件 3 の署名の生成処理を行うため，証明書全体並びに顔画像部分のハッシュ値，文字列のハッシュ値に対してディジタル署名を行う．署名においては ECDSA を用いる．ECDSA はディジタル署名に楕円曲線暗号（ECC）を用いる手法であり，従来用いられている RSA よりもより短い鍵長で RSA と同等の安全性があるとされている [7]．なお本論文にて用いる楕円曲線パラメータは鍵長が 256bit である P-256 とする．

登録者 C は署名鍵 K_{Sign} と検証鍵 K_{Verify} を生成する．署名鍵 K_{Sign} は登録者がハッシュ値の署名を行う際に用い，検証鍵 K_{Verify} は検証者がハッシュ値の検証を行う際に用いる．署名鍵 K_{Sign} を用いてハッシュ値の署名を行う．先述した通りハッシュ値は 3 種存在しており 1 つの証明書に対して 1 つの署名とするため，ハッシュ値をビット列に変換しビット連接を行うことで 1 つのハッシュ値へ変換を行う．まず証明書全体のハッシュ値と顔画像部分のハッシュ値を結合する．結合することで得られるハッシュ値を H_{AF} とし，証明書全体のハッシュ値を H_A，顔画像部分のハッシュ値を H_F，ビットの連接に係る処理を記号 || と表した場合，ハッシュ値 H_{AF} は $H_{AF} = H_A||H_F$ と求められる．

また結合したハッシュ値と文字列のハッシュ値の結合を行う．得られるハッシュ値を H_{AFT} とし，証明書全体のハッシュ値と顔画像部分のハッシュ値を結合したハッシュ値を H_{AF}，文字列のハッシュ値を H_T としビットの連接に係る処理を記号 || と表した場合，ハッシュ値 H_{AFT} は $H_{AFT} = H_{AF}||H_T$ と求められる．

求めたハッシュ値 H_{AFT} に対して生成した署名鍵 K_{Sign} を用いて，署名 $Sign_C(H_{AFT})$ を $Sign_C(H_{AFT}) = Sign(H_{AFT}, K_{Sign})$ と生成する．

生成した署名 $Sign_C(H_{AFT})$ 並びに原本の証明書全体のハッシュ値と顔画像部分のハッシュ値を結合した H_{AF} を連接し QR コードを生成する．これは 3.1 節で述べた要件 4 の署名を証明書とともに保管できる手法を実現するものである．なお署名の検証に必要となる文字列のハッシュ値は検証時に登録時と同様の手順にて新たに取得を行うものとする．QR コードに格納するビット列を I とし，ビットの連接に係る処理を記号 || と表した場合，I は $I = Sign_C(H_{AFT})||H_{AF}$ と求められる．

なお格納する署名 $Sign_C(H_{AFT})$ 及び原本のハッシュ値 H_{AF} の長さは一定であり，また連接される順番も固定である．また用いる QR コードは python のライブラリである pyqrcode を用いて生成する．QR コードの種類はモデル 2 が用いられ，誤り訂正率は pyqrcode の規定値である 7%とする．

3.7 署名を用いた原本のハッシュ値の検証

3.1 節で述べた要件 3 の署名の検証処理を行うために，QR コードに格納された署名を用いて同様に格納されている原本のハッシュ値並びに文字列の真正性の検証を行う．

QR コードには電子署名 $Sign_C(H_{AFT})$ 及び原本のハッシュ値 H_{AF} が連接されたビット列 I 格納されている．また電子署名 $Sign_C(H_{AFT})$ 及び原本のハッシュ値 H_{AF} の長さ及び順序は固定であり，正規の処理を行うならば変化しないものである．従ってビット列 I より電子署名 $Sign_C(H_{AFT})$ の長さ分抽出すれば電子署名 $Sign_C(H_{AFT})$ が抽出可能である．またこれは原本のハッシュ値 H_{AF} においても同様である．QR コードよりビット列 I を取り出し，電子署名 $Sign_C(H_{AF})$ 及び原本のハッシュ値 H_{AF} に分割する．また 3.3.1 項の処理を行い文字列記載部分を抽出し，3.5 節の手法を用いて文字列をハッシュ値 H_T に変換する．また 3.6 節のハッシュ値の結合処理を同様に行う．なお本処理における結合は，QR コードに格納されていた原本のハッシュ値 H_{AF} と H_T の結合である．結合されたハッシュ値を H_{AFT} とする．電子署名 $Sign_C(H_{AF})$ 及びハッシュ値 H_{AFT}，検証鍵 K_{Verify} を用いて，原本のハッシュ値 H_{AFT} の真正性を $X = verify(Sign_C(H_{AFT}), H_{AFT}, K_{Verify})$ と検証する．なお検証鍵 K_V は署名鍵生成時に同時に生成され検証用プログラムに同封されているものとする．

検証が正常に成功した場合 True が返され署名並びに原本のハッシュ値並びに文字列は改竄されていないものとし，失敗した場合は BadSignatureError が生じ原本のハッシュ値並びに文字列の真正性が失われたものとする．

3.8 原本のハッシュ値と検証対象のハッシュ値のハミング距離を用いた真正性の検証

3.1 節で述べた要件 5 を満たすために，原本のハッシュ値と検証対象のハッシュ値のハミング距離を用いて検証を行う．なお 3.7 節において原本のハッシュ値の真正性は確認されているものとする．また検証対象のハッシュ値 H'_{AF} は節にて説明した手法で取得を行う．原本のハッシュ値を H_{AF}，検証対象のハッシュ値を H'_{AF} とした場合，ハミング距離 C_D は $D(H_{AF}, H'_{AF}) = H_{AF} \ XOR \ H'_{AF}$，$C_D = Count\{D(H_{AF}, H'_{AF})\}$ と求める．

© 2022 Information Processing Society of Japan

この際に取得するハミング距離 C_D は，結合された状態の原本のハッシュ値及び検証対象のハッシュ値の同一位置において異なる値を取っていた数の合計である．取得したハミング距離 C_D が設定されている閾値を下回っている場合真正性が保たれているものとし，超えた場合には真正性が保たれていない，つまり偽造や改竄が行われている可能性があるものとする．ハミング距離はあるビット列と他のビット列の情報の異なる数である．従って本論文においてハミング距離を原本と検証対象の変化量としてとらえるものとする．閾値を T とした際に $C_D < T$ のとき成功，$C_D \geq T$ のとき失敗となる．

なお，この閾値について，適切な値が不明なため適当に 7 と設定して評価を行った．設定した閾値が適切であるかについて考察の章にて述べる．

3.9 登録と検証の手順

実際に登録及び検証を行う際の手順について説明する．

まず署名にて用いる署名鍵と検証鍵を生成する．署名鍵は証明書登録機関にて保管を行い，検証鍵については検証プログラムに同封されて検証者に渡される．なお検証プログラム並びに検証鍵は第三者の認証局によって認証されたものとし，検証プログラム及び検証鍵の改竄は起こらないものとする．

登録について，顔画像付き証明書をスキャナによって電子化する．電子化したスキャンデータより 3.3 節にて説明した手順に則り証明書全体データ並びに顔画像部分のデータ，文字列記載部分のデータを取得する．また 3.8 節の手順を用いて証明書全体データ及び顔画像部分のデータの知覚ハッシュ値を取得する．加えて 3.5 節の手順を用いて文字列の取得，並びにハッシュ値への変換を行う．またこの際文字列の取得にあたっては，認識ミスにより異なる文字列を取得している可能性が存在している．そこで登録者による取得した文字列と認識された文字列を比較し，適宜修正を行ってから署名を行うものとする．取得した知覚ハッシュ値並びに文字列のハッシュ値を元に，3.6 の手順を用いて署名を行い QR コードの発行を行う．発行した QR コードを証明書に添付することで登録が完了する．

検証について，QR コード付き顔画像付き証明書をスキャナによって電子化する．スキャンデータから 3.3 節にて説明した手順に則り証明書全体データ並びに顔画像部分のデータ，文字列記載部分のデータを取得する．また同様に 3.8 節の手順を用いて証明書全体データ及び顔画像部分のデータの知覚ハッシュ値を取得し，3.5 節の手順に則りハッシュ値の取得を行う．また文字列の取得並びにハッシュ値の取得時において，文字列の誤認識の可能性が存在している．誤認識された文字列のハッシュ値は正当なハッシュ値と異なるため，署名の検証が成功しない．そこで署名の検証が失敗した際に文字列の誤認識を想定し，再度スキャンを行い新たなスキャンデータを用いて検証を行う．再スキャンの限度は 2 回までとし，2 回再スキャンを行ったとしても検証に失敗した際には検証者の目視による確認を行うものとする．検証者による確認では，証明書のスキャンデータ並びに取得した文字列を表示し，目視による確認を行い文字列が誤認識されていた場合には適宜文字列の修正を行い，検証を行うこととする．3.7 節にて説明した手順に従い，QR コードに格納されている情報の検証を行う．そして 3.8 節の手順を用いて検証対象の真正性について検証を行う．

表 1 設定した文字列
Table 1 Preset character strings.

サンプル 1	サンプル 2
Nationality:Japan	Covid19:positive
No:TT0001850	Covid19:Negative
Issuingcountry:JPN	vaccination
Dateofissue:11AUG2019	
Dateofexpiry:11AUG2024	
Authority:MINISTRYOFFOREIGNAFFAIRS	
RegisteredDomicile:TOKYO	

4. 評価

4.1 評価用サンプルについて

生成する証明書について，3.2 節にて述べた仕様に則り生成する．なお記載する氏名の生成については Fake Name Generator[8] を用いる．本実験にて用いる顔画像データベースは Face Latex Lab London Set[9] である．このデータベースには男性と女性それぞれ白人，黒人，西アジア人，東アジア人の顔画像が含まれている．原本となる証明書について黒人，西アジア人並びに東アジア人は男性女性両方において含まれている顔写真全てを用いて作成を行った．白人においては男性女性ともに無作為に 10 人ずつ抽出し証明書の作成を行った．作成された証明書の種別とサンプル数は，男性では白人，黒人，西アジア人，東アジア人の順に 10，8，5，5，女性では同順に 10，5，5，4 となった．

文字列が記載されたサンプルの生成において，任意の文字列を記載したサンプルを作成した．まず記載する任意の文字列を設定した．1 つのサンプルに設定した文字列がすべて入らなかったため，サンプルを 2 パターン作成し印刷を行った．それぞれのサンプルに記載する文字列は以下の **表 1** のとおりである．

氏名については GAIMU SAKURA とした．なお当初の設定としてはランダムな文字列を生成しサンプルに記載する予定であったが，OCR を用いた文字認識においては文面からの推測補正が掛かってしまい存在しない文字列を正確に読み取らせることが難しいため，有意味な文字列の記載を行うこととした．設定した文字列については外務省が掲載しているパスポートのイメージ [10] を参考にし，加えて昨今注目されているワクチン証明書に用いられると考え

© 2022 Information Processing Society of Japan

られる文字列を採用することとした．またそれぞれサンプルにおいて 100 枚分のスキャンデータを用意した．

偽造証明書の生成において，既に作成した証明書を偽造攻撃の対象とする．正当な証明書の顔画像部分より抽出し正当な所持者の顔画像とし，入手した顔画像と攻撃者とした顔画像を用いて，偽造証明書にて用いる顔画像を生成した．また生成手法においては，GAN を用いたモーフィング手法にて顔画像の生成を行った．なお偽造顔画像の生成に際して必要となる対象画像の潜在変数を抽出においては stylegan-encoder[11] を用いて行う．また Venkatesh らの既存研究 [12] 及び Zhang らの既存研究 [13] より，正当な顔画像の潜在変数を L_1 とし，攻撃者の顔画像の潜在変数を L_2 とした場合，偽造顔画像の潜在変数 L_M は $L_M = \frac{w_1 * L_1 + w_2 * L_2}{2}$ のように求められる．なお潜在変数 L_1 及び L_2 の算出方法は Venkatesh らの研究 [12] を参考とした．また上式にて用いられる重み w_1 及び w_2 は既存研究 [13] において 1 としているため，本論文においても w_1=w_2=1 とする．求めた L_M を styleGAN にて偽造顔画像を生成する際に明示的に指定することで偽造顔画像の生成が可能である．生成においては同性別同人種の顔画像を攻撃者の顔画像とした．特に黒人，西アジア人並びに東アジア人おいてはサンプル数が少ないため，すべての顔画像の組み合わせで生成を行った．白人においては再度サンプルの中から無作為に 10 人ずつ抽出し，攻撃者の顔画像として生成を行った．なお 10 人とした根拠としては，10 人×10 人で 100 枚のサンプルが生成でき，評価においてサンプル数 100 程度であれば偏った結果は生じにくいと考えたからである．作成した偽造証明書の種別とサンプル数は，男性では白人，黒人，西アジア人，東アジア人の順に 100，56，20，20，女性では同順に 100，20，20，12 となった．

作成した証明書は PX-105 を用いフォト光沢紙に印刷を行い，電子化時のスキャンには LP-M5300 を解像度 600dpi の設定で用いた．

4.2 ランダムノイズを持つスキャンデータのハッシュ値に関する評価実験

本評価は本提案手法が [要件 1] を満たしているか評価するものである．作成した正当な証明書の原本スキャンデータ各 1 枚取得し，スキャンを各証明書につき 10 回行い検証データとした．男性における原本としたスキャンデータと検証対象のスキャンデータのそれぞれの最大ハミング距離を**表 2** に，女性における原本としたスキャンデータと検証対象のスキャンデータのそれぞれの最大ハミング距離を**表 3** に示す．また女性及び男性における識別成功率を表 3 に示す．表 2 並びに表 3 を見ると，本評価実験において最大ハミング距離は閾値を下回るものであり，今回設定した閾値はランダムノイズを持ったスキャンデータであっても正確に同一証明書を識別できることが認められた．なお

表 2 男性における各サンプルの最大ハミング距離
Table 2 Maximum Hamming distance between samples of men.

サンプル番号	1	2	3	4	5	6	7	8	9	10
白人	2	0	2	2	0	0	4	4	2	0
黒人	4	0	2	2	0	0	2	2	-	-
西アジア人	2	2	0	0	0	-	-	-	-	-
東アジア人	2	2	2	2	2	-	-	-	-	-

表 3 女性における各サンプルの最大ハミング距離
Table 3 Maximum Hamming distance between samples of women.

サンプル番号	1	2	3	4	5	6	7	8	9	10
白人	0	2	0	2	4	2	0	2	0	2
黒人	2	2	4	2	0	-	-	-	-	-
西アジア人	2	2	4	0	4	-	-	-	-	-
東アジア人	2	2	2	0	-	-	-	-	-	-

同一証明書の識別成功率は男女ともに 100%であり，本提案手法がランダムノイズが加わっているスキャンデータにおいても同一証明書を正確に識別出来ていることが認められた．

4.3 文字列の認識についての評価実験

本評価は本提案手法が [要件 2] を満たしているか評価するものである．用意したスキャンデータに対して OCR を用いた文字列の認識を行い，なお本評価において，記載されている文字列を完全に認識することが出来たものを成功とし，1 文字でも読み誤った場合には失敗とした．両サンプルにおいて 90%以上の精度で文字認識を行うことが認められた．

4.4 署名と証明書を一体化して保管することに対しての評価実験

本評価は本提案手法が [要件 4] を満たしているか評価するものである．本提案手法において QR コードに格納される情報は 80byte である．したがって作成する QR コードは 80byte 全てが 0 のもの，また 80byte 全てが 1 のものである．両者を本論文が対象とする証明書と同サイズの画像へそれぞれ貼り付けたもののハッシュ値のハミング距離は 2 であり，QR コードの模様の差がハッシュ値に与える影響は小さいことが認められた．

4.5 偽造された証明書に対する本手法の性能の評価実験

本評価は本提案手法が [要件 5] を満たしているか評価するものである．作成した正当な証明書に対し本論文の手法を用いて原本データに対し署名並びに QR コードの付与を行った．また正当な証明書を元に作成した偽造証明書へ対応する QR コードの貼り付けを行い，検証を行った．男性

© 2022 Information Processing Society of Japan

表 4 男性及び女性の各人種における偽造画像の最小及び最大ハミング距離

Table 4 Minimum and maximum Hamming distance of fabricated images of men and women in each race.

	男性		女性	
	最小	最大	最小	最大
白人	16	40	14	36
黒人	16	40	12	44
西アジア人	22	36	16	36
東アジア人	16	36	18	30

表 5 男性及び女性におけるハミング距離の標準偏差及び平均値

Table 5 Standard deviation and average of Hamming distance of men and women.

	男性		女性	
	標準偏差	平均値	標準偏差	平均値
白人	6.60	26.4	5.33	23.2
黒人	5.50	28.0	9.34	26.3
西アジア人	5.17	26.1	4.95	23.4
東アジア人	4.79	25.6	5.01	21.8

表 6 閾値を変更した際の識別成功率

Table 6 Relation between identification success rates and threshold.

閾値	8	10	12	14
男性	100%	100%	99.99%	99.99%
女性	100%	100%	100%	99.95%

及び女性のの各人種における偽造画像の最小及び最大ハミング距離，並びに標準偏差及び平均値を**表 4** に示す．また男女におけるハミング距離の標準偏差並びに平均値を**表 5** に示す．偽造攻撃におけるハミング距離を示した表 4 を見ると最小ハミング距離は設定した閾値を大幅に超える結果であった．表 5 を参照すると，男性において標準偏差に大きな変化は認められ無いが，女性においては黒人において突出した値が認められた．また男性女性両方の全人種において 100%の精度で識別が成功した．

5. 考察

5.1 ランダムノイズに関する評価結果に対する考察

4.2 節にて，ランダムノイズを持つスキャンデータに対して評価を行った．本評価実験において観測されたランダムノイズは同一の証明書の識別において影響を与えないものであり，同一識別性能は十分であると考える．しかしランダムノイズが大きくなった場合においても同一証明書であるとする識別を行うため，閾値が本評価にて設定したものより緩和された場合での利用が想定される．そこで閾値を緩和した際においても精度を保ったまま偽造攻撃の識別を行えるか再評価を行う．閾値を変化した際の識別成功率を**表 6** に示す．

表 6 を参照すると本評価実験において閾値を 12 まで緩和した場合男性にて誤識別するようになり，14 まで緩和した場合男性及び女性の両方にて偽造証明書を正当な証明書であると誤識別するようになることが分かった．これは偽造証明書で閾値に近いような小さい値，特に 12 や 14 などの値が存在しているため，識別成功率が低下しているものと考える．したがって，誤識別の値は非常に小さいものの，現在設定している閾値の近い範囲で誤識別をしてしまい始めることが分かった．

5.2 文字列の認識に関する考察

4.3 節にて本論文にて設定している証明書のフォント等の設定が適切であるか評価を行った．本論文にて設定しているフォント等を用いたサンプルにおいてそれぞれ 96%，90%という認識成功率であった．認識成功率が 100%でない理由として，文字の切り出しの処理において文字が存在しない空間に文字があると認識してしまうことや，正当な文字が他の誤った文字としても誤認識されてしまうためであると考える．また最低でも 90%の精度であれば，認識のたびに人間の手による修正を必要とするような事態は避けられるのではないかと考える．

5.3 署名を一体化することに関する評価結果に対する考察

4.4 節にて QR コードの模様によるハッシュ値の影響を評価した．本論文にて行った評価実験においては最小の情報を格納した QR コードを貼り付けたものと最大の情報を格納した QR コードを貼り付けたもののハミング距離は 2 であり，QR コードの模様の差が識別に与える影響は小さいことが認められた．これは知覚ハッシュ関数がハッシュ値を計算する際に画像のリサイズを行うため，模様の変化が小さくなりハッシュ値への影響が少なくなるためであると考える．

5.4 偽造証明書に関する評価結果に対する考察

偽造証明書に関する評価結果に対して考察を行う．

まず偽造攻撃における評価実験のサンプル数が十分かどうかについて考察を行う．偽造攻撃の評価結果に対し Shapiro-Wilk の正規性検定を行い，それぞれの結果に対する正規性を調べた．結果として正規性が認められたものは男性の黒人及び東アジア人，女性の白人及び黒人，西アジア人であり，その他は正規性が認められなかった．そこで正規性が認められたものに対しては Welch の t 検定を，正規性が認められなかったものに対してはウィルコクソンの順位和検定を用いて両側検定を行う．それぞれの集団を 2 つのグループに分割し，2 つのグループが等しいことを帰無仮説とし，2 つのグループが等しくないことを対立仮説とした．結果としてすべての場合において帰無仮説が棄却されなかった．したがって 2 つのグループにおいて有意差

© 2022 Information Processing Society of Japan

が認められず，本評価におけるサンプル数は十分であったと考える．

また想定されるハミング距離のバラツキの範囲は，信頼区間 95.4%の場合「平均値± 2 ×標準偏差」として求められる．これを本評価実験に適用した場合の各性別各人種のそれぞれの値を**表 7** に示す．またこの平均値±標準偏差の値は正規分布に従う場合にのみ適応可能である．したがって正規性の検定において正規性が認められた男性の黒人及び東アジア人，並びに女性の白人及び黒人，西アジア人のみに適応し，値を求める．

表 7 男性及び女性における
予想されるハミング距離の下限値と上限値

Table 7 Predicted minimum and maximum Hamming distance of men and women.

	男性		女性	
	下限値	上限値	下限値	上限値
白人	-	-	12.5	33.8
黒人	17.0	39.0	7.62	44.9
西アジア人	-	-	13.5	31.7
東アジア人	16.0	35.1	-	-

表 7 より，男性並びに女性における予想されるハミング距離の下限値及び上限値を求めた．なお，本提案手法においては求められるハミング距離が閾値を超えていれば正常に偽造攻撃を識別できるため，予想される範囲の最小値である下限値のみを用いて考察を行う．表 7 を参照すると，求めることのできたすべての下限値において現在設定している閾値を超えるものであった．このことより，信頼区間 95.4%における男性の黒人及び東アジア人，並びに女性の白人及び黒人，西アジア人において設定された閾値が適切であると考える．また信頼区間 99.7%においては，女性の黒人において下限値がマイナスの値を取った．このことは先述した通り，結果全体の最小値と最大値が女性の黒人に含まれており，値のバラツキが顕著なため標準偏差の値が大きくなった影響であると考えられる．

従って本評価において，サンプル数が妥当であり，また信頼区間 95.4%において予想される値が設定した閾値を上回るものであったため，本評価結果の信頼性は十分にあると考える．

6. 結論

本提案手法に求められる要件に対して評価実験を実際に行った．4 章の評価結果より，本提案手法はすべての要件を満たしているといえる．また，いくつかの代表的な人種のすべてに適用可能であった．

参考文献

[1] Putro, P. A. W.: Physical Document Validation with Perceptual Hash, *Proc. 2017 3rd International Conference on Science in Information Technology (ICSITech)*, pp.582–587, (2017). doi: 10.1109/ICSITech.2017.8257180.

[2] Athichitsakul, P., Phimoltares, S. and Mahaweerawat, A.: Printout Verification Using a New Image Hash Algorithm Based on Radon, Wavelet, and Fast Fourier Transforms, *Proc. 2015 IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, pp.395–400, (2015). doi: 10.1109/ICCSCE.2015.7482218.

[3] P. A. W. Putro and M. Luthfi: An Authentic and Secure Printed Document from Forgery Attack by Combining Perceptual Hash and Optical Character Recognition, *Proc. 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, pp.157–162, (2019). doi: 10.1109/ICIMCIS48181.2019.8985190.

[4] 河内誠明，宇田隆哉，松下温：顔写真入り許可証向け署名の提案，電子情報通信学会，2006 年暗号と情報セキュリティシンポジウム (SCIS2006)，3D1-2, (2006).

[5] Gonzalez, S., Valenzuela, A. and Tapia, J.: Hybrid Two-Stage Architecture for Tampering Detection of Chipless ID Cards, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol.3, No.1, pp.89–100, (2021). doi: 10.1109/TBIOM.2020.3024263.

[6] Ambadiyil, S., Vibhath, V. B. and Pillai, V. P. M.: Performance Analysis and Security Dependence of on Paper Digital Signature Using Random and Critical Content, *Proc. 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, (2016).

[7] Barker, E.: *Recommendation for Key Management: Part 1 - General*, NIST Special Publication 800-57 Part 1 Revision 5, (2020). https://doi.org/10.6028/NIST.SP.800-57pt1r5

[8] *FakeNameGenerator*, https://www.fakenamegenerator.com/, 参照 2021-10-10

[9] DeBruine, L. and Jones, B.: *Face Research Lab London Set*, https://figshare.com/articles/dataset/Face_Research_Lab_London_Set/5047666, doi: 10.6084/m9.figshare.5047666.v5.

[10] 旅券（パスポート）の別名併記制度について，https://www.mofa.go.jp/mofaj/ca/pss/page3_002789.html, 参照 2022-01-17

[11] *stylegan-encoder*, https://github.com/Puzer/stylegan-encoder, 参照 2021-10-10

[12] Venkatesh, S., Zhang, H., Ramachandra, R., Raja, K., Damer, N. and Busch, C.: Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs? - Vulnerability and Detection, *Proc. 2020 8th International Workshop on Biometrics and Forensics (IWBF)*, pp.1–6, (2020). doi: 10.1109/IWBF49977.2020.9107970.

[13] Zhang, H., Venkatesh, S., Ramachandra, R., Raja, K., Damer, N. and Busch, C.: MIPGAN-Generating Strong and High Quality Morphing Attacks Using Identity Prior Driven GAN, *IEEE Transactions on Biometrics, Behavior, and Identity Science*, Vol.3, No.3, pp.365–383, (2021). doi: 10.1109/TBIOM.2021.3072349.

© 2022 Information Processing Society of Japan