Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13

画像の構造を考慮した 重畳画像認証の改良に関する一検討

宮地隆雄† 長谷川まどか† 田中雄一† 加藤茂夫†

画像認証方式は，覗き見攻撃に弱い傾向があり，近年，これに対して様々な対策が研究されている．これまで我々は，画像の高周波成分は離れた位置からの認識が困難という性質に着目した重畳画像認証方式を提案し，その有効性を検証してきた．しかし，本方式は重畳する画像によっては，認証に適さない画像となる可能性があった．そこで本稿では，前景および背景画像の構造に着目し，それらの高周波成分に応じて前景画像の補正を行う手法について検討を行ったので報告する．

A Study on Improvement of Hybrid Image Authentication by Considering Image Structure

Takao Miyachi† Madoka Hasegawa† Yuichi Tanaka† and Shigeo Kato†

Although graphical passwords are easy to memorize, they are vulnerable against an observation attack. To solve this problem, we propose a graphical password method which is difficult for observers to recognize pass-images. And we have conducted a user study about usability and robustness against shoulder-surfing. This method uses hybrid image, but a hybrid image which is not suitable for authentication may be used in this method. In this paper, we study on improvement of our method by considering image structure.

1. はじめに

現在のユーザ認証方式は，パスワードや暗証番号など，文字列を用いたテキストパスワード方式が主流である．テキストパスワード方式は汎用性と利便性に優れているため，様々なシステムで利用されているが，WEB サービスの増加に伴い，1 人のユーザが管理するアカウントやパスワードの数は増大してきている．しかし，ランダムで長い文字列を記憶することは人間にとって容易でないことが多いため，ユーザは短い文字列や，自分の誕生日や名前など，記憶の容易なパスワードを設定したり，パスワードを紙などに書いて記録したりする傾向がある．その結果，第三者によるパスワードの予測や辞書攻撃によるパスワードの漏えい，パスワードの盗難などを招く恐れがある．また，コンピュータウイルスに感染し，PC にキーロガーが仕組まれると，テキストパスワードは容易に盗まれるという危険性がある．さらに，異なるシステムで同じパスワードを使いまわすことも多く，あるシステムでパスワードが漏えいすると，他のシステムにも影響を及ぼすことも問題としてあげられる．

これらの問題に対処する代替の認証方式としては様々な方式が提案されているが，その一つとして，画像認証がある[1]-[6]．画像認証とは，テキストパスワード方式における文字列の代わりに，画像を用いて認証を行う方式である．認証に画像を用いる利点としては，画像が人間にとって記憶が容易であり，またキーロガーなどで盗むことが困難であることがあげられる．画像認証での画像の使い方は方式によって異なるが，いずれも画像を使用することで，ユーザに要求する記憶負荷を軽減している．

テキストパスワード方式では，ユーザがパスワードを入力することで本人認証を行うが，画像認証では，システムが 1 枚以上の画像をユーザに提示し，ユーザは提示された画像に関して何らかの質問に回答し，その正誤で本人認証を行う．画像認証は 2 つの方式に大別できる．1 つ目は，囮を含む複数枚の画像の中から，ユーザがあらかじめパスワードの代わりとして登録しておいた画像（以下，パス画像と呼ぶ）を正しく選択することで認証を行う方式[1]-[5]であり，もう一つは 1 枚の画像に描かれている数個のオブジェクトや，位置，選択順序などをあらかじめ登録しておき，登録した通りに入力することで認証を行う方式[6]である．

本研究では，前者の画像選択型の方式に焦点を当てる．画像認証では，認証のたびにパス画像をディスプレイに表示するため，第三者による認証行為の覗き見（以下，覗き見攻撃）によりパス画像が漏えいする危険性があり，様々な方策が取られているが，画像の記憶の容易さとのトレードオフが存在する．

Dhamija らの提案する Déjà Vu[2]では，ランダムアートと呼ばれる，一見して意味がない幾何学模様の画像をパス画像に使用している．これにより，他人によるパス画像

† 宇都宮大学大学院工学研究科
Graduate School of Engineering, Utsunomiya University

ⓒ2011 Information Processing Society of Japan

Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13

の推測を困難にしているが，ユーザ本人の記憶負荷も高い．一方，有意味な画像を使ったシステムとしてはあわせ絵[4]や Passfaces[5]などがある．あわせ絵ではユーザが撮影した写真を使用しており，Passfaces は人物の顔画像を使用している．これらの方式は，ユーザの記憶負荷の低減が期待できるが，推測攻撃や覗き見攻撃への耐性の面で課題を残している．

これに対し我々は，記憶負荷の軽減と覗き見耐性を両立することを目的として，離散ウェーブレット変換(Discrete Wavelet Transform, DWT)を用いてパス画像と囮画像を合成した画像を画像選択型の認証に使用する方式を提案し，ユーザビリティと覗き見攻撃耐性の評価を行ってきた[7]-[9]．本方式では，DWT を用いてパス画像である前景画像の高周波成分と囮となる背景画像の低周波成分を合成した画像を作成して使用する．本方式は，画像の高周波成分は離れた位置からの認識が困難であるという人間の視覚特性を利用しており，ディスプレイから離れて覗き見を行う者に対してパス画像の認識が困難になることが期待される．一方で，ディスプレイの正面で認証を行うユーザにとっては，パス画像の認識が容易であるという特徴がある．また，パス画像の高周波成分のみをシステムに保存しておけばよいため，必要な記録容量も減少する．

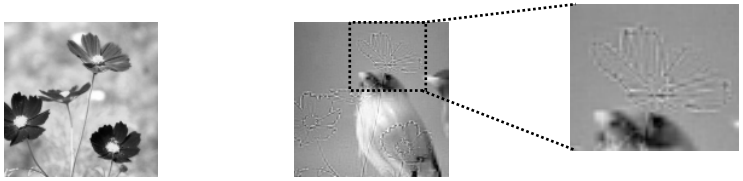
しかし，本方式には，パス画像の視認性は合成する画像の内容に依存するという問題が残されている．例えば，合成する背景画像が画素値の変化の少ない平坦な画像の場合，合成後のパス画像は比較的視認性が高くなる傾向がある．このような画像は認証を行うユーザにとって見やすい画像であるものの，覗き見攻撃者にとっても見やすくなるといった問題がある．逆に，覗き見攻撃者にとって見にくい画像の場合は，正規のユーザにとってユーザビリティを損ねたものとなる可能性が考えられる．

そこで本研究では，上記の問題点を解決することを目的とし，方式の改良手法について検討を行う．パス画像の視認性に影響する要因としてはいくつか考えられるが，今回の検討では画像の構造，および，前景画像と背景画像の周波成分の大きさに着目し，パス画像の視認性を調整する方式を検討する．

2. DWT を用いた重畳画像認証

2.1 方式の概要

著者らがこれまでに提案した DWT を用いた重畳画像認証は，パス画像の高周波成分を，別の画像の低周波成分と合成することにより作成した画像を使用する方式である．作成される画像は，図 1(b)に示すような，パス画像の高周波成分を，囮画像の上に重ねた画像である．一般に，画像の高周波成分は，近くで見た場合は認識が容易であるが，離れた位置からは認識が困難になるという性質がある．また，覗き見攻撃は認証画面からある程度離れた位置で行われると考えられる．DWT を用いた合成画像認証は，これらの性質に着目しており，パス画像の高周波成分を合成した画像を使用することで，覗き見を行う攻撃者にとってパス画像の認識を困難にすることを目的とした方式である．なお，別画像の低周波成分も使用するのは，覗き見をさらに困難にするためである．認証で使用する画像は，離散ウェーブレット変換により，画像から各周波成分を抽出し，それらを合成するという手順で作成される．



(a) パス画像　　(b) 重畳画像とその拡大図(一部)

図 1　DWT を用いた重畳画像

認証画面の例を図 2 に示す．認証時には，上記の手順で作成された画像がユーザに複数枚提示される．提示画像には，囮画像の高周波成分を別の囮画像の低周波成分と合成した画像も含まれる．ユーザはその中から，パス画像の高周波成分が合成された画像を選択するように要求される．このとき，パス画像を正しく回答できれば，認証成功となり，システムにログインすることができる．ただし，パス画像および囮画像には，認証の度に異なる囮画像の低周波成分が合成される．認証の度に組合せを変えることで，低周波成分画像の記憶により高周波成分画像が特定されるのを防いでいる．

画像の高周波成分のみを認識するという認証方法にすることで，認証画面に近い位置で認証操作を行う正規のユーザは画像を認識でき，逆に，認証画面から離れて覗き見を行う者は画像の認識が困難になることが期待される．

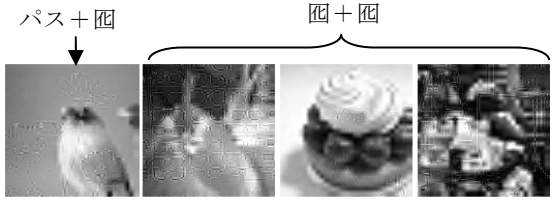


図 2　認証画面の例

ⓒ2011 Information Processing Society of Japan

Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13

2.2 重畳画像の作成手順

DWT を用いた重畳画像の作成方法を述べる．図 3 に高周波成分として合成する画像を前景画像，低周波成分として合成する画像を背景画像として，それらを合成する処理の流れを示す．画像から高周波成分と低周波成分を抽出するために，離散ウェーブレット変換を使用する．

まず，前景画像と背景画像の両方に DWT によるオクターブ分割を施す．*n* 回のオクターブ分割により，画像を各サブバンドに分け，画像の高周波成分と低周波成分を得る．2 回のオクターブ分割の例を図 4 に示す．各サブバンドは，それぞれ異なる周波数成分を持っており，LL*n* バンドが最低周波数成分，HL1 バンド，LH1 バンド，HH1 バンドが高周波成分である．

次に，背景画像の LL*n* バンドの変換係数と，前景画像の HL1 バンド，LH1 バンドおよび HH1 バンドの変換係数を合成し，さらに，それら以外の周波数成分におけるサブバンドの値を 0 としたに変換係数信号を作成する．ここで，残りのサブバンドの値を 0 とするのは，背景画像からエッジ情報を削減し，前景画像におけるエッジ情報を相対的に強調するためである．

最後に，合成した変換係数信号に対して逆ウェーブレット変換（IDWT）を施し，本方式で使用する重畳画像を得る．また入力画像がカラー画像の場合は，各カラープレーンに対して上記の処理を行うことで，同様の画像を得ることが可能である．

なお，本方式におけるウェーブレット変換としては，画像符号化の国際標準方式 JPEG2000 で使用されている可逆 5×3 変換[10]を使用している．

2.3 問題点

DWT を用いた重畳画像認証における問題点について述べる．我々のこれまでの研究では，DWT を用いた重畳画像を認証に用いることで，ユーザビリティを保ちつつ，覗き見攻撃に対しても有効であることを示してきた．しかし，一部の画像の組み合わせによる重畳画像では，必ずしもユーザビリティと覗き見攻撃耐性を両立した画像とならない場合がある．

図 5 は前景画像の視認性が高い重畳画像の例であり，図 5(a)の画像を前景画像として，ある背景画像と合成した重畳画像を図 5(b)に示している．図 5(b)の重畳画像は，前景画像のエッジ部分が明確に見てとれるため，前景画像の視認性が高い重畳画像であると考えられる．このような画像の場合，正規のユーザにとって見やすい画像になるが，その一方で覗き見攻撃を行う者にとっても見やすくなる可能性があり，安全性を損ねた画像になってしまう．また，図 6 は前景画像の視認性が低い重畳画像の例であり，図 6(a)の画像を前景画像として，ある背景画像と合成した重畳画像を図 6(b)に示している．図 6(b)のような重畳画像は，前景画像のエッジ部分が見にくくなっており，前景画像の視認性が低い画像となっている．そのため，覗き見を行う者にとって，

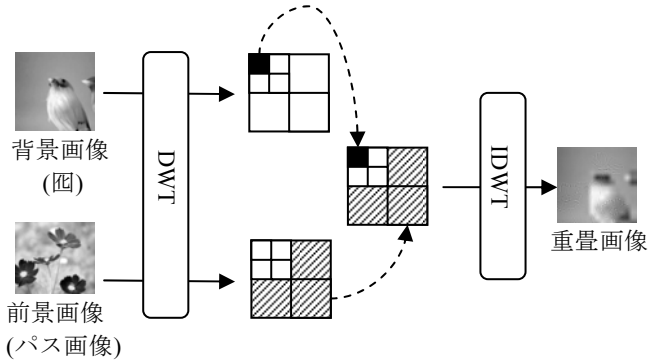


図 3　重畳画像の作成

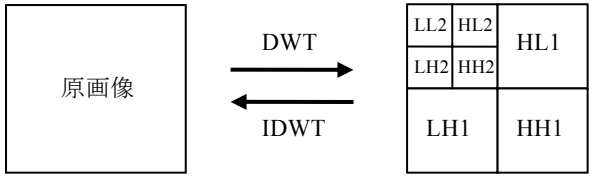


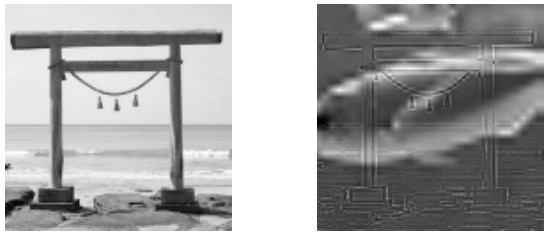
図 4　オクターブ分割

前景画像が見にくくなりパス画像の盗難が困難な画像と考えられるが，このような画像ではユーザビリティが損なわれてしまうと考えられる．

以上のように，画像の組み合わせ次第で認証に適さない重畳画像となる場合がある．したがって，覗き見によりパス画像を視認できる画像では，パス画像を見にくくし，逆に正規ユーザにとってパス画像が認識しにくい画像では，パス画像を見やすくする工夫が必要であると考えられる．しかし実際には，前景画像と背景画像内のオブジェクトの配置によって，局所的に見やすかったり，見にくかったりするため，上記のような処理を行う場合は，画像内のオブジェクトの配置を考慮した局所的な処理が必要である．

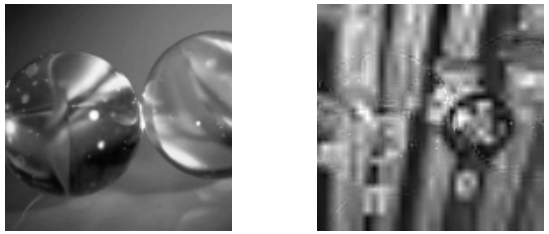
ⓒ2011 Information Processing Society of Japan

Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13



(a) 前景画像　　(b) 重畳画像

図 5　視認性の高い重畳画像の例



(a) 前景画像　　(b) 重畳画像

図 6　視認性の低い重畳画像の例

3. 画像の構造を考慮した重畳画像認証の改良

本節では DWT を用いた重畳画像認証の改良手法について述べる．本研究では，重畳画像において，前景画像が見にくい部分を見やすく，視認性が高すぎる部分は視認性を抑えるように，前景画像を局所的に補正することを目的とする．そこで，重畳画像における前景画像の視認性は，前景および背景画像の性質に依存するものと考え，主に 2 つの点に着目する．

まず 1 つ目に，背景画像中の空や壁などの平坦な部分では前景画像の視認性が高くなりやすく，逆に背景画像であってもオブジェクトがあるような平坦でない部分では前景画像がマスクされ視認性が低くなりやすいことに着目する．図 7(a)は，前景がコスモス，背景がひまわりの画像であるが，背景画像の空の部分のように，平坦であるほど前景画像が見やすく，ひまわりがある部分は前景が見にくくなっていることが分かる．2 点目としては，DWT により得られた前景画像の高域の変換係数の値が大きいほど，視認性は高くなりやすいことが挙げられる．図 7(b)は図 7(a)で使用した前景画像の高域の変換係数を 2.5 倍に強調処理した画像であるが，こちらの方が前景画像の

(a) 重畳画像　　(b) 前景画像の強調

図 7　前景画像の視認性

視認性が高いことが分かる．これらのことを考慮して，前景および背景画像の構造から前景画像の補正処理を行うことを検討する．

図 8 に改良手法における前景画像の補正処理の手順を示す．本方式では，前景画像の高域の変換係数（HH1, HL1, LH1 バンド）に対してある実数 α を乗算することで，前景画像の補正を行う．このとき，α の値が 1 未満の場合は前景画像の視認性を低くする減衰処理，α の値が 1 より大きい場合は前景画像の視認性を高くする強調処理となる．ただし，実数 α は高域の変換係数 1 つごとに決定する値であり，前景の視認性が低い部分の変換係数に対する α の値は大きく，視認性が高い部分の変換係数に対する α の値は小さくする．

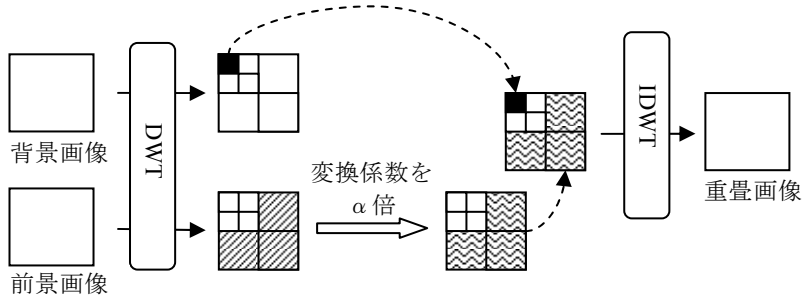


図 8　補正処理の概要

ここで実数 α は，式(1)のように，背景画像の変換係数から決定される変数 α_B と，前景画像の変換係数から決定される変数 α_F の関数により決定する．

$$\alpha = f(\alpha_B, \alpha_F) \tag{1}$$

ⓒ2011 Information Processing Society of Japan

Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13

変数α_Bは背景画像の変換係数から決定される値であり，背景画像の平坦部では小さく，エッジ部では大きくなるように決定する．平坦さの度合いは，背景画像のLLnバンドに残存する高周波成分から判断するため，LLnバンドをさらにウェーブレット変換して得られるLHn+1，HLn+1，HHn+1バンドの変換係数から決定する．各帯域内の変換係数が小さいほど平坦であると判断してα_Bの値を小さくし，逆に，変換係数が大きい場合は平坦ではないと判断してα_Bの値を大きくする．

一方，変数α_Fは前景画像の高域の変換係数から決定される変数であり，変換係数が小さいほどα_Fの値を大きくし，大きいほどα_Fの値を小さくする．これにより，前景画像の視認性の低い部分を見やすくし，視認性が高すぎる部分は見やすさを抑えることができると考えられる．

これを実現するため，今回の検討では，α_Bとα_Fは，あらかじめレンジを設定し，着目する変換係数値をレンジ内の値に線形変換することで算出するものとした．α_B，α_Fの算出式を式(2)，式(3)に示す．

$$\alpha_B = \frac{R_{\max} - R_{\min}}{|C|_{\max} - |C|_{\min}} \left(|C_B| - |C|_{\min} \right) + R_{\min} \tag{2}$$

$$\alpha_F = \frac{R_{\min} - R_{\max}}{|C|_{\max} - |C|_{\min}} \left(|C_F| - |C|_{\min} \right) + R_{\max} \tag{3}$$

ここで，$R_{\max}$，$R_{\min}$はそれぞれ左辺のパラメータ(α_Bまたはα_F)のレンジの最大値と最小値であり，$|C_B|$，$|C_F|$は入力となる変換係数の絶対値である．また，$|C|_{\max}$, $|C|_{\min}$はそれぞれ着目する帯域内の変換係数の絶対値の最大値と最小値である．

以上の方法により，対応関係にある変換係数から求めたα_Bとα_Fからαを算出し，対応する前景画像の変換係数にαを乗じることで，前景画像の補正を行う．図9に変換係数の対応関係を示す．オクターブ分割をn回行ったとき，LLnバンドと原画像の縦横のサイズ比は1:2^nとなるため，背景画像のLHn+1，HLn+1，HHn+1バンドの変換係数1つに対して，前景画像のLH1，HL1，HH1バンドの$2^n \times 2^n$の変換係数が対応する．

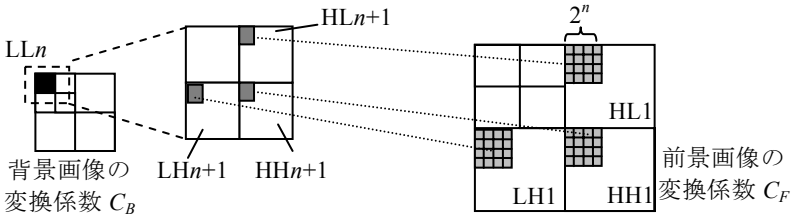


図 9　変換係数の対応関係

4. シミュレーション

4.1 シミュレーション条件

本手法を用いて画像を生成する実験を行った．本手法は，画像の高域の変換係数を線形変換することで，画像の補正を行う2つのパラメータα_B，α_Fを算出しαを決定するが，シミュレーションでは各パラメータの効果を評価することを目的とし，α_Bおよびα_Fのダイナミックレンジを個別に変えた場合の結果を示している．その際，αはα_Bとα_Fの積により算出したが，α_Bについてのシミュレーションでは常にα_F=1とし，α_Fのシミュレーションでは常にα_B=1として算出した．なお，重畳画像を作成する際のウェーブレット変換におけるオクターブ分割の回数は2回とした．また，使用した画像はサイズが128×128画素のカラー画像である．使用画像を図10に示す．

(a) 背景画像　　(b) 前景画像

図 10　使用画像

4.2 シミュレーション結果

シミュレーション結果について以下に述べる．ただし以下の結果は，背景画像から決定される変数α_Bと，前景画像から決定される変数α_Fについて，それぞれ個別にシミュレーションを行った結果を示している．つまり，α_Bおよびα_Fを用いて式(1)により決定されるαについては考察を保留し，α_Bおよびα_Fそれぞれにおける重畳画像の補正効果を検証する．

図11は背景画像から決定されるα_Bのみを前景画像の高周波成分に乗算した結果である．図11は左から順に補正を行っていない重畳画像，α_Bのレンジを0.5から3.0とした重畳画像，α_Bのレンジを0.5から6.0とした重畳画像となっている．結果より，背景画像において平坦となっている部分では，補正なしの画像よりも補正を行った画像の方が，前景画像が若干目立たなくなっていることが確認できる．また，平坦でない部分に関しては，α_Bのレンジが大きい場合に，補正なしの画像よりも補正を行った画像の方が，視認性が高くなっていることが分かる．ただし，前景画像において視認性が低い部分と，背景画像の平坦な部分が重なっている場合，その部分での前景画像は視認性が極端に低下してしまうという問題がある．そのため，このような組み合わせにおいて前景画像の強度を下げすぎないパラメータの決定について今後検討する必要がある．

ⓒ2011 Information Processing Society of Japan

Vol.2011-CSEC-54 No.32
Vol.2011-SPT-1 No.32
2011/7/13

(a) 補正なし　(b) α_B=0.5～3.0　(c) α_B=0.5～6.0

図 11　背景画像の構造を考慮した重畳画像

図 12 は前景画像から決定される α_F のみを前景画像の高周波成分に乗算した結果である．図 12 は左から順に補正を行っていない重畳画像，α_F のレンジを 0.5 から 1.5 とした重畳画像，α_F のレンジを 0.5 から 2.0 とした重畳画像となっている．図より，補正なしの画像において視認性の低かった部分が，補正後の画像では見やすくなっていることが分かる．しかし，補正なしの場合でも十分に視認性の高かった部分でも，必要以上に強調されていることも分かる．そのため，前景画像において視認性が十分高い部分においては，必要以上に強調しないパラメータの決定についても今後検討する必要がある．

(a) 補正なし　(b) α_F=0.5～1.5　(c) α_F=0.5～2.0

図 12　前景画像の構造を考慮した重畳画像

5. おわりに

本研究では，これまでに我々が提案してきた DWT を用いた重畳画像認証の改良手法について検討を行った．改良手法としては，画像の構造と画像信号のウェーブレット変換の変換係数の値に着目し，背景画像および前景画像の変換係数の大きさから前景画像の補正量を決定する手法を提案した．シミュレーションより，背景画像の変換係数から，背景画像が平坦な部分では前景画像の視認性を低くし，背景画像が平坦でない部分では前景画像の視認性を高く補正できることを確認した．しかし，前景画像の変換係数から前景画像を補正する効果については，良好な結果が得られず，今後さらなる検討が必要であると考えられる．

また，各パラメータについては，画像ごとに適切な値は異なると考えられる．今回はパラメータのレンジを実験的に決定したが，今後は画像の高周波成分などから，α を自動で決定する手法についても検討が必要である．さらに，本手法の有効性については，複数人の被験者による評価実験を行い，ユーザビリティと覗き見攻撃耐性の観点から評価することが必要であると考えられる．

最後に，今回は画像の構造に着目して前景画像を補正する手法を提案したが，色情報も前景画像の視認性に影響する要素のひとつとして考えられる．そこで今後は，色情報が前景画像の視認性に与える影響についても調査し，色情報から前景画像の補正を行うことも検討する予定である．

謝辞

本研究の一部は科学研究費補助金基盤(C)(22500105)の助成を受けたものである．

参考文献

1) I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," Proceedings of the 8th USENIX Security Symposium, 1999.
2) Rachna Dhamija, Adrian Perrig, “Déjà Vu: A User Study Using Images for Authentication,” 9th USENIX Security Symposium, pp.45-58, 2000.
3) 山本匠, 漁田武雄, 西垣正勝, "不鮮明化画像を利用した暗示・応答型画像認証方式の提案," 情報処理学会論文誌, vol.50, no.9, pp.2062-2076, Sept. 2009.
4) 高田哲司, 小池英樹, "あわせ絵: 画像登録と利用通知を用いた正候補選択方式による画像認証方式の強化法," 情報処理学会論文誌, Vol.47, No.8, pp.2602-2612, Aug. 2006.
5) passfaces, http://www.passfaces.com/
6) S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, ``PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies, Vol.63, pp.102-127, 2005.
7) Madoka Hasegawa, Yuichi Tanaka and Shigeo Kato, “A Study on an Image Synthesis Method for Graphical Passwords,” Proc. of ISPACS, pp.643-646, Dec. 2009.
8) Madoka Hasegawa, Takao Miyachi, Yuichi Tanaka and Shigeo Kato, “A Graphical Password Using Discrete Wavelet Transform and Its Evaluation,” Proc. of IEVC2010, 1P-5, Mar. 2010.
9) Takao Miyachi, Keita Takahashi, Madoka Hasegawa, Yuichi Tanaka, Shigeo Kato, "A Study on Memorability and Shoulder-Surfing Robustness of Graphical Password Using DWT-Based Image Blending," Proc. of PCS 2010, pp. 134 - 137, Dec. 2010.
10) 小野定康, 鈴木純司, “わかりやすい JPEG2000 の技術,” オーム社, 2003.

ⓒ2011 Information Processing Society of Japan