Vol.2012-CSEC-58 No.46
Vol.2012-SPT-4 No.46
2012/7/20

ハイブリッド画像を利用した 画像選択型認証のための画像対選定に関する一検討

高橋渓太[†]　長谷川まどか[†]　加藤茂夫[†]

画像選択型認証の覗き見防止策のひとつとして，ハイブリッド画像を利用する方式がある．この手法では，画像の高周波成分は遠方からの認識が困難という性質に着目し，パス画像の高周波成分をおとり画像に重畳した画像を使用している．しかし，画像の組み合わせによっては，認証に不適当な重畳画像となる場合がある．そこで，本研究では，このような認証に適さない画像対を事前に除去することを目的として，画像の構造情報を利用した客観的画像対評価尺度を考案し，主観評価との関連について検討を行ったので報告する．

A Study on Image Pair Selection for Graphical Password Using Hybrid Images

KEITA TAKAHASHI[†]　MADOKA HASEGAWA[†]　SHIGEO KATO[†]

We discuss a structural similarity evaluation method in order to generate hybrid images for graphical password. The hybrid image consists of two components. One is high spatial frequencies of a key image and the other is low spatial frequencies of a decoy image. Visibility of the hybrid image depends on the viewing distance and the structural similarity of the images. This property of the hybrid image is useful for preventing shoulder-surfing of graphical password. However, an evaluation method for checking whether the decoy image is appropriate to overlay on the key image has not been established. To address this issue, we utilize structural information of the images. A user study with 20 participants has been performed to test the visibility of key images in the hybrid images. Experimental results show that our similarity measure mostly coincides with the subjective visibility of the key image.

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の文字列を秘密情報として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高い汎用性や利便性を有するため様々なシステムで広く利用されているが，その一方で，近年の Web サービスの多様化に伴い，ユーザが管理すべきアカウントやパスワードの数は年々増加してきており，ユーザの記憶負荷が問題となっている．ランダムで長い文字列を記憶することは人間にとって困難である場合が多いため，ユーザは単純で短い文字列や，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き留めたりすることが多い．その結果，第三者による推測攻撃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 [1) 2)]．また，日常的に使用する PC にキーロガーが仕組まれることによって，テキストパスワードは容易に盗まれるという危険性もある．さらに，同一のパスワードを複数のシステムで使い回す場合も多く，あるシステムにおけるパスワードの漏えいが別のシステムにも影響を及ぼすことも問題として挙げられる．

前述の問題に対処するための方式は数多く提案されているが，そのひとつに画像認証がある [3) -12)]．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替として，画像を用いて認証を行う方式である．秘密情報を画像とすることで，記憶容易性や想起性の向上を図ることが可能であり，キーロガーによる秘密情報漏えいの危険性が低い．

テキストパスワード方式ではユーザにパスワードの入力を求め，事前に登録した文字列と一致するか否かで本人認証を行うが，画像認証では提示された画像に関する何らかの質問に対する応答が正しいか否かで本人認証を行う．画像認証における画像の使い方は，画像選択型方式と画像内選択点再現型方式の 2 種類に大別できる．画像選択型認証の代表的な方式として Déjà vu[4)] や Passfaces[5)]，画像内選択点再現型方式の代表例として PassPoints[6)] が挙げられる．本研究では，前者の画像選択型認証に着目する．

画像選択型認証では，ユーザが鍵として記憶した画像とおとり画像とで構成される複数枚の画像の中から，ユーザがあらかじめ鍵として登録しておいた画像を正しく選択することで本人認証を行う．以下，ユーザが自分の鍵として登録した画像をパス画像と呼ぶものとする．この方式では，認証操作のたびにパス画像がディスプレイに表示されるため，第三者による認証操作の覗き見によってパス画像が漏えいする危険性が存在する．覗き見防止策として，認証に用いる画像を不鮮明化する方策が提案されており，モザイクフィルタを利用する方式 [7) -9)]，油彩フィルタを利用する方式 [10)]，ハイブリッド画像を利用する方式 [11) 12)] などがある．ハイブリッド画像 [13) 14)] とは，2 枚の異なる画像の高周

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

波成分と低周波成分とを合成することで作成される重畳画像であり，眺める距離によってその見え方が変化する．これまでの研究において，我々は，ハイブリッド画像における高周波成分は，遠方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，覗き見に頑健な画像選択型認証法を提案した [11) 12)]．本方式では，画面近くで操作する正規ユーザだけが知覚すべき画像（以下，前景画像と呼ぶ）の高周波成分を，おとりとなる無意味な画像（以下，背景画像と呼ぶ）の低周波成分に重畳しているため，背後から認証操作を覗き見られた場合でもパス画像の漏えいが発生しにくい．

しかしながら，重畳する画像の組み合わせによっては，前景画像の高周波成分を背景画像の低周波成分で十分にマスキングすることができず，認証に不適当な重畳画像となる場合がある．加えて，実際に認証システムを運用する際には，膨大な数の画像の中から重畳に適した背景画像を選択し，前景画像と重畳する必要があるため，認証に適した画像対の評価尺度の確立が望まれる. そこで, 本研究では，認証に不適当な画像対を事前に除去することを目的として，画像の構造情報を利用した客観的画像対評価尺度を考案し，ユーザ実験による画像対の主観評価結果と提案する評価尺度との関連について検討を行ったので報告する．

以下の本稿の構成は次のとおりである. まず, 2 節では，研究対象であるハイブリッド画像を用いた画像選択型認証について説明する．3 節では，提案手法である，画像の構造情報を利用した客観的画像対評価尺度について述べる. 4 節では，主観的な画像の見え方と，提案する客観的評価尺度との関連を評価するためのユーザ実験について説明する．最後に 5 節において, まとめと今後の課題について述べる．

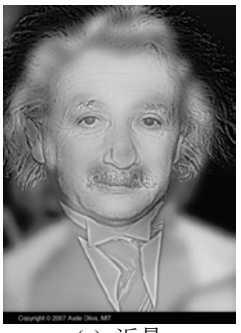
2. ハイブリッド画像を用いた画像選択型認証

2.1 ハイブリッド画像

ハイブリッド画像は，ある画像の低周波成分と，別の画像の高周波成分とを組み合わせて作成される．人間の視覚には，画像の高周波成分を遠方から認識することが困難であるという特性があり，ハイブリッド画像ではこれを利用することで，距離に応じて見え方が変化する画像を生成している．図 1 は，アインシュタインの顔写真の高周波成分と，マリリン・モンローの顔写真の低周波成分とを組み合わせて作られたハイブリッド画像の一例である [14)]．近距離で見る場合，高周波成分が目立つため図 1(a)のようにアインシュタインの顔写真に見えるが，遠方から眺める場合は低周波成分によって高周波成分がマスキングされ，同図(b)のようにマリリン・モンローの顔写真に見える．

2.2 画像選択型認証への応用

図 2 に認証システムのユーザインタフェースの構成例を示す．まず，認証システムは複数枚のハイブリッド画像を画面上に提示する．このうちの 1 枚はパス画像の高周波成分とおとり画像の低周波成分を組み合わせたものである．残りのハイブリッド画像は，2 枚の異なるおとり画像を組み合わせて作成したものである．正規ユーザは実際の認証時に，システムから提示された複数のハイブリッド画像の中から，ユーザ自身が事前に設定したパス画像の高周波成分が用いられているものを探し，選択する．このチャレンジ＆レスポンス操作を複数回繰り返すことで，本人認証が行われる．登録する画像の枚数や，チャレンジ＆レスポンス操作回数が多いほど，パスワード空間が広くなるが，記憶しなければならない画像の枚数も増える．



(a) 近景　(b) 遠景

図 1　ハイブリッド画像 “Marylin Einstein” [14)]

Figure 1　Hybrid image “Marylin Einstein”. [14)]

図 2　認証システムの一例

Figure 2　Example of an authentication system.

2.3 問題点

覗き見攻撃者は正規ユーザの背後の離れた位置から覗き見を試みるため, 前景画像の高周波成分は視認しにくい. しかしながら，背景画像の低周波成分が平坦である場合，前景画像の高周波成分が十分にマスキングされず，部分的に視認可能となる場合がある．例えば，図 1 における襟カラーの部分は，背景画像が平坦であると同時に前景画像が特徴的であるため，遠距離でも視認できる可能性がある．ハイブリッド画像を画像認証に利用するには，高周波成分を効果的にマスキングすることができない背景画像を事前に除去することが重要であり，マスキングの度合いを測る客観的画像対評価尺度が必要である．

3. 画像の構造情報を利用した客観的画像対評価尺度の提案

提案する画像対評価尺度では，“背景画像のオブジェクト領域が前景画像のオブジェクト領域と重なりマスキングする度合い”を，画像類似度として定義する．ここで，オブジェクト領域とは，画像中における特徴が顕著な領域を表す．また，本研究では，画像のオブジェクト領域を検出

Vol.2012-CSEC-58 No.46
Vol.2012-SPT-4 No.46
2012/7/20

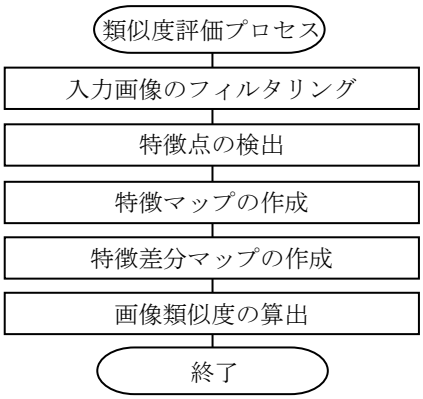


図 3　類似度評価プロセス

Figure 3　Similarity evaluation process.

するための手法として，SURF (Speeded Up Robust Features) [15] に着目する．図 3 に類似度評価処理のプロセスフローを示し，図 4 に各プロセスにおける出力画像を示す．以下では，各プロセスを順に説明する．

ステップ 1: 入力画像のフィルタリング

前景画像 I_H に対して高域通過フィルタを適用し，前景画像の高周波成分 I'_H を作成する．一方，背景画像 I_L に対しては低域通過フィルタを適用し，背景画像の低周波成分 I'_L を作成する．2 枚の入力画像及びそのフィルタリングの出力を図 4(a)-(d)に示す．

ステップ 2: 特徴点の検出

2 枚のフィルタリング出力 I'_H, I'_L に対して，SURF を利用した特徴点の検出を行う．SURF では，次の手順で特徴点を検出している．①入力画像に対して Fast Hessian detectors を，カーネルサイズを段階的に変更しながら適用する．②Fast Hessian detectors の出力ピラミッドの各画素において，しきい値以上の画素値を持つ座標を特徴点の候補とする．③Non-maximum suppression (NMS)を実行する．NMS では図 5 に示すように，着目画素（×印）を周辺 26 画素（●印）と比較し，着目画素が極値となった場合，その座標を特徴点として検出する．

特徴点検出結果を図 4(e),(f)に示す．図 4(e),(f)において，各円の中心は検出された特徴点の座標，各円の半径は特徴点が検出された際のフィルタのカーネルサイズにより決定される特徴量の大きさを表している．

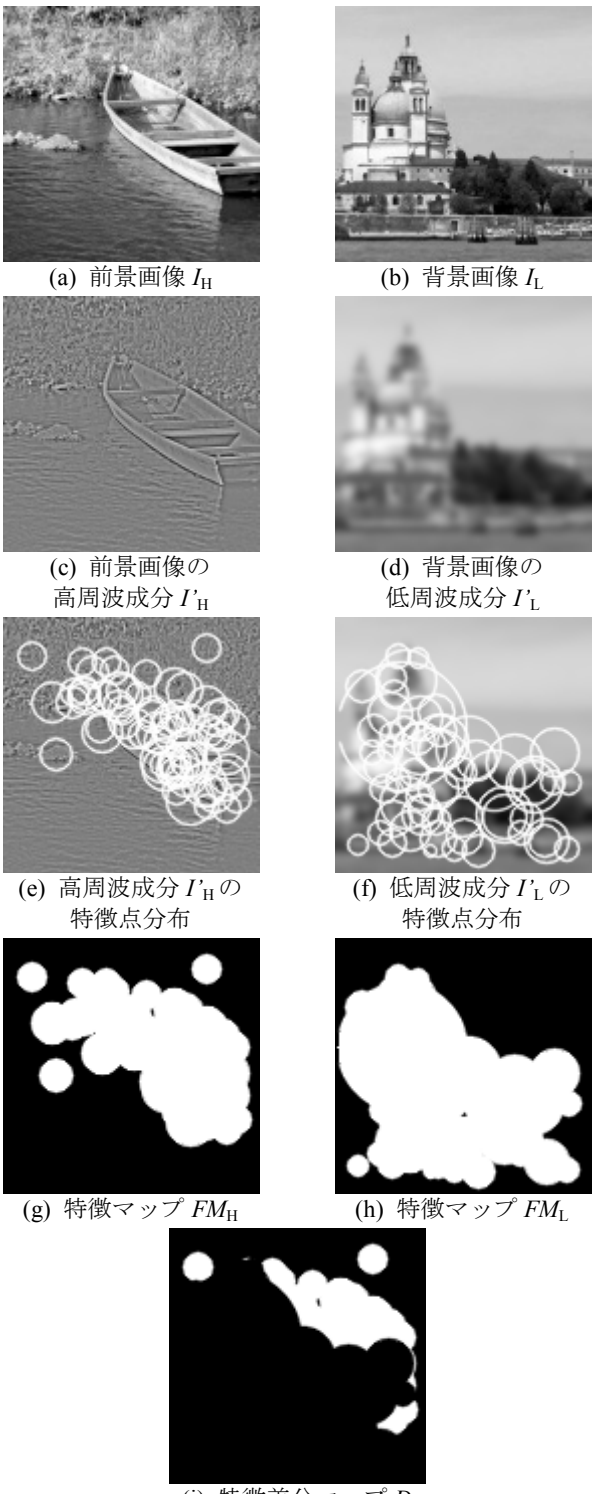
ステップ 3: 特徴マップの作成

ステップ 2 の特徴点検出処理によって生成された画像の各円の内部を 1（白），それ以外の領域は 0（黒）とすることで，図 4(g),(h)に示すような 2 値の特徴マップ FM_H, FM_L を作成する．これにより，画像のオブジェクト領域を近似する．

ステップ 4: 特徴差分マップの作成

式(1)を用いて，特徴差分マップ D を作成する．

$$D(x,y)=\begin{cases}1 & for\ FM_H(x,y)=1\ and\ FM_L(x,y)=0\\ 0 & others\end{cases} \quad (1)$$



(a) 前景画像 I_H　(b) 背景画像 I_L

(c) 前景画像の高周波成分 I'_H　(d) 背景画像の低周波成分 I'_L

(e) 高周波成分 I'_H の特徴点分布　(f) 低周波成分 I'_L の特徴点分布

(g) 特徴マップ FM_H　(h) 特徴マップ FM_L

(i) 特徴差分マップ D

図 4　各段階における出力画像

Figure 4　Output of each step in similarity evaluation.

ここで，式中の(x, y)は画素座標を示している．得られる特徴差分マップの例を図 4(i)に示す．D の白領域の面積が狭い場合，前景画像が背景画像によって効果的にマスキングされていることを意味する．

ステップ 5: 画像対類似度の算出

最後に，特徴差分マップをもとに画像類似度を算出する．本稿では，画像類似度 S を式(2)で定義した．

Vol.2012-CSEC-58 No.46
Vol.2012-SPT-4 No.46
2012/7/20

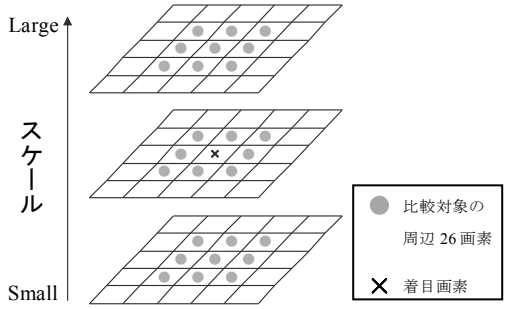


図 5　NMS を用いた特徴点のローカライズ
Figure 5　NMS for interest point localization.

$$S = 1 - \frac{1}{XY}\sum_{y=0}^{Y-1}\sum_{x=0}^{X-1} D(x,y) \qquad (2)$$

ここで，式中の X, Y は画像の幅と高さをそれぞれ示す．S の値域は 0.0～1.0 である．この値が大きい場合，前景画像と背景画像が構造的に類似していることを意味し，その画像対から生成されたハイブリッド画像は画像選択型認証において，比較的高い覗き見耐性を持つと考えられる．

図 6 に，ハイブリッド画像の作成例と，提案する画像対評価尺度を用いて算出した画像類似度を示す．S が 1 に近い図 6(d)では前景画像が効果的にマスキングされているのに対し，S が小さい図 6(e)では背景が平坦な部分でカブトの形状が視認しやすいことが確認できる．

4. 主観評価実験

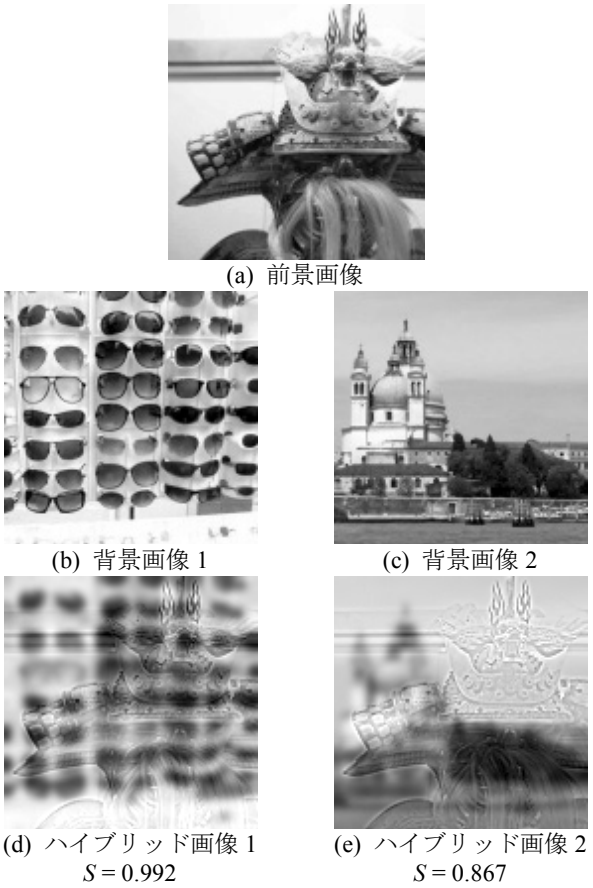
提案する画像対評価尺度による評価スコアが，ハイブリッド画像における前景画像の主観的な見え方と一致するか否かを検証するために，画像の主観評価実験を実施した．今回の実験では，前景画像の主観的な見えやすさを，一対比較法を用いて判断した．以下に詳細を述べる．

4.1 シェッフェの一対比較法における浦の変法

実験サンプル（本稿では画像）が多数の場合，すべてのサンプルを一度に比較評価することは困難であるため，サンプルの中から 2 個ずつ取り出して比較し，最終的にサンプル全体を相対的に評価する方法をシェッフェの一対比較法の原法という．

n 個のサンプルを N 人の被験者によって評価する場合を考える．n 個から 2 個ずつ取り出す組み合わせは，順序も含めて $P(n, 2)$対となる．シェッフェの一対比較法の原法では， N 人の被験者を $P(n, 2)$群に分け，1 群の被験者数を $m = N / P(n, 2)$人とする．次に，この被験者の各群に $P(n, 2)$ 対のサンプルをランダムに 1 対ずつ割り当てて判断させる．従ってサンプル 1 対に対して，m 個の判断が得られる．

しかし，被験者数 N が少数の場合，シェッフェの一対比較法の原法では得られる判断の個数が少なく，統計的に扱うには不適当である．浦の変法はこの問題を解決するための方法であり，$P(n, 2)$対のサンプルすべてを 1 人の被験者が 1 回ずつ評価することで，各サンプル対に対して N 個の判断を得る．今回の実験では，この，浦の変法を使用した．



(a) 前景画像
(b) 背景画像 1
(c) 背景画像 2
(d) ハイブリッド画像 1
$S = 0.992$
(e) ハイブリッド画像 2
$S = 0.867$

図 6　ハイブリッド画像の評価例
Figure 6　Examples of hybrid images and their similarities.

4.2 実験条件

実験には，図 7 に示すハイブリッド画像 6 枚（縦横共に 128 画素）を使用した．これらのハイブリッド画像に用いた前景画像はすべて同一であり，背景画像のみが異なっている．これにより，背景画像の構図の違いが前景画像の見え方に与える影響を評価する．シェッフェの一対比較法における浦の変法に基づき，2 枚のハイブリッド画像の組み合わせ（以下，サンプル対とする）30 対を作成し，被験者全員に 30 対すべてを比較評価させた．

被験者は，視覚健常者（眼鏡等の使用者を含む）の 20 代男性 19 名，女性 1 名，計 20 名である．画像の提示には DELL 社製ラップトップ PC Latitude E4200 と，そのオンボード 12.1 インチ液晶ディスプレイ（解像度 1280 画素×800 画素）を使用した．被験者は机上の実験システムの正面に着席して評価を行う．ディスプレイの角度は視線に対して垂直になるように調整し，画面までの視距離は 60cm とした．

図 8 に，実験に使用したアプリケーションのユーザインタフェースを示す．画面上には，3 枚の画像と 1 個のボタンが表示される．上部の 1 枚の画像は，前景画像から抽出した高周波成分画像である．下部の 2 枚の画像は，比較の対象となるハイブリッド画像である．被験者は，2 枚のハ

Vol.2012-CSEC-58 No.46
Vol.2012-SPT-4 No.46
2012/7/20

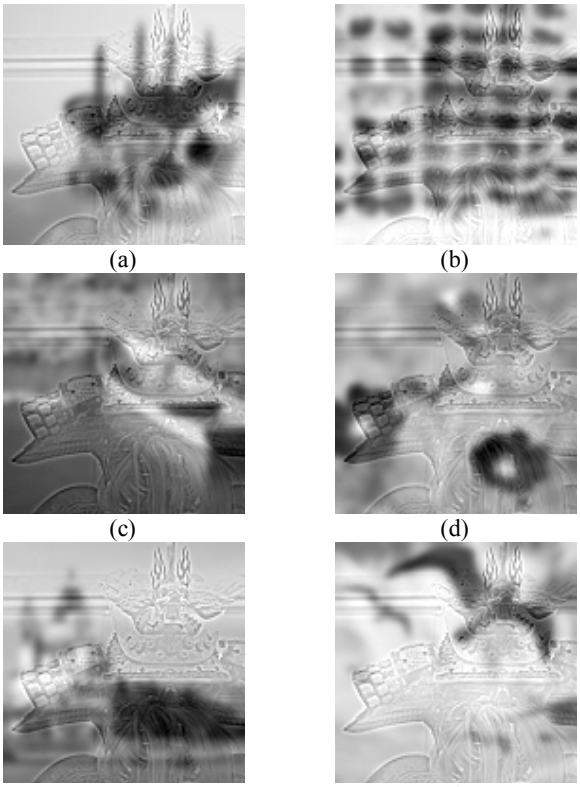


図 7　実験に使用したハイブリッド画像

Figure 7　Hybrid images used for user study.

図 8　主観評価実験のユーザインタフェース

Figure 8　User interface for paired comparison.

イブリッド画像のうち，高周波成分画像が見やすいと感じた方をマウスでクリックして回答する．また，両者の見え方がほぼ同程度だと感じた場合には，下部中央の「どちらでもない」ボタンをクリックする．1 回の評価において，左右どちらかの画像がクリックされた場合はその画像にのみ+1 を与え，判断ができなかった場合はいずれにも加点しない. ひとつのサンプル対あたりの比較評価には 10 秒の時間制限を設けており，制限時間内で回答できなかった場合は,「どちらでもない」が選択されたものとして処理される．また，1 対の評価が終わるたびに灰色一色の画面を 5 秒間表示するインターバルを設け，目の残像現象が次の画像対の評価に与える影響をリセットしている．

実験用アプリケーションには「練習モード」と「実験モード」の 2 つのモードを用意した．練習モードでは，練習用に用意した 3 枚 6 対のハイブリッド画像をランダムな順序で提示し，比較評価の練習を行う．実験モードでは，図 7 に示す 6 枚 30 対のハイブリッド画像を用い，被験者に評価させる．また，実験モードでは，15 対の評価が完了した段階で 1 分間の休憩を設けた．

4.3 実験手順

まず，本実験の前に，実験手順の教示とアプリケーションの操作のトレーニングを実施した. 実験手順の教示では，日本語文と図による説明資料，及び，実験用アプリケーションの練習モードを用いて，実験手順の説明を行った．また，座位置やディスプレイの調整はこの段階で実施し，調整後は画面までの視距離を動かさないことについても教示した．その後，トレーニングとして，被験者に練習モードを 1 度操作させ，希望があれば 2 回目以降のトレーニングも可能とした．

続いて，実験モードを用いて本実験を実施した．本実験において，被験者は,「提示される 2 枚のハイブリッド画像のうち，どちらの方が重畳されている高周波成分画像を見やすいか」を主観評価する．

最後に，アンケート調査を実施した．アンケート項目として，矯正視力等のデモグラフィック調査項目と，サンプル対評価の際に画像のどのような点に着目したかを調査する項目を用意した．このうち，後者の評価の着目点に関する項目では，背景画像の明度の高低による見え方の違い，及び，背景画像のオブジェクトの有無による見え方の違いについての 2 項目を用意した．

4.4 実験結果

本節では，主観評価実験の結果と，客観的評価尺度である提案尺度及び SSIM により算出したスコアを示す．SSIM とは，2 枚の画像間の類似性を測定するための客観的画質評価尺度である [16]．ここで，主観評価スコアの値域は−1.0〜+1.0 であり，SSIM の値域は 0.0〜1.0 である．全被験者の主観評価データの平均を数直線上にプロットしたものを図 9 に示す．図 9 では値が小さいほど，高周波成分が見やすい，すなわち，背景画像によってマスクされていないと評価された画像であることを示す. また，図 10 には提案尺度によるスコア，図 11 には SSIM スコアを，それぞれ数直線上にプロットしたものを示す．これらのスコアは，各ハイブリッド画像を構成する入力画像対（前景画像と背景画像）について算出した．表 1 は，これらの結果を表にまとめたものである．なお，図表におけるラベル(a)-(f)は，図 7 に示すハイブリッド画像のインデックスと対応している．

ユーザ実験で得られた主観評価データに対して分散分析を行った結果，主効果の F 値が 141.375 であったのに対し，$F(5, 470) = 3.055$ であるため，6 枚のハイブリッド画像間の平均評価値に有意な差（$\alpha = 0.01$）が認められた. また，ヤードスティック（$\alpha = 0.01$）を用いて，各ハイブリッド画

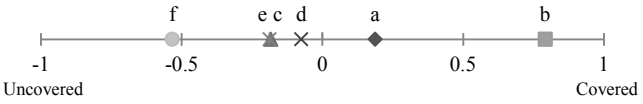


図 9　主観評価スコア

Figure 9　Subjective score.

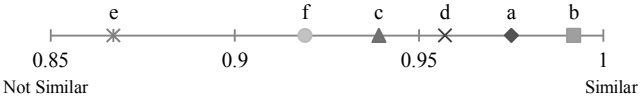


図 10　提案尺度スコア

Figure 10　Proposed objective score.

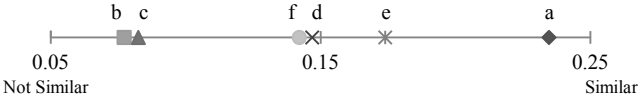


図 11　SSIM スコア

Figure 11　SSIM score.

表 1　各評価手法によるスコア

Table 1　List of score by each evaluation method.

手法	(a)	(b)	(c)	(d)	(e)	(f)
主観評価	0.188	0.792	-0.183	-0.075	-0.188	-0.533
提案尺度 S	0.975	0.992	0.939	0.957	0.867	0.919
SSIM	0.235	0.077	0.082	0.147	0.174	0.142

像間の平均評価値を検討した結果，(c)-(d)間，(c)-(e)間，及び(e)-(d)間の平均評価値には有意な差がないことが判明した（$Y = 0.185$）．

実験後に実施した，高周波成分画像の見やすさについてのアンケートの結果を以下に示す．背景画像が明るい方が見やすいと回答した被験者は 13 名，暗い方が見やすいと回答したのは 7 名であった．また，20 名の被験者全員が，背景画像にオブジェクトがない方が見やすいと回答した．

4.5 考察

まず，主観評価スコア（図 9）と提案尺度スコア（図 10）を比較すると，主観的に高周波成分がマスキングされていると評価されたハイブリッド画像（図 7(b),(a),(d)）は，提案尺度のスコアが高く，またその順序も一致していることがわかる．よって，提案尺度を用いることで，前景画像の高周波成分がマスキングされていると主観的に感じるハイブリッド画像を自動的に選別できると考えられる．また，主観評価スコア（図 9）と SSIM スコア（図 11）を比較すると，SSIM スコアは主観評価との相関が全く見られないことから，SSIM のような従来の画像の類似度評価尺度は本目的には不適当であることがわかる．

5. おわりに

本研究では，画像選択型認証に不適当なハイブリッド画像を事前に除去することを目的とした，客観的画像対評価尺度を提案した．提案尺度では，SURF 特徴点を利用して得た画像の構造的情報をもとに特徴マップ及び特徴差分マップを作成し，画像対の類似度評価を行っている．実験を通して，提案尺度はハイブリッド画像の主観的な見え方とほぼ一致することが確認できた．

今回の実験は 6 枚のハイブリッド画像を使用しており，比較的小規模なデータセットでの評価であったが，今後，背景画像を固定し，前景画像を変更して作成したハイブリッド画像など，より多くの画像についての検証を進める予定である．また，主観評価実験やアンケートの結果をもとに提案尺度に改良を加え，より主観評価に一致する評価尺度への改良を行うことも今後の課題として挙げられる．

謝辞

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

参考文献

1) J. Yan, A. Blackwell, R. Anderson, A. Grant, “Password memorability and security: empirical results,” IEEE Security & Privacy, Vol.2, No.5, pp.25-31, 2004.
2) L. F. Cranor, S.Garfinkel, A. Grant, “The Memorability and Security of Passwords,” Security & Usability, Chapter 7, pp.129-142, O'Reilly, 2005.
3) X. Suo, Y. Zhu, G. S. Owen, “Graphical Passwords: A Survey,” ACSAC '05, pp.463-472, Dec. 2005.
4) R. Dhamija, A. Perrig, “Deja Vu: A User Study Using Images for Authentication,” 9th USENIX Security Symposium, pp.45-58, 2000.
5) Passfaces, http://www.passfaces.com/, last accessed on June 2012.
6) S. Wiedenbecka, J. Watersa, J.C. Birgetb, A. Brodskiyc, N. Memon “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, Vol.63, pp.102-127, July 2005.
7) 原田篤史, 漁田武雄, 西垣正勝, “モザイク画像認証の提案とその実現可能性”, コンピュータセキュリティシンポジウム 2004 論文集, pp.385-390, Oct. 2004.
8) 原田篤史, 漁田武雄, 水野忠則, 西垣正勝, “画像記憶のスキーマを利用したユーザ認証システム”, 情処論, Vol.46, No.8, pp.1997-2013, Aug. 2005.
9) 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,” 情処論, Vol.50, No.9, pp.2062-2076, Sept. 2009.
10) E. Hayashi, N. Christin, R. Dhamija, A. Perrig, “Use Your Illusion: Secure Authentication Usable Anywhere,” SOUPS2008, pp.35-45, 2008.
11) M. Hasegawa, Y. Tanaka, S. Kato, “A Study on an Image Synthesis Method for Graphical Passwords,” ISPACS2009, pp.643-646, Dec. 2009.
12) 宮地隆雄, 長谷川まどか, 田中雄一, 加藤茂夫, “視覚特性を利用した画像認証方式に関する一検討,” 信学論, Vol.J94-D, No.9, pp.1513-1521, Sept. 2011.
13) A. Oliva, A. Torralba, P. G. Schyns, “Hybrid images,” ACM Trans. on Graphics, Vol.25, No.3, pp.527-532, July 2006.
14) Hybrid Images @ MIT, http://cvcl.mit.edu/hybridimage.htm, last accessed on June 2012.
15) H. Bay, A. Ess, T. Tuytelaars, L. V. Gool, “SURF: Speeded Up Robust Features,” Computer Vision and Image Understanding, Vol.110, No.3, pp.346-359, 2008.
16) Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. on Image Processing, vol.13, no.4, pp.600-612, Apr. 2004.