高速切替え表示を用いた撮影耐性を有する文字表示方式

西垣正勝[†1] 宮木孝[†2] 塩田和也[†3]
吉田英樹[†4] 小澤雅治[†3]

近年，個人情報や機密情報の取扱いなど，ディジタルコンテンツの保護が重要な課題となっている．この問題に対し各種情報保護技術が提案されているが，ディスプレイやプロジェクタの画面を直接カメラで撮影してしまうという攻撃に対してまで配慮した方式は稀有である．そこで本論文では，人間の視覚特性を利用した，カメラでの撮影に耐性を有する文字表示方式の提案を行う．今回はそのプロトタイプとして人間の「動きを検知する能力」の高さを利用することで，人間だけが文字を知覚可能で，カメラでの撮影では文字が写らない表示方式を提案し，その実装と評価を行う．

Character Display Scheme against Illegal Photocopy by Camera Using Rapid Images Succession

Masakatsu Nishigaki,[†1] Takashi Miyaki,[†2] Kazuya Shioda,[†3]
Hideki Yoshida[†4] and Masaharu Ozawa[†3]

Recently, the protection of digital content such as personal information and/or confidential information becomes an important issue. Although various content protection techniques have been proposed, most of the conventional schemes can not protect from all the attack of taking a picture of the screen of display or projector directly with a camera. This paper proposes a character display scheme using human sight characteristics which has tolerance in taking a picture with a camera; only person can perceive the character, while the character will not be reflected in taking a picture with a camera. In this paper, an implementation of the prototype system and its evaluation are carried out.

1. はじめに

近年，個人情報や機密情報などの漏洩が問題になっている．このような課題に対し，重要な情報の漏洩を防ぐための様々な手法が研究されている．代表的な例として，電子すかし技術[1),2)]や暗号技術[3),4)]を利用した方式，コンピュータのPrintScreen機能などを制御する方式[5)–8)]などがある．また，これらのソフトウェア的な対策のほかにハードウェア的な対策も存在する[9)–13)]．しかしながら，一般的な手法のほとんどがデータを暗号化するなどのシステム内におけるデータ保護方式であり，システムの外側における物理的な手段による情報の漏洩を防ぐことは困難である．たとえば，銀行のシステム内においてシステムが顧客のパスワードをしっかり守っている場合でも，ATMにおいて顧客がパスワードを入力する操作を，肩越しにあるいは隠しカメラによる盗撮などの手段を用いて覗き見ることができれば，攻撃者は容易にパスワードを知ることが可能である．また，企業において機密情報を守るためにシンクライアントの導入やアクセス権限の管理などを厳密に行っている場合においても，ディスプレイやプロジェクタなどの画面に対する覗き見，隠しカメラによる撮影といった行為によって機密情報が容易に盗まれてしまう．

これらの問題は，コンピュータと人間とが情報をやりとりする際に視覚などの五感を介して「生の情報」をやりとりする必要があることに起因する．情報を扱うのは人間である以上，コンピュータの中では高度な暗号などによって情報を秘匿していたとしても，それが人間に提示される時点においては，情報は必ずオ

†1 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University
†2 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University
†3 チャンスラボ株式会社
Chance Lab. Corporation
†4 株式会社NTTデータビジネスソリューション事業本部
Business Solutions Sector, NTT Data Corporation

リジナルの状態に戻される．すなわち，ユーザがコンピュータを操作する場面は究極的な脆弱ポイントであるといえる．

特に本論文では，コンピュータの画面をカメラで撮影するという攻撃による情報漏洩の問題の解決に焦点をあてる．我々の調べた限り，このような攻撃手段による情報漏洩に対しては，画像認証の分野において覗き見に耐性を有する認証方式などが研究されている程度であり，今後の対策が急がれる課題の 1 つであると認識している．

「画面の撮影」という攻撃は，ディジタルコンテンツ保護の研究分野にも深く関係する．たとえば著作画像が映っている画面をスクリーンキャプチャリングするという行為は，不正コピーの常套手段の 1 つである．この問題に対し，我々は人間の視覚特性を利用したコンテンツ保護技術である画像変調方式の提案を行ってきた[14)–17)]．画像変調方式においては，オリジナル画像を 2 枚にコピーしたうえで，片方の画像に対しては輝度を $+\alpha$ し，他方の画像においては輝度を $-\alpha$ することにより，2 枚の変調画像を生成する．画像を購入したユーザには，2 枚の変調画像が渡される（購入者にもオリジナル画像は渡さない）．ユーザは PC 上で 2 枚の変調画像を高速に切り替えながら表示する．切替え速度が 100 Hz 程度以上になると，人間の眼はその切替わりを認識できなくなり，混色が起こって $+\alpha$ の明るさと $-\alpha$ の暗さが相殺され，頭の中ではオリジナル画像が知覚されるようになる．しかし，時々刻々にディスプレイに表示されている画像はいずれかの変調画像であり，すなわち，コンピュータの中に存在しない情報をユーザに知覚させることが可能となっている．

本論文では，この画像変調のコンセプトを，ディスプレイをカメラで撮影することによって情報を盗むという攻撃に対する対策として使用することを考える．つまり，「コンピュータの中に存在しない情報」をユーザに知覚させる方式を発展させ，「カメラに写っていない情報」をユーザに知覚させる方式を実現する．具体的には，人間の視覚特性とカメラの撮影特性の違いを利用することで，ユーザは情報を知覚できるが，カメラによって撮影された映像からは情報が得られない方式の考案を目指す．ここでは，そのプロトタイプとして，人間の「動きを知覚する能力」の高さを利用し，カメラでは撮影できない動きを人間のみが知覚することによって，人間だけが文字を知覚することができ，カメラには文字が映らない方式を提案する．

2 章では一般的な撮影対策手法について述べる．3 章においては，ディジタルスチルカメラによる盗撮耐性を有する文字表示方式の基本原理を示す．4 章では，提案方式をディジタルビデオカメラによる盗撮にも耐性を有する方式へと改良する方法を含む，いくつかの検討事項を述べる．5 章では提案方式の評価をし，6 章で本論文をまとめる．

2. 撮影対策における既存手法と要件

人間やカメラ撮影によるディスプレイの覗き見攻撃への対策は従来から大きな課題であり，特に画像認証（タッチパネル入力形態のパスワード認証を含む）の分野では認証画面の覗き見攻撃に対して様々な技術の研究，開発が行われている．

単純な方式としては，パスワード入力のときに画面にパスワードを表示せず，「*」などの記号で入力状態を示すような運用が広く採用されている．ただしこの方式は，キーボードなどの入力機器の操作を覗き見られることでパスワードが知られてしまう．カメラでの撮影による覗き見にも耐性を有する画像認証方式としては，同一ユーザの認証を 1 回覗き見ても正確なパスワードを推測することが不可能な方式[18),19)]などが提案されている．しかし，ビデオカメラを用いた録画による覗き見が複数回行われた場合にも耐性を有するものは稀有である．また，これらの方式は人間からコンピュータに入力される秘密情報を覗き見から保護することを目的としており，ディスプレイなどを通じてコンピュータから人間に提示される秘密情報を覗き見から守る際には適用することができない．

画面に表示される秘密情報に対する覗き見防止策として，プライバシフィルタがあげられる．プライバシフィルタは，PC や携帯電話などのディスプレイに貼り付けることで視野角を意図的に狭め，正面にいる人間にしか画面を見ることができないようにする物理的な光学フィルタである．すなわち，プライバシフィルタの視野角内から覗き見された場合には，その効果は得られない．また，正規ユーザであっても，この視野角から外れると画面を見ることができなくなる．このため，ユーザ自身の位置や画面の位置・角度を手軽に調整できる携帯電話などにおいてはプライバシフィルタの効果が発揮されると思われるが，据え置き型となる ATM の画面などにおいては正規ユーザの利便性の低下という弊害のほうが大きくなりうることも予想される．加えて，ハードウェアによる対策では導入コストが高くなるうえ，プロジェクタのような画面を投影するタイプの表示装置においては，適用不可能である．

一方，覗き見攻撃者の観点から考えると，攻撃者本

人が直接，覗き見をする場合は，記憶力の限界があるうえに，正規ユーザに攻撃者の存在や行為が気付かれる可能性があるためリスクが高い．したがって，攻撃者の心理としても，隠しカメラによる盗撮などの方法が好まれるのではないかと考えられる．また，企業説明会などにおいては，最近はプロジェクタの投影画面をカメラ（ディジタルスチルカメラやビデオカメラ）で撮影する参加者を多く見受けるが，企業には，その会場内に限定して情報を提示したいといった要望がある場合がある．

以上のことをふまえると，(i) 撮影耐性，(ii) 視認性，(iii) 汎用性を満たす表示方式が必要であることが分かる．撮影耐性はカメラによる静止画・動画撮影に耐性を有すること，視認性は提示された情報の見やすさ，汎用性はハードウェアなどに依存せずいかなる表示装置においても利用可能なことである．そこで，次章からは以上の要件を満たした文字情報の表示方式の実現を目指す．本論文で実装する表示方式は，(i) 撮影耐性に対しては，固定されたカメラによる静止画撮影および動画撮影に対する耐性を有する，(ii) 視認性に対しては，最低限の視認性を有する，(iii) 汎用性に対しては，ソフトウェアにより実装可能であるが，動画による撮影耐性を備えるにはある程度以上のリフレッシュレートを有する表示装置が必要である，という性質を持つ．

3. 撮影耐性を有する文字表示方式

たとえば，川を見た場合，動画であれば水がどちらからどちらへ流れているかはすぐに判断できる．しかし，カメラ（ディジタルスチルカメラ）で撮影された川の写真を見た場合には，その判断は難しいものとなる．このような動画と静止画の違いを利用することで，人間のみが知覚可能であり，カメラ（ディジタルスチルカメラ）で撮影しても写らないような文字表示方式が実現できる．

3.1 動きを使った文字の知覚

人間に動きを知覚させる方法は多数あるが，提案方式では，単純にランダムドット画像を左右に動かすことで動きを知覚させる．たとえば，**図 1** のような 3 枚の画像を (a) → (b) → (c) → (a) → ⋯ の順番にディスプレイにある程度の切替え速度で映すことで，人間はランダムドットが右に動いているように知覚する．

この動きの知覚を利用して，ランダムドット画像の領域の違いをユーザに認識させる．たとえば，**図 2** のような 3 枚の画像を，(a) → (b) → (c) → (a) → ⋯ の順番にディスプレイにある程度の切替え速度で映した場合，上半分の領域は右に動いているように知覚するが，下半分の領域は動いてないことを知覚する．これにより，ユーザは上半分と下半分を別の領域として認識することになる．

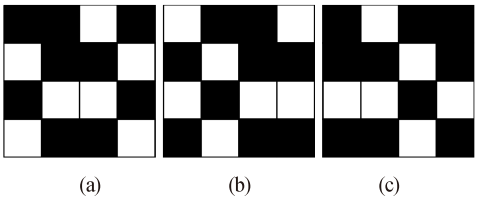


図 1 右に動くランダムドット
Fig. 1 Random dot that moves to the right.

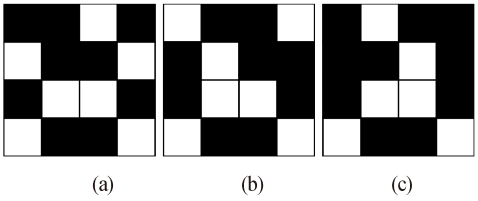


図 2 上半分が右に動くランダムドット
Fig. 2 Random dot, the upper half of which moves to the right.

これを文字表示に適用する場合，文字領域と背景領域をともにランダムドットで表し，文字領域のランダムドットのみに動きを与える（または，背景領域のランダムドットのみに動きを与える）ことになる．ユーザは文字領域だけ（または，背景領域だけ）に動きを知覚するため，文字領域と背景領域の区別ができる．一方，カメラで画像の 1 コマのみを撮影した場合，写真には無意味なランダムドットしか映らないことになる．これによって人間のみが文字を知覚でき，カメラ（ディジタルスチルカメラ）では文字が撮影できない仕組みが実現できる．

3.2 カメラの撮影に耐性を有する方式

前節で述べた方式では，カメラの露光時間が長く，1 枚の写真に複数枚のランダムドット画像が映った場合には対応できない．動いている領域と動いていない領域が同時に存在する場合，動いている領域のみが複数枚の異なるランダムドットを平均化した「ぼやけた」画像となる．一方，動いていない領域は「はっきり」と写るため，両者の領域の違いが写真に現れてしまうのである．これを図 2 の場合で考えてみると，たとえばシャッタが開いてから閉じるまでの間に図 2 の 3 枚のランダムドット画像が表示された場合，撮影される写真は**図 3** のような画像（図 2 (a)〜図 2 (c) の 3 枚のランダムドット画像の各画素の時間平均をとった画像）となり，領域の違いが認識されてしまう．

この問題を解決するために，カメラの特性を利用す

る．カメラはシャッタが開いた直後から光を取り込み始め，シャッタが閉じる瞬間までにレンズに入った光の総量によって写真が生成されることになる．よって，2 つの領域（文字領域と背景領域）における各時刻の表示画像が異なっていても，光量の合計が同じであれば，両者の領域のカメラでの撮影イメージは同じものになる．

このカメラの露光特性を先ほどの方式に適用する．すなわち，文字領域も背景領域もともに同じ速度で動くランダムドット画像として構成し，その動く方向のみを逆にする．これにより，複数コマのランダムドット画像が 1 枚の写真としてカメラに写った場合でも，右に動く領域と左に動く領域は等価値のランダムドット画像になるため，写真から領域の区別をつけることはできなくなる．たとえば，**図 4** のような 3 枚の画像を (a) → (b) → (c) → (a) → ⋯ の順番に高速切替え表示することで，人間には上半分の領域が右に，下半分の領域が左に動いているように知覚されることになるが，たとえば露光時間中に 3 枚のランダムドット画像が表示された場合の写真は**図 5**（図 4 (a)〜図 4 (c) の 3 枚のランダムドット画像の各画素の時間平均をとった画像）のようになり，上半分と下半分が異なる領域であると認識することは不可能となる．

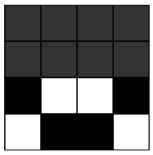


図 3 図 2 の撮影結果のイメージ
Fig. 3 Image by taking a picture of Fig. 2.

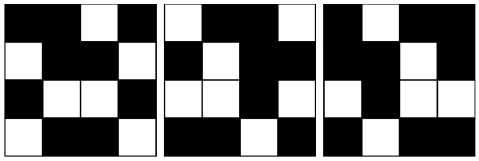


図 4 上半分が右，下半分が左に動くランダムドット
Fig. 4 Random dot, the upper half of which moves to the right, while the lower half moves to the left.

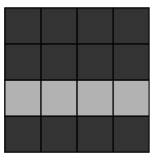


図 5 図 4 の撮影結果のイメージ
Fig. 5 Image by taking a picture of Fig. 4.

4. 提案方式の問題とその解決策

本章では，本提案方式を使って実際に文字を表示する際に起こりうる問題点とその解決策について述べる．特に 4.2 節では，提案方式をディジタルビデオカメラによる盗撮にも耐性を有する方式へと改良する方法について示す．

4.1 エッジの問題

提案方式で文字を提示する場合，文字領域と背景領域の境目，すなわち文字のエッジ部分において，領域の差が発覚するような場合が発生することがある．たとえば**図 6** は，3 枚の画像を (a) → (b) → (c) → (a) → ⋯ の順番で高速切替え表示することで，左半分の領域が右方向に，右半分の領域が左方向に動くように知覚されるが，たとえば露光時間中に 3 枚のランダムドット画像が表示された場合の写真は**図 7**（図 6 (a)〜図 6 (c) の 3 枚のランダムドット画像の各画素の時間平均をとった画像）のようになり，両領域の間で急激な輝度の変化が発生していることから，写真中央に縦のエッジが存在することが知られてしまう．図 6，図 7 は左半分の領域が右方向に，右半分の領域が左方向に流れる場合（左方向と右方向の流れが合流するエッジ）の例であるが，左半分の領域が左方向に，右半分の領域が右方向に流れる場合（左方向と右方向の流れが分流するエッジ）や，隣り合う領域が同じ方向に流れている場合も同様である．

この問題に対応するために，ダミーのエッジを生成させることを考える．上述のとおり，カメラで撮影した写真においてエッジが知覚されてしまう箇所は，流れが分断される「領域と領域の境目」となる．これを

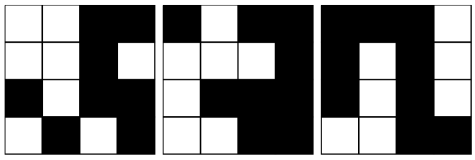


図 6 左半分が右，右半分が左に動くランダムドット
Fig. 6 Random dot, the left half of which moves to the right, while the right half moves to the left.

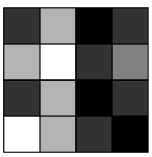
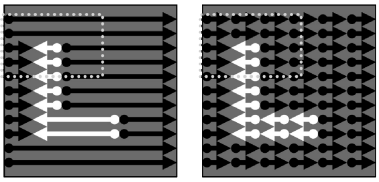


図 7 図 6 の撮影結果のイメージ
Fig. 7 Image by taking a picture of Fig. 6.



(a) (b)

図 8 大きな流れの細分化
Fig. 8 Subdivision of big stream.

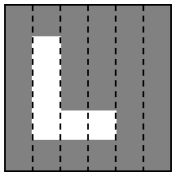


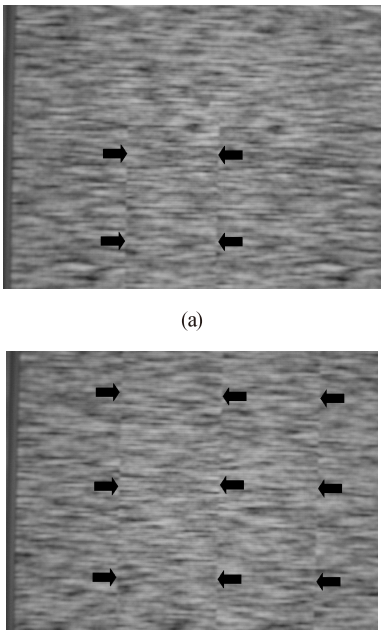
図 9 図 8 (b) の撮影イメージ
Fig. 9 Image by taking a picture of Fig. 8 (b).

利用し，1 つの横方向への大きな流れを同じ方向の小さな流れに分割することで，ダミーエッジの生成を実現する．たとえば**図 8** は，アルファベットの「L」という文字の流れ（図 8 (a)）を等間隔の小さな流れになるように領域分割した例（図 8 (b)）である．「各ドットが図 8 (b) のように流れる」ように知覚される複数のランダムドット画像を生成し，これらのランダムドット画像を連続的に切替え表示した場合，これをカメラで撮影した写真においてエッジが発覚する可能性のある場所を**図 9** の点線で示す．このように，写真全体に等間隔で縦のエッジが発生しうるため，たとえエッジが分かったとしても表示されている文字を判別することはできないと考えられる．

図 8 (a) と図 8 (b) の実際の画像例を**図 10** (a) および図 10 (b) に示す．図 10 (a)，図 10 (b) はそれぞれ図 8 (a) および図 8 (b) の点線の枠内をズームアップした写真である．図 10 (a) では文字と背景の境目にのみエッジが観測されるが，図 10 (b) においては全体的にエッジが発生するため，文字と背景の境目の情報が隠されていることが見て取れる（図 10 においては，縦のエッジが発生している箇所を分かりやすく示すために矢印を記してある）．

4.2 ビデオ撮影の問題

ここまでに述べた方式はあくまでも，ディスプレイなどの表示機器の映像を，静止画として撮影される攻撃に対する耐性を有する表示方式である．しかしながら，一般に隠しカメラなどによる撮影がビデオカメラで行われることも十分考えられるため，ビデオ撮影に対する耐性についても検討する必要がある．



(a)

(b)

図 10 大きな流れを細分化した場合の画像例
Fig. 10 Example images of subdivision of big stream.

一般的なビデオカメラの場合，動画は 24 Hz〜30 Hz 程度のフレームレートとなる．まして隠しカメラなどのように小型のものであれば，ランダムドット画像が綺麗に写るような高解像度の画質で，30 Hz 以上のフレームレートでの撮影ができるとは考えにくい．したがってここでは，30 Hz 程度のフレームレートでのビデオ撮影に耐性を有する文字表示方式を考案していく．

本論文では，ビデオカメラによって撮影された複数のフレームから，ランダムドットの流れが特定されることを防ぐ方式を検討する．なお，以下の対策手法については，フレームの切替えと画面のリフレッシュのタイミングが一致している場合を例に説明するが，両者のタイミングがずれていても同様の理論が成り立つ．

4.2.1 連立方程式の求解による攻撃に対する対策

たとえば，**図 11** のような 2 × 2 画素の 3 枚の画像を (a) → (b) → (c) → (a) → ⋯ の順番に 60 Hz の速度で高速切替え表示したとしよう．ここで，図 11 における A_i，B_i（$1 \leqq i \leqq 3$）の値は各画素の輝度である．図 11 は，上半分が左に，下半分が右に流れているように知覚される．この画面をフレームレートが 30 Hz であるビデオカメラによって撮影する場合，ディスプレイの切替え表示速度とビデオカメラの撮影速度の関係から，(フレームの切替えと画面のリフレッシュのタイミングが一致していれば）ビデオの 1 フレームには

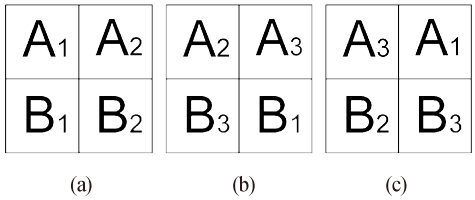
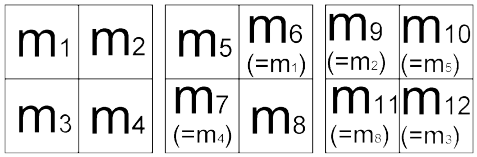


図 11 有限個のランダムドット画像の繰返し
Fig. 11 Succession of limited number of random dot images.



(a) 図 11 の(a)と(b)の平均画像　(b) 図 11 の(c)と(a)の平均画像　(c) 図 11 の(b)と(c)の平均画像

図 12 図 11 を撮影したフレーム
Fig. 12 Frames by taking a movie of Fig. 11.

2 枚の画像の時間平均値が写ることになる．今，ビデオカメラで 3 フレーム分の撮影する 1/10 秒の間に，ちょうど「(a) → (b) → (c) → (a) → (b) → (c)」の 6 画像が 1/60 秒ずつ画面に表示されていた場合，1 フレーム目には (a) と (b) の平均画像が，2 フレーム目には (c) と (a) の平均画像が，3 フレーム目には (b) と (c) の平均画像が写ることになるので，**図 12** のような 3 枚の連続したフレームが得られることになる．この結果，撮影した 3 枚のフレームに写った平均画像における各画素の輝度 m_i（$1 \leqq i \leqq 12$）から，

$$(A_1 + A_2)/2 = m_1, \quad (A_2 + A_3)/2 = m_2,$$
$$(A_1 + A_3)/2 = m_5, \quad (B_1 + B_2)/2 = m_4,$$
$$(B_2 + B_3)/2 = m_8, \quad (B_1 + B_3)/2 = m_3$$

という連立方程式が得られることとなり，A_i，B_i（$1 \leqq i \leqq 3$）が求められてしまう．したがって，図 11 の (a)，(b)，(c) のそれぞれの画像が判明してしまい，各領域（図 11 の例では上半分と下半分）の流れの方向が解析されてしまう．

そこで，有限個のランダムドット画像の繰返しによりドットの流れを知覚させるのではなく，無限個のランダムドット画像によりドットの流れを知覚させる．この例を**図 13** に示す（図 13 は，無限個のランダムドット画像のうちのある連続した 6 枚を示している）．ここで，A_i，B_i（$1 \leqq i \leqq \infty$）はそれぞれ乱数系列である．

今，図 11 の例のときと同様に，ビデオカメラで 3 フレーム分の撮影をする 1/10 秒の間に，ちょうど「(a) →(b) → (c) → (d) → (e) → (f)」の 6 画像が 1/60 秒ずつ画面に表示されていた場合，1 フレーム目には

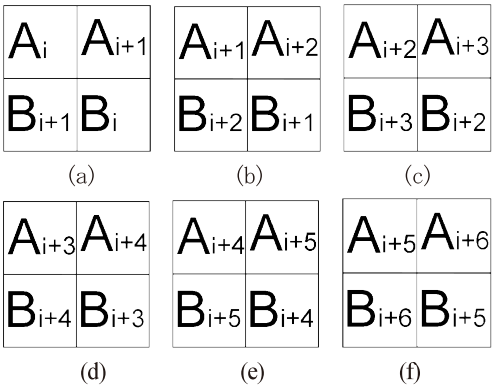
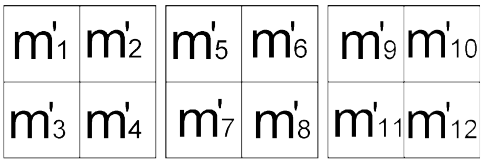


図 13 無限個のランダムドット画像の切替え
Fig. 13 Succession of unlimited number of random dot images.



(a) 図 13 の(a)と(b)の平均画像　(b) 図 13 の(c)と(d)の平均画像　(c) 図 13 の(e)と(f)の平均画像

図 14 図 13 を撮影したフレーム
Fig. 14 Frames by taking a movie of Fig. 13.

(a) と (b) の平均画像が，2 フレーム目には (c) と (d) の平均画像が，3 フレーム目には (e) と (f) の平均画像が写ることになる（**図 14**）．この場合も攻撃者は，撮影した 3 枚のフレームに写った平均画像における各画素の輝度から連立方程式を立てることは可能であるが，今回は変数である A_i，B_i の数が方程式の数よりも多いため，方程式を解くことができない．すなわち，ビデオカメラに写った複数枚のフレーム画像から，ランダムドットの流れの向きを解析することは理論上，不可能である．

ただし，もしランダムドットが白と黒のみで構成されている場合には，すべての変数が 0 または 1 の 2 値となるため，攻撃者が総当り攻撃により変数のすべての組合せを試せば，連立方程式の解となる変数の組を容易に発見することができてしまうのではないかという不安が残る．そこで，ランダムドットの各画素を 24 ビットカラーの RGB で表示することを考える．これにより，変数の総当り攻撃への耐性が格段に向上する．この場合，ビデオカメラに写る各画素の平均輝度も 256 階調となるため，精細なビデオカメラで撮影をしなければ各フレームにおける画素の輝度値（m'_i）を正確に得ることができず，不正者が連立方程式を立てること自体を困難にするという効果も期待できる．

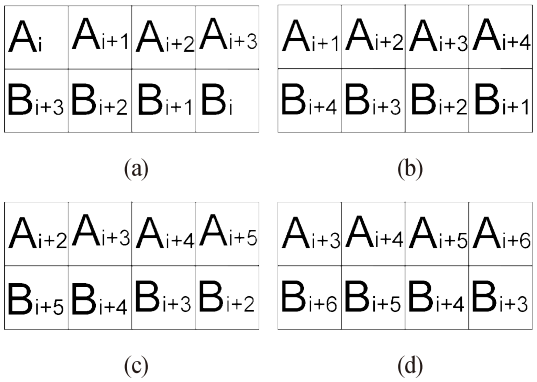


図 15 無限個の 2×4 のランダムドット画像の切替え
Fig. 15 Succession of unlimited number of 2×4 random dot images.

また，ビデオカメラに写る各画素の平均輝度が白（または黒）であった場合には，そのフレームの露光時間の間は，その画素はつねに白であった（またはつねに黒であった）ことが確定する．これは，連立方程式における変数の数を減らすことに通じる．そこで，ランダムドット（乱数系列）の生成に制限を設け，特定の画素の色がある程度連続して同じ色に固定されてしまうことがないようにする必要がある．

4.2.2 フレーム間の共通領域の解析による攻撃に対する対策

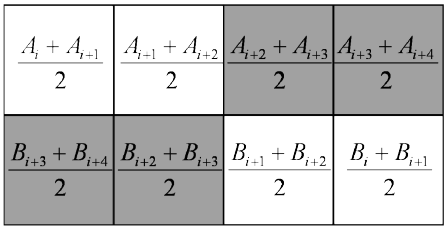
ビデオカメラで撮影された動画における各フレームには，1/30 秒間ごとの平均輝度が時系列で連続的に写っている．すなわち，領域ごとの平均輝度の画像も，領域が移動する方向に流れているように写る．不正者がこの動きをとらえることができれば，連立方程式を解くことなく領域の移動方向が知られてしまう．

たとえば，図 13 のランダムドット画像が 2×4 画素であった場合を考えよう．すなわち，**図 15** のような画像が (a) → (b) → (c) → (d) → ⋯ の順番に 60 Hz の速度で高速切替え表示されている（図 15 は，無限個のランダムドット画像のうちのある連続した 4 枚を示している）．今，ビデオカメラで 2 フレーム分の撮影をする 2/30 秒の間に，ちょうど「(a) → (b) → (c) → (d)」の 4 画像が 1/60 秒ずつ画面に表示されていた場合，1 フレーム目には (a) と (b) の平均画像が，2 フレーム目には (c) と (d) の平均画像が写ることになる（**図 16**）．図 16 から明らかなように，1 フレーム目と 2 フレーム目には同色となる画素（図 16 においてグレーで記されている画素）が含まれるため，この画素の移動方向から各領域（図 15 の例では上半分の領域と下半分領域）の流れの方向が判明してしまう．

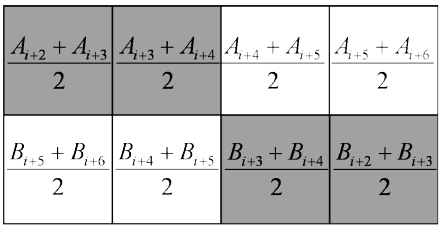
そこで，4.1 節の方法を採用し，大きな流れを小領域に細分化することにより，ビデオカメラにおける 1 フレームあたりの撮影間隔である 1/30 秒間のうちに，各小領域のランダムドットがすべて入れ替わるような対策をとるようにする．そのためには，小領域の幅 T [pixel] が，ディスプレイのリフレッシュレート R [Hz] とビデオカメラのフレームレート F [Hz] に対して，

$$T \leqq R/F \tag{1}$$

を満たせばよい．これを図 15，図 16 の例に適用すると，R/F は 2 であるから，$T = 2$ と設定することで **図 17**，**図 18** のようになり，フレーム間に共通画素が現れることはなくなる．ここで，A_i，B_i，C_i，D_i（$1 \leqq i \leqq \infty$）はそれぞれ乱数系列である．



(a) 1 フレーム目（図 15 の(a)と(b)の平均画像）



(b) 2 フレーム目（図 15 の(c)と(d)の平均画像）

図 16 2 フレーム間の共通画素
Fig. 16 Identical pixels between two frames.

式 (1) の条件から分かるように，表示装置のリフレッシュレートがある程度高い場合でなければ，この対策は意味をなさない．たとえばプロジェクタなどは，現在の製品で 30 Hz 程度のリフレッシュレートのものが一般的であるので，これらの方法が適用できない．画面をプロジェクタで投影する場合における，ビデオカメラでの盗撮対策については今後の課題である．

4.3 カメラの手ぶれの問題

画面を撮影する際にカメラの手ぶれが加わることによって，ディスプレイに映されている文字が写真に写る可能性がある．カメラから見れば，手ぶれの発生は，ディスプレイが手ぶれの速度と同じ速さで逆の方向に動いたことになる．すなわち，手ぶれの影響でランダムドットの「右方向への動きの速度（カメラとの相対速度）」と「左方向への動きの速度（カメラとの相対速

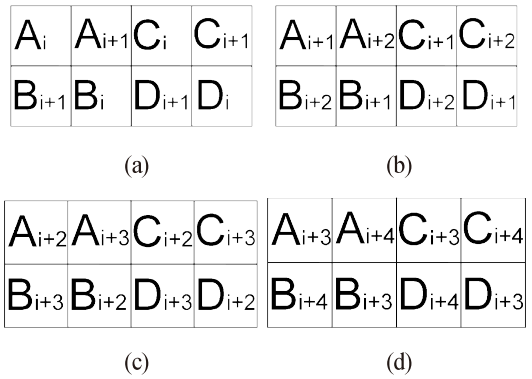


図 17 無限個の 2 × 4 のランダムドット画像の切替え（小領域の幅を 2 とした場合）
Fig. 17 Succession of unlimited number of 2 × 4 random dot Images (stream width = 2).

$\frac{A_i + A_{i+1}}{2}$	$\frac{A_{i+1} + A_{i+2}}{2}$	$\frac{C_i + C_{i+1}}{2}$	$\frac{C_{i+1} + C_{i+2}}{2}$
$\frac{B_{i+1} + B_{i+2}}{2}$	$\frac{B_i + B_{i+1}}{2}$	$\frac{D_{i+1} + D_{i+2}}{2}$	$\frac{D_i + D_{i+1}}{2}$

(a) 1 フレーム目（図 17 の(a)と(b)の平均画像）

$\frac{A_{i+2} + A_{i+3}}{2}$	$\frac{A_{i+3} + A_{i+4}}{2}$	$\frac{C_{i+2} + C_{i+3}}{2}$	$\frac{C_{i+3} + C_{i-4}}{2}$
$\frac{B_{i+3} + B_{i+4}}{2}$	$\frac{B_{i+2} + B_{i+3}}{2}$	$\frac{D_{i+3} + D_{i+4}}{2}$	$\frac{D_{i+2} + D_{i-3}}{2}$

(b) 2 フレーム目（図 17 の(c)と(d)の平均画像）

図 18 フレーム間に共通画素は出現しない
Fig. 18 No identical pixels between two frames.

度）」に差が生じる．この結果，右に動く領域と左に動く領域の間の「シャッタが開いてから閉じるまでにカメラの撮像素子に届く光量」のバランスに違いが生じ，領域の違いがカメラに写ってしまうことが起こりうる．

この問題に対しては，今後対策を検討していく予定である．ただしこの問題は，隠しカメラなどのように固定配置されているカメラによる盗撮では生じない．

5. 提案方式の評価

5.1 評価実験の緒言

提案方式のプロトタイプシステムを実装し，評価を行う．実験には，HP 社の CRT ディスプレイ p1230 と Panasonic 社のディジタルカメラ DMC-FX5 を用いた．CRT の解像度の画面設定は 1,280 × 960 画素である．DMC-FX5 は静止画および動画の撮影が可能であり，静止画撮影および動画撮影における解像度はそれぞれ 1,600 × 1,200 画素，320 × 240 画素，静止画撮影における露光時間は 1〜1/2,000 秒の間で自動調節，動画撮影におけるフレームレートは 30 Hz である．

今回はこの CRT ディスプレイを使い，400 × 400 画素（12.0 cm 四方）の枠の中に大きく 1 文字を表示した．文字は 4.2 節の方式（4.2.1 項で説明した対策と 4.2.2 項で示した対策の両者を採用した方式；以下，提案方式）で作成した．すなわち，文字領域は左方向に流れる 24 ビットカラーのランダムドット，背景領域は右方向に流れる 24 ビットカラーランダムドットで構成する．また，式 (1) で示した条件（$T \leqq R/F$）が満たされるように，文字領域および背景領域は 4 画素ごとに流れの領域を細分化した．細分化されたすべての領域は，右（または左）に 1 画素移動すると新たなランダムドットが左（または右）から 1 画素追加される．細分化した領域から右（または左）に飛び出した 1 画素は捨てられる．これをビデオカメラのフレームレートの 4 倍の速度で動かすことにより，1/30 秒間のうちに各小領域のランダムドットがすべて入れ替わるようにする．すなわち，ディスプレイのリフレッシュレートは 120 Hz にセットした．

4.1 節で示したダミーエッジの効果を確認するために，提案方式に対してダミーエッジを導入していない方式（以下，方式 1）についても評価を行う．また，プロジェクタなどのように高いリフレッシュレートを持たない表示機器での効果を確認するために，提案方式のリフレッシュレートを 40 Hz に落とした方式（以下，方式 2）についても評価を行う．さらに，比較のために，提案方式に対してダミーエッジを導入せず，かつ，リフレッシュレートを 40 Hz とした方式（以下，方式 3）についても評価する[⋆1]．

2 章で示した本方式の要件（(i) 撮影耐性，(ii) 視認性，(iii) 汎用性）に鑑み，以下では撮影耐性および視認性の評価を実施する．汎用性の評価（本方式を適用することが可能な表示装置の仕様を調査）に関しては，方式 2 および方式 3 に対する撮影耐性評価・視認性評価実験が，これを担っている．

⋆1 提案方式，方式 1，方式 2，方式 3 の表示例を下記 URL に用意した．
http://minamigaki.cs.inf.shizuoka.ac.jp/modulation/index.html

5.2 視認性評価実験

静止画の画質評価においては PSNR などの指標を用いての客観評価が可能であるが，動画の画質評価については，動画像が被験者にどのように「知覚」されるかを測る必要があるため，物理的な客観評価が難しい．このため，認知系の研究分野においても動画の画質評価は主観評価実験によって行われることが一般的である．そこで本論文では，視覚心理学の研究分野で確立されている視認性評価実験法である調整法[20] の手順に従って本方式の視認性の評価を行った．調整法では，提案方式，方式 1，方式 2，方式 3 による画像を「標準画像」，被験者自身が鮮明度を変えることができる静止画像を「比較画像」とし，被験者に標準画像と同等に知覚される比較画像を答えてもらうことにより，比較画像を物差しとして標準画像の視認性を評価することになる．

今回の実験では，表示する文字は 1 文字の平仮名とし，「あ」と「こ」と「ゆ」の 3 種類を使用した．それぞれの文字を提案方式，方式 1，方式 2，方式 3 によって表示した画像が各方式の標準画像となる．一方，比較画像は，各文字のオリジナル画像とカラーのランダムドット画像の各画素を $(255-m):m$ の割合で加重平均して生成する（$m=0$〜255）．例として，「あ」の文字に対する，オリジナル画像，$m=210$ の比較画像，$m=220$ の比較画像，$m=230$ の比較画像，$m=240$ の比較画像，$m=250$ の比較画像，ランダムドット画像を**図 19** に示した（実際にはカラーのランダムドットであるが，印刷上はモノクロ）．図 19 には各画像の PNSR 値も併記した．被験者がマウスのホイールを前後に回すと，それに応じて画面上の比較画像も m の値が 1 ずつ段階的に上下したものに変わるようになっている．なお，標準画像，比較画像の各々が 400×400 画素の大きさである．

被験者は本学の学生 10 名であり，ディスプレイから 60 cm 離れた距離に顎台を設置し，その位置から肉眼で文字の視認性を評価してもらった．この位置から実験画面（**図 20**）を見た場合の視角は，画面の左端から右端までが約 35.5°，上端から下端までが約 27.0°，画像（標準画像，比較画像のそれぞれ）の左端から右端まで約 29.1°，上端から下端までが約 11.4°，標準画像と比較画像の間隔が約 6.9° となる．顎台には覗き窓が設置されており，実験画面以外が被験者の視野に入らないようにしてある．背景はグレイ（RGB の値が $(127,127,127)$）である．

提案方式，方式 1，方式 2，方式 3 の 4 つの方式のそれぞれについて，3 種類の文字の実験をした．実験

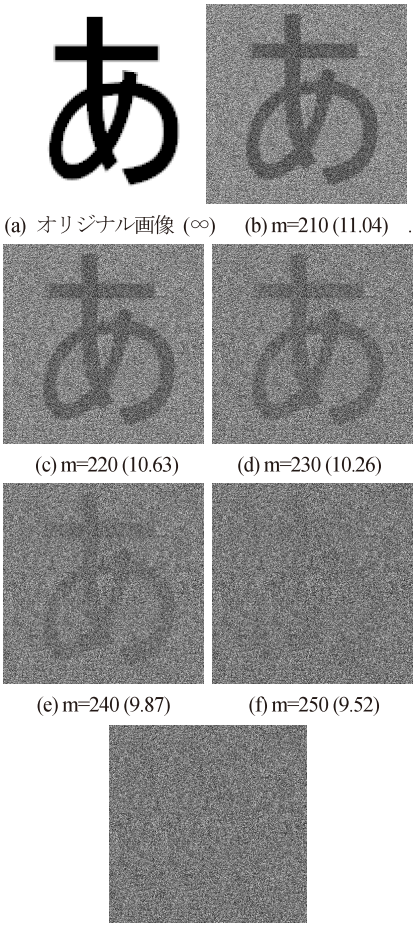


図 19 視認性評価実験における比較画像例（括弧内は PSNR 値）
Fig. 19 Images for readability evaluation.

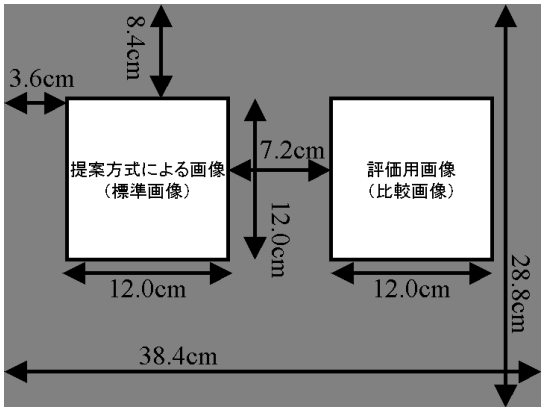


図 20 実験画面
Fig. 20 Experimental window.

においては，被験者の反応は空間誤差，時間誤差やその他の偶発的誤差を含むので，測定の回数を増やすと

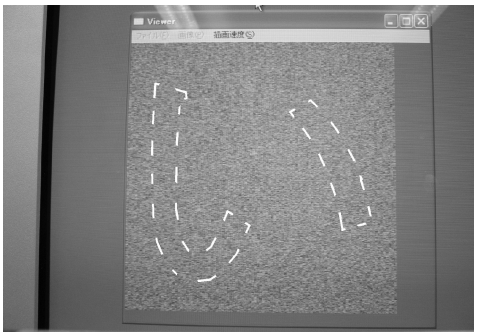


図 21 静止画写真
Fig. 21 Still picture image.

ともに，調整の方向を変化させる必要がある．今回は，各方式・各文字に対する 1 回の実験につき 8 回の測定を行うこととし，その 8 回の中に，下降的調整（m の値を 250〜255 の中からランダムに選んで比較画像を生成し，この画像を比較画像の初期値として調整を始める）と上昇的調整（比較画像の初期値を $m = 100$〜150 の中からランダムに選び，この画像から調整を始める）を，下降，上昇，下降，下降，上昇，下降，上昇，上昇の順に配置する．なお，各測定を終えるごとに，今まで被験者が見ていた画像が被験者の眼に与える影響を消すために，30 秒間ディスプレイ全体をグレイにする．また，実験画面における標準画像と比較画像の表示位置（右と左）は測定ごとにランダムに入れ替わる．

被験者は，3 種類の平仮名それぞれに対し，提案方式，方式 1，方式 2，方式 3 の表示方法によってディスプレイに映し出される文字（標準画像）がどのように知覚されるかを，比較画像の m の値を調整して「標準画像に最も近いと思われる比較画像を主観的に選ぶ」という形で回答することになる．各被験者の 8 回の測定における m の値の平均値を各実験における評価値とする．

5.3 撮影耐性実験

表示する文字は，視認性評価実験と同様に 400×400 画素の大きさの枠に 1 文字の平仮名とし，今回は「い」，「え」，「ち」，「と」，「に」，「は」，「へ」，「り」，「ろ」，「を」の 10 種類を使用した．各平仮名をそれぞれ提案方式，方式 1，方式 2，方式 3 の表示方式によりディスプレイに映し出し，その際の画面をカメラによって静止画および動画撮影した．撮影は，画面の正面方向にディスプレイから 20 cm 離れた距離にカメラを固定する台を置き，手ぶれの発生しない状態で行った．**図 21** は，提案方式により「い」を表示させている画面を静止画撮影した際の写真（原寸は 1,600 × 1,200 画素；実際にはカラーのランダムドットであるが，印刷上はモノクロ）である．

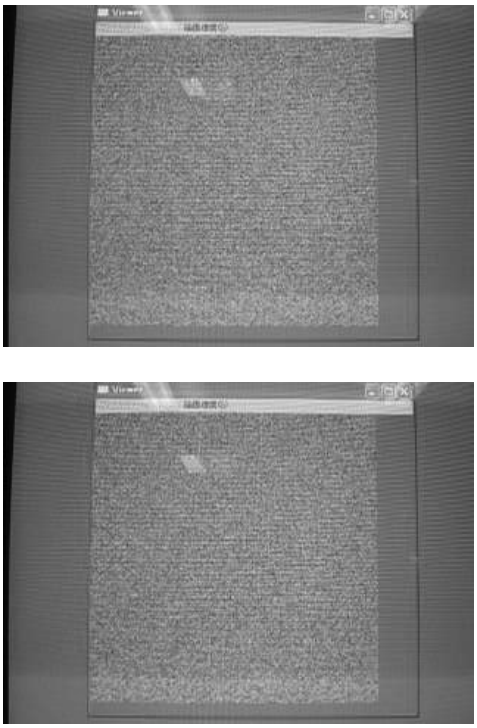


図 22 動画中の連続する 2 フレーム
Fig. 22 Two consecutive frames in movie.

図 22 は，同じく「い」を動画撮影した際の動画の中の任意の連続した 2 フレームの写真（原寸は 320 × 240 画素；同じく印刷上はモノクロ）である．なお，図 21 には，文字の表示領域を破線で記してある．

撮影耐性の評価においては，上記のように撮影された静止画および動画をパソコンのビューアソフトによってディスプレイに表示させ，被験者がこれを解読可能かどうか測定した．具体的な表示方法は以下のとおりである．静止画は，インターネットエクスプローラ（以下，IE）を最大化表示にした状態で，自動リサイズ機能（IE のサイズに合わせて画像サイズを自動調節する機能）を利用して画面全体に表示させた．画面に映った文字（文字を表示させた 400 × 400 画素の枠）のサイズは約 16.5 × 16.5 cm であった．動画は，IE 上で QuickTime を利用し，100%のサイズで表示した．画面に映った文字（400 × 400 画素の枠）のサイズは約 9.0 × 9.5 cm であった．なお，各方式（提案方式，方式 1，方式 2，方式 3）で文字を表示させたディスプレイと，その文字を撮影した画像を被験者に表示した際に使用したディスプレイは同じものである．

被験者は視認性評価実験の被験者と同じ学生 10 名

表 1 視認性評価実験と撮影耐性評価実験の結果
Table 1 Experimental results.

	視認性評価値	静止画判読成功率（評価値）	動画判読成功率（評価値）
方式1	211.150	0.0（—）	1.0（1.0）
方式2	234.767	0.0（—）	1.0（1.6）
方式3	220.675	0.0（—）	1.0（1.0）
提案方式	238.183	0.0（—）	0.0（—）

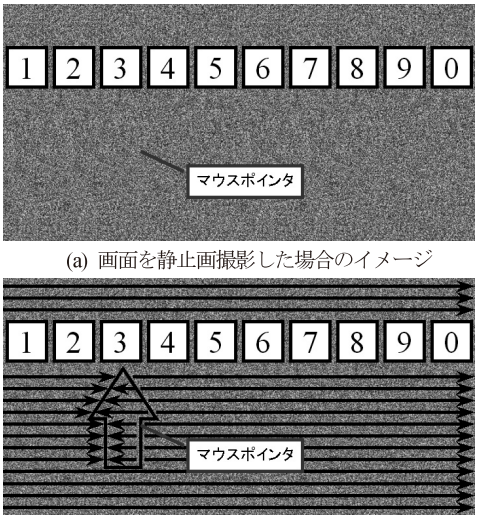
であり，被験者ごとに 10 種類の平仮名からランダムに 1 文字を選択し，実験を行った．被験者には，ディスプレイから 60 cm 程度離れた距離から肉眼でディスプレイに映し出された文字を見てもらい，それが何の文字に見えるか回答してもらった．また，文字が判別できた被験者に対しては，文字がどの程度知覚できたかについて，「1：完全に知覚できた」，「2：なんとなく知覚できた」，「3：何かが写っているように感じた」，「4：何も写っていないように感じた」の 4 つから 1 つを選んで答えてもらった．なお，被験者には平仮名が使用されていることのみを事前に伝えてある．

5.4 実験結果および考察

5.2 節および 5.3 節の評価実験を行った結果を**表 1** に示す．表 1 の「視認性評価値」の列は 5.2 節の実験で得られた全被験者・全文字の評価値の平均値を示している．「静止画判読成功率」および「動画判読成功率」の列は，5.3 節の実験において，静止画または動画から文字が判別できた被験者の割合が記されている．また，文字を判別できた被験者に対しては「その文字がどの程度知覚できたか」を回答してもらったが，文字を判別できた全被験者の評価値の平均値を括弧の中に併記してある．

視認性実験の結果から，提案方式の視認性は，文字を知覚できないほどではないが，かなり低いことが判明した．方式 1 および方式 3 の視認性が方式 2，提案方式よりも高いことから，ダミーエッジの影響による視認性の低下が大きいといえる．方式 2 の視認性が提案方式とほぼ変わらないことから，ランダムドットの流れのスピードは視認性に影響するものの甚大ではないと考えられる．

静止画撮影については，今回の実験ではどの表示方式も大きな撮影対策効果が得られることが確かめられた．方式 1 および方式 3 においてはダミーエッジを導入していないため，静止画撮影された場合に文字と背景の境目がエッジとして観測されると予想されたが，表示されている文字が判読されることはなかった．ランダムドットを 24 ビットカラーで作成することによってエッジの発生が抑えられ（エッジが知覚されにくくなり），これが方式 1 および方式 3 の静止画撮影耐性を向上させたのだと考えられる．



(a) 画面を静止画撮影した場合のイメージ
(b) 画面を直接みた場合のイメージ

図 23 銀行 ATM への適用例
Fig. 23 An example application to ATM.

また，動画撮影に対する耐性については，4.2 節で示した式 (1) を満たす提案方式のみにその有効性が確認されるという結果となった．

以上の結果より，提案方式はカメラによる撮影に十分な耐性を有した文字表示方式であることが確認できた．しかし，肉眼で文字を知覚可能ではあるものの，ランダムドット画像により構成されているため，通常の文字に比べ，その視認性が極端に低いことが分かった．また提案方式は，リフレッシュレートの低い表示装置では動画撮影への対応ができないという問題がある．これらの問題に関しては今後，早急に改善していく必要がある．

特に，今回の実験では 400×400 画素（12.0 cm 四方）の枠の中に大きく 1 文字を表示しているにもかかわらず，十分な視認性が得られておらず，現時点の方式では実用に向けてのハードルは高い．ただし，銀行 ATM で暗証番号を入力する場面などにおいては，文字（ATM の画面に表示される 0〜9 の数字）ではなく，これを指し示すマウスポインタを提案方式によって表示するようなシステムを構成することは可能であるのではないかと考える．この場合，(i) 暗証番号の入力画面を撮影されてもマウスポインタが写らず，どの数字を入力したのかを盗撮から守ることができる，(ii) 0〜9 の数字そのものは通常の表示であるため，詳

細な形状の認識が必要な文字に対しては視認性の低下はない，(iii) マウスポインタにおいては（詳細な形状の認識よりも）その位置さえ分かればよいので，視認性の低い提案方式での表示であっても致命的な問題とはならない，などのある程度の妥当性を有するシステムとしての運用が期待される．**図 23** に本方式の画面例のイメージを示した．

6. ま と め

本論文では，撮影耐性・視認性・汎用性を有する文字表示方式の実現を目指し，人間の「動きを知覚する能力」の高さを利用した文字表示方式を提案した．プロトタイプシステムによる評価実験の結果，提案方式は，(i) 撮影耐性に対しては，固定されたカメラによる静止画撮影および動画撮影に対する耐性を有する，(ii) 視認性に対しては，最低限の視認性を有する，(iii) 汎用性に対しては，ソフトウェアにより実装可能であるが，動画による撮影耐性を備えるにはある程度以上のリフレッシュレートを有する表示装置が必要である，という性質を持つことが確認された．

今回の提案方式では，固定設置されたカメラでの撮影への対策に限定される，リフレッシュレートの低い表示装置では動画撮影への対応ができない，文字の判読性が極端に低いといった問題を有するものの，機密情報を扱う職場や ATM などにおける隠しカメラへの対策としては効果を発揮することが期待される方式であると考えられる．

今後は，上記の問題の解決や，文字だけでなく画像などへの適用なども検討し，提案方式の実用性を高め，様々な状況におけるカメラでの撮影による攻撃を防ぐことが可能な方式を目指していきたい．

謝辞 静岡大学情報学部林部敬吉先生には評価実験に関するご助言をいただいた．同大学院情報学研究科小島悠子氏には評価実験の実施にあたって補助を担当していただいた．また，本研究は一部，（財）セコム科学技術振興財団の研究助成を受けた．ここに謝意を表する．

参 考 文 献

1) Zhao, J. and Koch, E.: Embedding robust labels into images for copyright protection, *Proc. ICIPR*, pp.242–251 (1995).
2) Tanaka, K., Nakamura, Y. and Matsui, K.: Embedding Secret Information Into a Dithered Multilevel Image, *Proc. 1990 IEEE Military Communications Conference*, pp.216–220 (1990).
3) Diffie, W. and Hellman, M.E.: New direction in cryptography, *IEEE Trans. Information Theory*, Vol.IT-22, No.6, pp.644–654 (1976).
4) Rivest, R.L., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
5) トリニティーセキュリティーシステムズ：Pirates Buster for Picture. http://www.trinity-ss.com/
6) Don't Capt Technology. http://dontcapt.com/
7) MarkAny: Web Defender. http://www.markany.co.jp/
8) Vintage Solutions, Ltd.: ANTIDOTE for PC HTML Protector. http://www.vintage-solutions.com/
9) Best, R.M.: Crypto microprocessor for executing enciphered programs, US patent 4278837, Issued September 1981.
10) Best, R.M.: Crypto microprocessor that executes enciphered programs, US patent 4465901, Issued September 1984.
11) Best, R.M.: Microprocessor for executing encrypted programs, US patent 4168396, Issued September 1979.
12) 末松俊成，今井秀樹：CMP（Crypto Microprocessor）の一構成方法とその応用例，電子情報通信学会技術報告，ISEC98-8, pp.71–79 (1998).
13) 西垣正勝，小澤卓也，曽我正和，田窪昭夫：動的復号型表示方式による画像コンテンツの不正コピー防止，情報処理学会論文誌，Vol.42, No.8, pp.1983–1991 (2001).
14) 塩田和也，吉田英樹，曽我正和，田窪昭夫，林部敬吉，中村逸一，水野忠則，西垣正勝：視覚特性を利用した画像型ディジタルコンテンツの不正コピー防止，情報処理学会論文誌，Vol.46, No.8, pp.2078–2097 (2005).
15) 宮木 孝，塩田和也，吉田英樹，西尾秀一，西垣正勝：視覚型秘密分散を用いたテキスト型秘密分散方式の提案，コンピュータセキュリティシンポジウム 2004 論文集，pp.73–78 (2004).
16) 宮木 孝，塩田和也，吉田英樹，小澤雅治，西垣正勝：自然画像を用いた視覚複合型秘密分散によるテキストハイディング，情報処理学会研究報告，2004-CSEC-30-31, pp.221–228 (2005).
17) 宮木 孝，塩田和也，吉田英樹，小澤雅治，西垣正勝：自然画像を用いた拡張 VSS 型画像変調によるテキストハイディングの改良，コンピュータセキュリティシンポジウム 2005 論文集，pp.571–576 (2005).
18) 桜井鐘治，吉田真利子，撫中達司：モバイル個人認証方式の提案と評価，コンピュータセキュリティシンポジウム 2004 論文集，pp.625–635 (2004).
19) 徐 強，西垣正勝：ニーモニックに基づくワンタイム・パスワード型画像認証の実現可能性に関する

検討，情報処理学会研究報告，2006-CSEC-32-54, pp.317–322 (2006).
20) 大山　正，今井省吾，和氣典二：新編感覚知覚心理学ハンドブック，誠信書房 (1994).

(平成 19 年 3 月 19 日受付)
(平成 19 年 10 月 2 日採録)

西垣　正勝（正会員）

平成 2 年静岡大学工学部光電機械工学科卒業．平成 4 年同大学大学院修士課程修了．平成 7 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，平成 8 年静岡大学情報学部助手．平成 11 年同講師，平成 13 年同助教授．平成 18 年より同大学創造科学技術大学院助教授．平成 19 年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．

宮木　孝

平成 17 年静岡大学情報学部情報科学科卒業．平成 19 年同大学大学院情報学研究科修士課程修了．同年三菱電機エンジニアリング入社．在学中，情報セキュリティに関する研究に従事．

塩田　和也

平成 12 年静岡大学情報学部情報科学科卒業．平成 14 年同大学大学院修士課程修了．平成 17 年同大学院博士課程修了．同年チャンスラボ株式会社入社．博士（情報学）．在学中，情報セキュリティに関する研究に従事．

吉田　英樹

平成 8 年三重大学人文学部卒業．同年日本電信電話株式会社（研究開発職）入社．その後，東日本電信電話株式会社，西日本電信電話株式会社，株式会社 NTT データを経て平成 19 年より株式会社三菱東京 UFJ 銀行．IT 事業部調査役として IT ビジネスの企画・商用化に従事．

小澤　雅治

昭和 58 年 3 月横浜市立大学文理学部文科卒業．昭和 60 年 8 月株式会社ブレーンウエア入社．昭和 62 年 4 月株式会社エー・ブイ・エス入社，常務取締役就任．平成 2 年 7 月チャンスラボ株式会社（旧株式会社エーティーティー総研）入社，同年 11 月代表取締役就任．平成 18 年 6 月株式会社アドバックス代表取締役就任．