社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (45)
2007－CSEC－ 36 (45)
2007／3／2

高速切替表示を用いた撮影耐性を有する文字表示方式の提案

宮木 孝* 塩田 和也† 吉田 英樹‡ 小澤 雅治† 西垣 正勝††

* 静岡大学大学院情報学研究科, 432-8011 静岡県浜松市城北 3-5-1
† チャンスラボ株式会社, 104-0045 東京都中央区築地 1-4-5 第 37 興和ビル 6 階
‡ 株式会社 NTT データ, 135-6033 東京都江東区豊洲 3-3-3 豊洲センタービル
†† 静岡大学創造科学技術大学院, 432-8011 静岡県浜松市城北 3-5-1
E-mail: nisigaki@inf.shizuoka.ac.jp

あらまし 近年，個人情報や機密情報の取り扱いなど，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．

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

Takashi Miyaki, Kazuya Shioda, Hideki Yoshida, Masaharu Ozawa, Masakatsu Nishigaki

* Graduate School of Informatics, Shizuoka University,
3-5-1 Johoku Hamamatsu-shi, Shizuoka, 432-8011 Japan
† Chance Lab. Corp., Nihon-koa-Ginza-biru-8F, 7-13-10 Ginza, Shuo-ku, Tokyo, 104-0061 Japan
‡ NTT Data Corp., Toyosu-Center-biru, 3-3-3 Toyosu, Koto-ku, Tokyo, 135-6033 Japan
†† Graduate School of Science and Technology, Shizuoka University,
3-5-1 Johoku Hamamatsu-shi, Shizuoka, 432-8011 Japan
E-mail: nisigaki@inf.shizuoka.ac.jp

Abstract. 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 isn't 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．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が困難である．例えば，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，肩越しに或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た場合においても，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等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言える．

特に本稿では，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一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．例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一つである．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[1,2,3,4]．画像変調方式においては，オリジナル画像を2枚にコピーした上で，片方の画像に対しては輝度を＋αし，他方の画像においては輝度を－α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．切替速度が 100Hz 程度以上になると，人間の眼はその切り替わりを認識できなくなり，混色が起こって＋αの明るさと－α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．

本稿では，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．すなわち，高速切り替え表示を利用することで，「コンピュータ上には存在しない機密情報を人間だけが知覚できる」という仕組みを実現することを検討する．コンピュータがディスプレイに描画する情報はコンピュータ内に存在する情報に他ならないため，ディスプレイ画面をカメラ（ディジタルスチルカメラ）で撮影したとしても，コンピュータ上に存在しない機密情報をカメラに写すことはできない．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．

2．一般的な撮影対策手法

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一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[5,6]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挙げられる．プライバシフィルタは，PC や携帯電話等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得ることも予想される．加えて，プロジェクタのようなに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上に，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．

以上のことを踏まえると，ディスプレイやプロジェクタ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カメラで撮影するという行為に対する対策が必要であることがわかる．そこで，次章からはカメラによる撮影に耐性を有する文字情報の表示方式の提案を行う．

3．撮影耐性を有する文字表示方式

例えば，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の実現を目指す．

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．例えば，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速度で映すことで，人間は領域の上半分のランダムドットが右に動いているように知覚する．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．

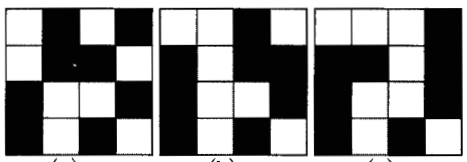


図1．上半分が右に動くランダムドット

これを文字表示に適用する場合，文字領域と背景領域を共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可能となる．

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はっきりと現れてしまうのである．これを図1の場合で考えてみると，例えばシャッターが開いてから閉じるまでの間に図1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2のような画像(図1.(a)～図1(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．

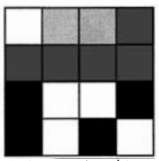


図2．図1の写真イメージ

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，一定時間内に捉えた光の総量によって画像を生成する．例えば，写真を撮る場合には，シャッターが開いた直後から光を取り込み始め，シャッターが閉じる瞬間までの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，二つの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共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．例えば，図3のような3枚の画像を(a)→(b)→(c)→(a)→・・・の順番に高速切替表示することで，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，例えば露光時間中に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4(図3.(a)～図3.(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．

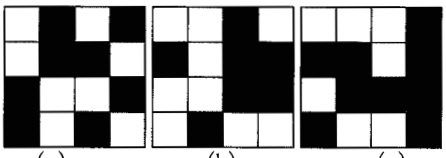


図3．上半分が右，下半分が左に動くランダムドット

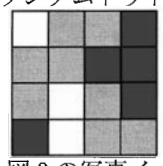


図4．図3の写真イメージ

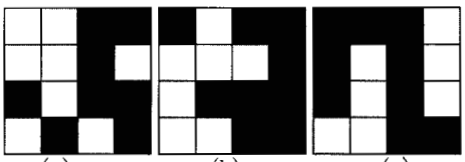
4．提案方式の問題とその解決策

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可能性がある．例えば図5は，3枚の画像を(a)→(b) →(c) →(a) →・・・の順番で高速切替表示することで，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，例えば露光時間中に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 6 のようになり，急激な輝度の変化が発生している箇所が現れることから，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5，図6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．



(a) (b) (c)

図5．左半分が右，右半分が左に動くランダムドット

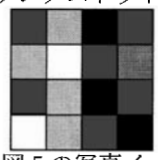
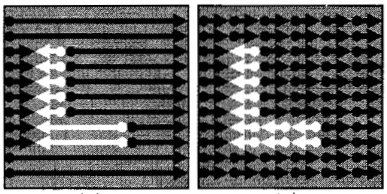


図6．図5の写真イメージ

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．例えば図7は，アルファベットの「L」という文字の流れ（図7.(a)）が等間隔の小さな流れになるように領域分割した例（図 7.(b)）である．「各ドットが図7.(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生する可能性のある場所を図8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得るため，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．

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



(a) (b)

図7．大きな流れの細分化

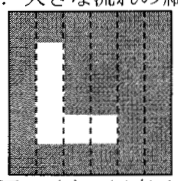


図8．図7.(b)の写真イメージ

も十分考慮されるため，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．

一般的なビデオカメラの場合，動画は 24Hz～30Hz 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，30Hz 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．したがって本稿では，30Hz 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．

本稿では，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．

例えば，図9のような2×2画素の3枚の画像を(a)→(b) →(c) →(a) →・・・の順番に60Hzの速度で高速切替表示したとしよう．ここで，図9における $Ai, Bi\ (1 \le i \le 3)$ の値は各画素の輝度である．図9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 30Hz 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10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

$Ci\,(1 \le i \le 12)$から，

$(A_1 + A_3)/2 = C_1, (A_2 + A_1)/2 = C_2, \ldots$

という連立方程式が得られることとなり，$Ai, Bi\,(1 \le i \le 3)$が求められてしまう．したがって，図9.(a)，(b)，(c)のそれぞれの画像が判明してしまい，各領域(図9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り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11に示す．ここで，$Ai, Bi\,(1 \le i \le \infty)$はそれぞれ乱数系列である．

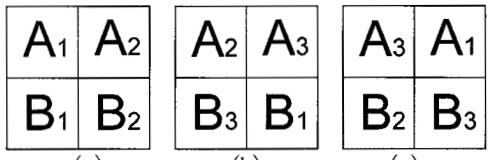


図9．有限個のランダムドット画像の繰り返し

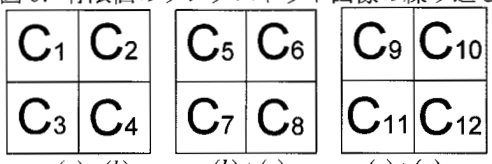


図10．図9を撮影したフレーム

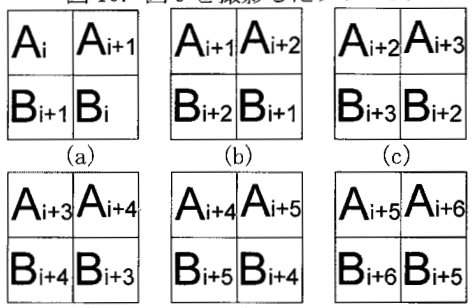


図11．無限個のランダムドット画像の切替

今，図9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(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．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Ai, Bi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Ai, Bi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み合わせを試せば，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．この結果，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その輝度値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．

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，その画素は常に白であった（または常に黒であった）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白や黒に固定されてしまうことがないようにする必要がある．

一方，ビデオカメラで撮影された動画における各フレームの画像は，1/30秒間ごとの平均輝度が写った画像が連続的に並んだものとなっている．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．これを動きを捉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．そこで，4.1節の方法を採用し，流れの領域を細分化することにより，1/30秒間の内に，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採る必要がある．

なお，以上の方法については，フレームの切替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したが，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．ただし，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．例えばプロジェクタなどは，現在の製品で30Hz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．

5．提案方式の評価

提案方式のプロトタイプシステムを実装し，評価を行った．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．DMC-FX5は静止画および動画

の撮影が可能であり，静止画撮影における露光時間は1～1/2000秒の間で自動調節，動画撮影におけるフレームレートは30Hzである．

今回は400×400画素の背景の上に大きく「あ」という文字を表示した．文字は4.2節の方法で作成した．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．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秒間の内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120Hzである．

まず，肉眼でディスプレイを見た場合には，「あ」の文字が十分に知覚可能であった．ただし，ディスプレイから離れた場合には知覚しにくい状態となった．これはランダムドット画像のドットが小さくてよく見えないことが原因であると考えられる．判読性を向上するにはランダムドット画像の1ドットのサイズを大きくすればよいだろう．

次に，このディスプレイの画面をカメラによって撮影した．撮影はカメラを固定された台の上に配置し，手ブレの発生しない状態で行った．静止画写真を図12に，動画中の任意の連続した2フレームを図13に示す．いずれの写真も完全なランダムドット画像となっており，それぞれ1枚の写真から文字を読み取ることはできなかった．なお，図12には，文字の表示領域を破線で記してある．また，4.2節で説明したように，動画中の全フレームの画像を解析したとしても，文字領域と背景領域の区別を付けることは不可能であるはずである．

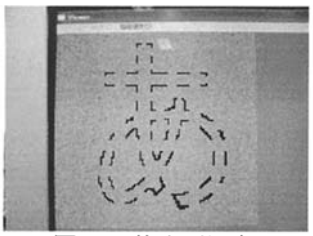


図12．静止画写真

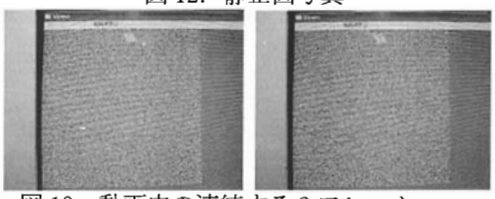


図13．動画中の連続する2フレーム

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，肉眼では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，その判読性が極端に低い．この問題に関しては今後，早急に改善していく必要がある．

6．まとめ

本論文では，カメラによる撮影に耐性を有する文字表示方式の提案を行った．人間の「動きを知覚する能力」の高さを利用した方式を提案し，その実装例を示した．プロトタイプシステムによる実験の結果，提案方式を用いることで，人間が文字を知覚することを可能にしつつ，カメラでは撮影されないような表示が実現していることが証明された．

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，提案方式の汎用性を高め，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く予定である．

参考文献

[1] 塩田，吉田，曽我，田窪，林部，中村，水野，西垣，“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 num.8 pp.2078-pp.2097

[2] 宮木，塩田，吉田，西尾，西垣，“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，pp.73-pp.78，Oct.2004

[3] 宮木，塩田，吉田，小澤，西垣，“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，” ISEC2005-07，pp.221-pp.228，Jul.2005

[4] 宮木，塩田，吉田，小澤，西垣，“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，pp.571-pp.576，Oct.2005

[5] 桜井，吉田，撫中，” 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，pp.625-pp.635，Oct.2004

[6] 徐，西垣，“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，” 2006-CSEC-32，pp.317-pp.322，Mar.2006