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

西垣正勝[†1] 小澤卓也[†2]
曽我正和[†3] 田窪昭夫[†4]

画像コンテンツの不正コピー防止技術の実現を阻害する原因の1つとしてあげられるのが，OSの持つスクリーンキャプチャ機能である．画像コンテンツに対して暗号化を施したとしても，ユーザがコンテンツを鑑賞する時点ではコンテンツの暗号化は解かれ，オリジナルデータがVRAM上に展開される．よってスクリーンキャプチャ機能により，VRAMからオリジナルデータの複製を作ることが可能である．また，VRAMは通常，メインメモリにマッピングされているため，これを直接アクセスされることにより画像データは漏洩する．そこで本論文では，暗号化された画像コンテンツの復号をディスプレイ表示の直前に行う「動的復号型表示方式」を提案する．本方式によればCPUの管理するいかなる記憶装置上にも著作画像のオリジナルデータは残らない．本方式においては画像の表示速度に追従するだけの高速な復号装置が必要になるが，復号回路を並列パイプライン化することによりこれを実現する．

A Copy Protection of Image Data by Dynamic Decryption

Masakatsu Nishigaki,[†1] Takuya Kozawa,[†2] Masakazu Soga[†3]
and Akio Takubo[†4]

In the conventional computer system, data encryption can not protect image data from illegal copying. Encrypted images are decoded by the CPU and stored in the VRAM before being displayed. As a result of this, the information is vulnerable while it is in the VRAM. This paper proposes to decode encrypted image data by using a dedicated hardware module placed between the VRAM and RAMDAC. In so doing, the data remains encrypted in the VRAM and is protected against illegal copying.

1. はじめに

近年，画像データをPCからディスプレイにデジタル信号のまま転送するDVI（Digital Visual Interface）[1]が注目を浴びている．また，この際のデータ転送時におけるセキュリティを守るためにDVI CPS（Content Protection System）[2]の提案が行われている．しかし，DVI CPSはあくまでもデバイス間を流れるデータの保護を目的としており，VRAM上にはオリジナルデータが存在する．すなわち，スクリーンキャプチャによってVRAM上の画像データを不正にコピーすることは可能である．

スクリーンキャプチャによる画像の不正コピー防止を目的として開発されたシステムとしてClever Content Viewer[3]があげられる．Clever Content Viewerはアプリケーションが OSにスクリーンキャプチャを要求する命令をフックすることでスクリーンキャプチャによる不正コピーを防止している．しかしクラッカーは同様の方法でClever Content Viewerがフックした命令をもう一度フックし，不正コピーを行うことが可能である．またVRAM上の情報はメインメモリにマッピングされているため，メインメモリに直接アクセスすることでオリジナル情報を取得することができる．このように基本的にソフトウェアによる不正コピー防止システムには限界があるといえる．

我々は，スクリーンキャプチャや機械語によるメモリへの直接アクセスなどから画像データを守るためにはVRAM上の内容自体を暗号化して保護する必要があると考える．そこで，暗号化された画像コンテン

†1 静岡大学情報学部情報科学科
Faculty of Information, Shizuoka University
†2 日本システムウェア株式会社ネットワークソリューション事業本部
Nippon Systemware Co. Ltd.
†3 岩手県立大学ソフトウェア情報学部
Faculty of Software and Information Science, Iwate Prefectural University
†4 三菱電機情報システム製作所
Mitsubishi Electric Corp.

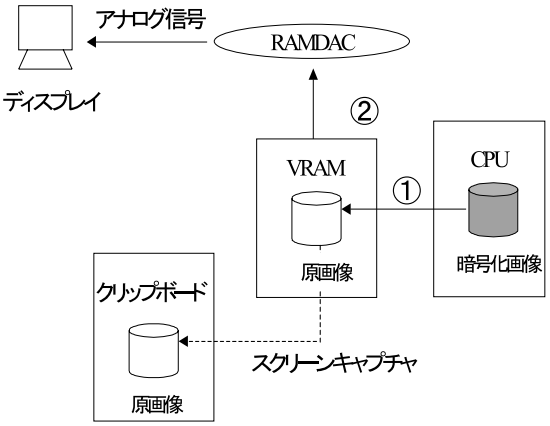

図 1 現在の画像表示機構
Fig. 1 Flow of data processing to display images.

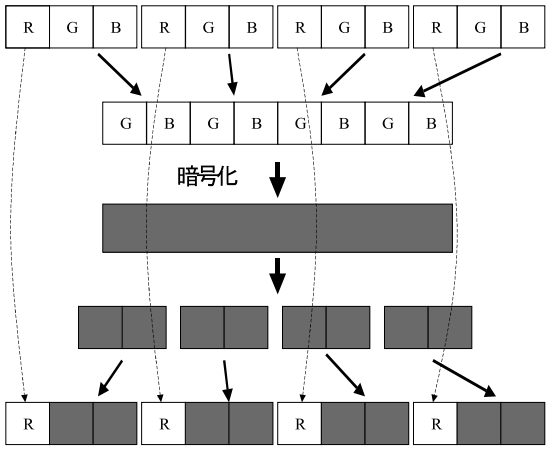

図 2 4 画素単位による画像の暗号化
Fig. 2 Encryption by four pixels of image data.

ツの復号をディスプレイ表示の直前に行う「動的復号型表示方式」を提案する．ここで，データの復号がソフトウェア的に行われた場合には，メインメモリ上に復号結果が残ることになり，セキュリティホールが発生する．また，データをリアルタイムで復号する必要があることからも，本方式における復号機構はハードウェア的に実装されなければならない．

2. スクリーンキャプチャ機能と著作権保護

スクリーンキャプチャは VRAM メモリ上の情報をクリップボード（メインメモリなどのバッファ用領域）にコピーする機能である．現在の画像表示機構では，まず CPU はグラフィックボードに画面構成要素の各々に対する画像情報を送り（**図 1** における ①），VRAM 上にディスプレイ 1 画面分の画面情報を構築する．次に，VRAM 上の画面情報は RAMDAC に渡され（図 1 における ②），各画素ごとにアナログ信号に変換された後，ディスプレイに送られる．

コンテンツの不正コピーに対抗する手段として暗号化が注目されている．しかし，従来システムにおいては，コンテンツの復号は CPU が行っており（図 1 における ①），VRAM には原画像が存在することとなる．このため，スクリーンキャプチャ機能やメモリへの直接アクセスによって容易に画像データの複製が行えてしまう．

本論文では，画像コンテンツの復号を RAMDAC（図 1 における ②）において行う方式を提案する．この方式ではコンテンツは VRAM 上においても暗号化されたままである．したがって，スクリーンキャプチャやメモリアクセスによって VRAM 上の暗号化画像データがコピーされてしまっても（復号鍵が盗まれないかぎり）問題はない．ここでは，本方式を「動的復号型」の表示方式と呼ぶこととする．

3. 動的復号型表示方式

3.1 画素単位の暗号化

ディスプレイの 1 画面中に表示される画像データは，コンテンツどうしの重なりやウィンドウの縮小などにより，その画像コンテンツの一部分のみが表示されることも多い．したがって，画像コンテンツ全体に対する暗号化や連鎖モード（CBC モードや CFB モード）の暗号化を行ってしまっては，画面に表示されている部分の情報のみからコンテンツを復号することが不可能となる．そこで本論文では，著作物画像データを画素ごとに暗号化する方式を採用する．これにより，暗号化画像の一部が欠落しても，残りの画像を復号することが可能となる．

ただし，各画素ごとの暗号化を行った場合には，同一の色は同一の暗号化データに変換されてしまい，攻撃耐性が低くなる．したがって本方式においては，データ長が 64 ビットのブロック暗号を用い，X 軸方向に連続した 4 画素を 1 単位として暗号化を行うこととする．RGB 各 8 ビットの計 24 ビットの画素情報から，各画素における GB ビットを 4 画素分結合して 64 ビットとし，これを暗号化する（**図 2**）．

3.2 著作物コンテンツの識別

VRAM 内で構築された 1 画面分の画像情報の中には，暗号化されている画像コンテンツ（著作物コンテンツ）と暗号化されていない画像コンテンツが混在する．両者を正しくディスプレイに表示させるには，画面上のどこに著作物コンテンツが存在するかを識別し，その部分のみを復号する必要がある．

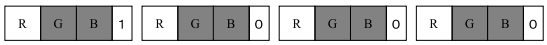

図 3 識別フラグを追加した画素情報
Fig. 3 Image data with a flag for copyright detection.

この識別方法として，今回は画素情報に新たに識別ビットを加え，1 画素を 25 ビットデータとすることを提案する．識別フラグは，3.1 節で述べた暗号化ブロックを構成する 4 画素における先頭の画素のみが「1」にセットされ，残りの 3 画素は「0」にセットされる（**図 3**）．また，著作物でない画像コンテンツの識別フラグにはすべての画素において「0」がセットされる．この結果，画面情報において識別フラグビットのみを検査していき，「1000」が検出された 4 画素分のデータが 1 つの暗号化ブロックであることを容易に識別することができる．

なお，各画素に識別フラグが付加されるため，本方式により暗号化される画像データのファイル形式は従来の形式とは異なったものとなる．従来のファイル形式により配信されている暗号化の必要のない画像データに対しては強制的にすべての識別フラグを「0」として扱うことにより，本方式は何の問題もなく従来の画像ファイルにも対処することが可能である．

3.3 高速な復号機構

本方式で提案する復号機構には，RAMDAC における D/A 変換の動作速度に追従できるデータ処理速度が求められる．そこで画像データの暗号化には公開鍵暗号方式よりも処理速度の高い共通鍵暗号方式を用いる．本論文では MISTY2 暗号[4]を採用する．そして，復号機構を並列化およびパイプライン化することでその高速化を達成する．

MISTY2 暗号はハードウェアによる高速な暗号化処理が実現できるように設計された暗号化方式であり，パイプライン処理が可能である．ただし，MISTY2 暗号は，復号と比べ，暗号化の方が並列処理性が高くパイプライン化に適するという性質を有する．本方式においてはコンテンツの復号処理に高速性が求められるので，MISTY2 の復号アルゴリズムによって画像コンテンツを暗号化し，MISTY2 の暗号化アルゴリズムによって暗号化コンテンツを復号することとする．すなわち，本方式では，MISTY2 暗号化機構をハードウェア化し，復号器として VRAM と RAMDAC の間に組み込む．

3.4 鍵の生成と保護

VRAM 上には 1 画面分の画像情報が構築される．1 つの画面上には複数の著作物画像が表示されうるが，VRAM 上では各画素がどの著作物画像に含まれるものであるかを特定するための情報は失われている．したがって，著作物データ暗号化用の共通鍵を統一する必要がある．そして，利用者本人がコンテンツを不正に復号してしまうことを防ぐために，この共通鍵は正規利用者に対しても秘匿されなければならない．このため本論文では，著作物データ暗号化用の共通鍵は利用者ごとに公の機関が生成するとし，その共通鍵は各利用者の PC のセキュアレジスタ（レジスタの内容を読み出すための機械語命令が用意されていない特別なレジスタ[5]）に格納されるという前提を置く．また，著作物コンテンツの暗号化も公の機関が請け負う．

4. 復号機構の実装

4.1 パイプライン型復号

3.3 節で述べたとおり，復号によるオーバヘッドが RAMDAC の D/A 変換の速度を落とすことがあってはならない．現在，RAMDAC の D/A 変換の処理速度は 200〜300 MHz である．よって本方式では RAMDAC の処理を妨げないように 400 MHz で動作可能な復号機構を設計する．これは各画素の復号を 2.5 nsec で行うことを意味する．本方式においては 4 画素を 1 ブロックとして暗号化しているので，各暗号化ブロックの復号を 10 nsec 以内に完了させる必要がある．すなわち，復号回路は 100 MHz で動作することとなる．

4 段 MISTY2 暗号化回路（本方式では復号器として使用する）をパイプライン化した回路を図 4〜図 8 に示す．上記の処理速度の制限を考慮し，4 段 MISTY 暗号器を 4 フェーズのパイプラインとして設計した．文献 4) では安全性と速度のバランスを考慮し MISTY2 の暗号化回路を 12 段とすることを推奨している．本論文の**図 4** の復号回路は文献 2) 44 ページの Figure 2 における 4 段分の暗号化回路に対応しているので，図 4 の復号回路を 3 段，縦続に用意することにする．よって，パイプラインの全フェーズ数は 12 となる．

図 4 中の FL ボックス，F0 ボックスを示したものが，それぞれ**図 5**，**図 6** である．さらに，図 6 中の FI ボックスの中身が**図 7** である．図 7 中の S9 ボックス，S7 ボックスはそれぞれ 9 ビット，7 ビット入出力の全単射関数をハードウェア化したものである（ここでは S9 ボックス内の一部のみを**図 8** に示した）．また，図中の KEY_i は，鍵スケジュール部によって 128 ビットの暗号化鍵から作られる各拡大鍵である．

図 4 の復号回路の各フェーズ内に存在するゲートの段数のうち，その最大数は 19 である．使用するゲートは AND，OR，XOR ゲートのみである．現在の標準的なプロセスでは，これらのゲートの 1 ゲート分の

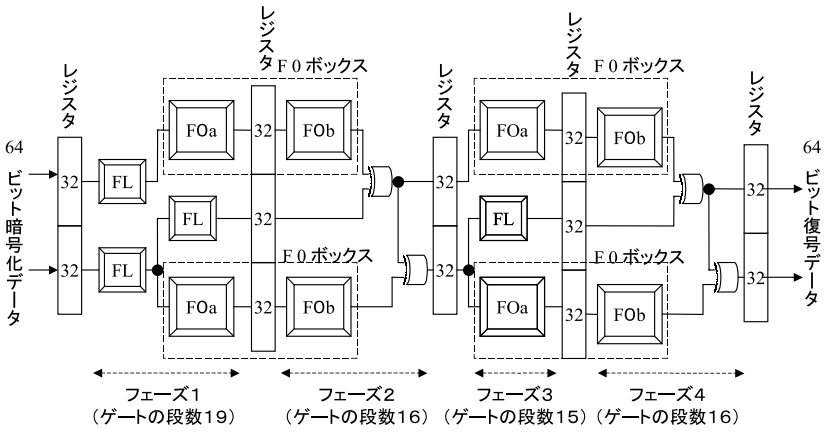

図 4 パイプライン型復号回路
Fig. 4 Pipelined decryption module.

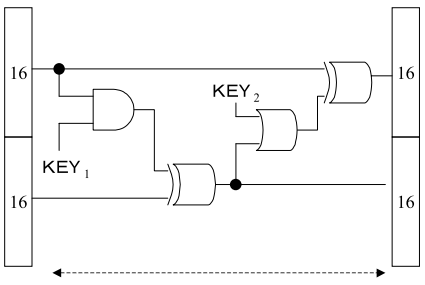

図 5 FL ボックス
Fig. 5 The FL box.

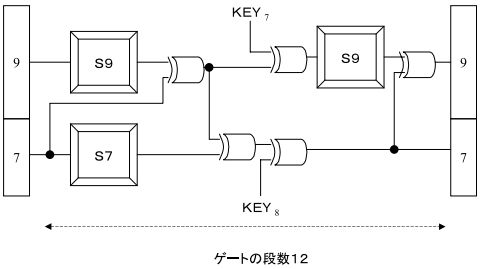

図 7 FI ボックス
Fig. 7 The FI box.

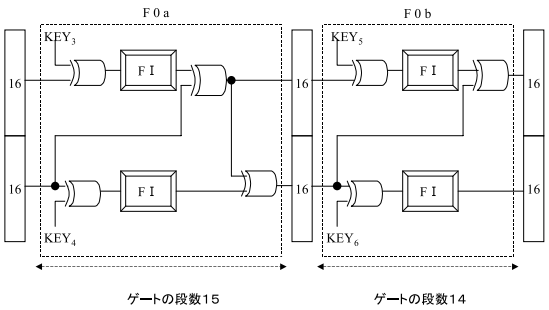

図 6 F0 ボックス
Fig. 6 The F0 box.

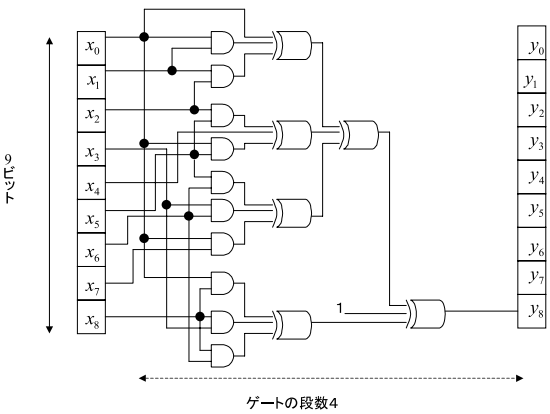

図 8 S9 ボックス（9 ビット目の出力のみ）
Fig. 8 The S9 box (only the 9th output is shown).

遅延時間は遅くとも 0.5 nsec であると考えてよいと思われる．したがって，本パイプラインの 1 フェーズの最大処理時間は 9.5 nsec 程度となり，上述の要求を満たす．このパイプライン型復号回路を 4 つ並列に配置することで 400 MHz で動作する復号機構を実現する．

4.2 復 号 機 構

図 9 に本方式の復号機構を示す．

③〜⑥ が 4.1 節で作成したパイプライン型復号回路である．① および ② は 4 画素分のデータを保持する 4 段のキュー（FIFO）である．① 内の 4 画素分のデータ GB（64 ビット）は後段のパイプライン型復号回路に送られる．その 4 画素が暗号化ブロックである場合には，信号 S が「1」となり，これを通知する．

同期回路 β ⑪〜⑬ はパイプラインを通過する暗号化データに他のデータ（暗号化されていないデータ）

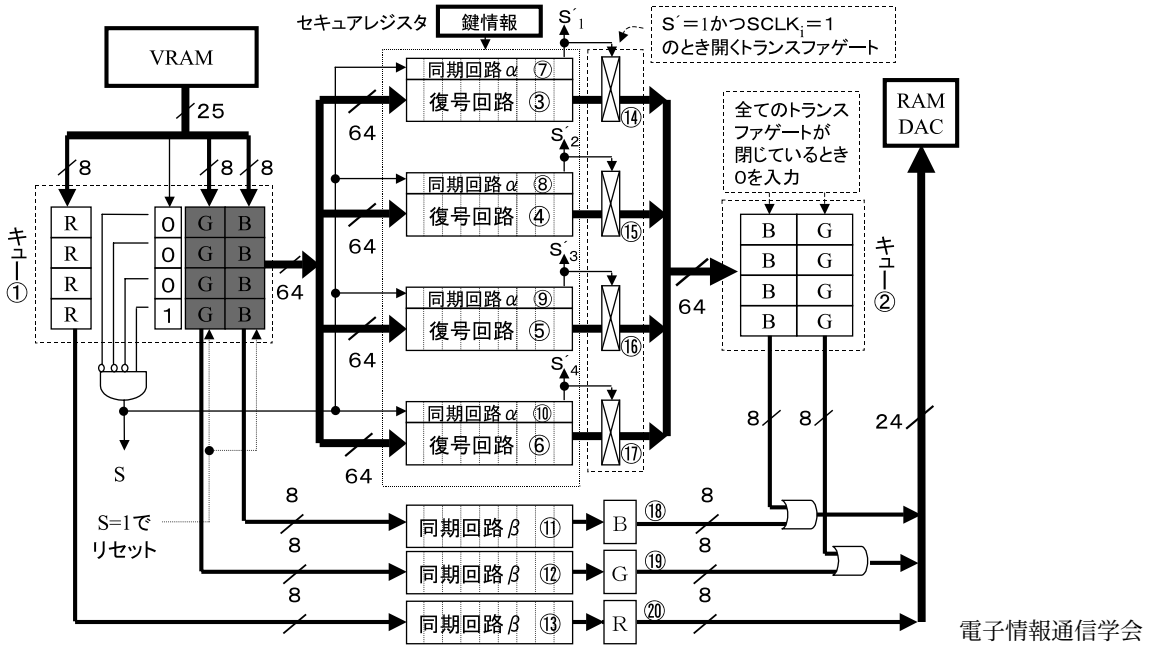

図 9 復号機構
Fig. 9 System diagram for dynamic decryption.

の転送速度を合わせる役割を果たしており，パイプラインのフェーズ数を N とした場合，$4N$ 段のシフトレジスタ（FIFO）により実装される（今回のパイプラインは $N = 12$ であるので，同期回路 β ⑪〜⑬ は 48 段のシフトレジスタである）．レジスタ ⑱〜⑳ は同期回路 β ⑪〜⑬ の出力をいったん保持するために設置されている．

4 つの復号回路（パイプライン）③〜⑥ には S 信号用の同期回路 α ⑦〜⑩ が付加されており，これは N 段のシフトレジスタ（FIFO）により実装されている．暗号化ブロックがパイプラインの最終フェーズに到達した時点で S 信号は S'_i 信号として取り出され，S'_i が「1」になることにより復号が完了したことを通知する．S'_i 信号によりトランスファゲート ⑭〜⑰ が開き，復号結果がキュー ② に格納される．

ここでパイプライン型復号回路および同期回路 α のみが 100 MHz で動作し，他のモジュールは 400 MHz で動くことに注意する．4 つのパイプラインおよび同期回路 α には，**図 10** で示されるように 1 クロックずつシフトしたクロックが印加される．なお，以下では復号機構中のすべてのレジスタがダウンエッジトリガでデータを取り込むとして説明する．

4.2.1 暗号化データの識別

本方式では暗号化データを復号する前段階として，VRAM から送られてくる各画素のデータが暗号化されているものなのか，そうでないものなのかを識別する必要がある．本方式においては 3.2 節で述べたとおり各画素情報に新たに識別フラグビットが追加されているので，4 画素分の暗号化ブロックを集めるために用意される 4 段のキュー（FIFO）においてこの識別が可能になる．復号機構は，クロック CLK に同期して VRAM から 1 画素分ずつ送られる画素情報を順次キュー ① に積んでいく．4 画素分のデータ GB（64 ビット）と信号 S はつねにパイプラインおよび同期回路 α に送られる．ここで，パイプラインおよび同期回路 α のクロック（図 10 における DCLK_i, SCLK_i）と他のモジュールのクロック（図 10 における CLK）の関係により，パイプラインおよび同期回路 α は CLK の 4 クロックごとにデータを取り込むことになる．すなわち，たとえば図 10 の例では，パイプライン ③ および同期回路 α ⑦ は I, V, IX, ⋯ のクロック期間でデータ GB と信号 S を取り込む．同様に，④ と ⑧，⑤ と ⑨，⑥ と ⑩ はそれぞれ II, VI, ⋯ のクロック期間，III, VII, ⋯ のクロック期間，IV, VIII, ⋯ のクロック期間でデータを取り込む．この結果，どのクロック期間で S が「1」になったとしても，その時点の暗号化ブロックと信号 S はいずれかのパイプラインおよび同期回路 α に正しく送られ，かつ，S が「0」の時点のデータがすでにパイプラインに送られている暗号化データを壊すこと

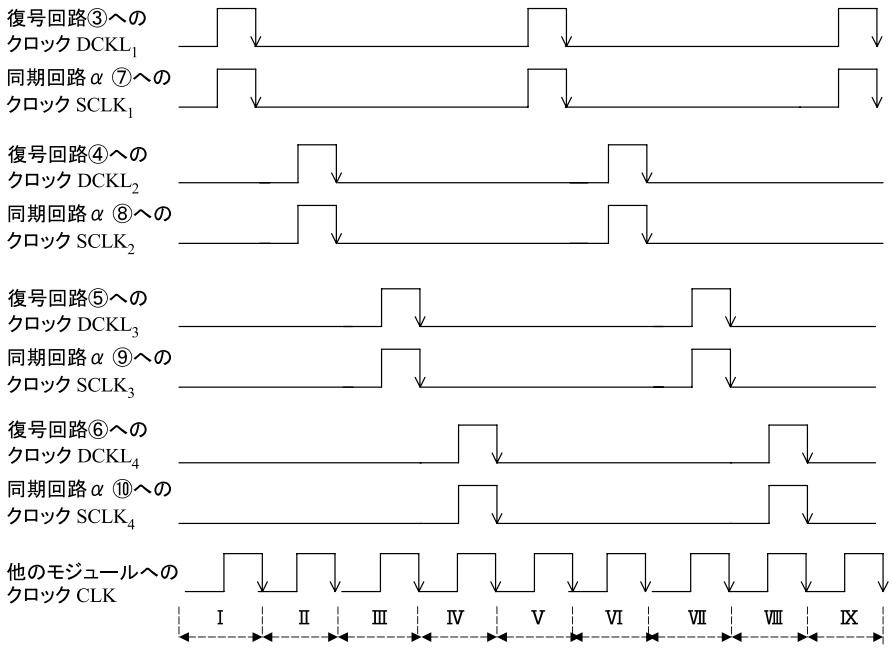

図 10 各モジュールへのクロック
Fig. 10 Clock signals given to each module.

もない．

なお，キュー ① からは，クロック CLK に同期してつねに 1 画素分のデータ GB が同期回路 β ⑪，⑫ に送られている（このデータは 4 クロック前にキュー ① に格納されたものであることに注意）．また，S が「1」の場合には，暗号化ブロックがパイプラインに送られるとともに，当該データがキュー ① から削除される（実際には，暗号化ブロック（64 ビット）がいずれかのパイプラインに取り込まれるクロックにおいて，キュー ① の過去 3 画素分のデータ GB をリセットし，同期回路 β ⑪，⑫ には「0」を送る）．すなわち，データ GB が暗号化データだった場合には，その時点から 4 画素分の「0」データが同期回路 β ⑪，⑫ に送られることになる．データ R は，キュー ① を通過した後に機械的に同期回路 β ⑬ に送られる．

4.2.2 復号データの抽出

復号データは 4 つのパイプラインのいずれかから出力される．しかし，各パイプラインには DCLK_i に同期してつねにデータが送り込まれているため，暗号化ブロックがパイプラインの最終フェーズに到達していない間は，パイプラインからは無意味なデータが出力されることになる．したがって，4 つのパイプラインから正しい復号データのみを抽出することが必要となる．

各パイプラインに付加されている S 信号用の同期回路 α ⑦〜⑩ およびトランスファゲート ⑭〜⑰ がこれを可能にする．同期回路 α ⑦〜⑩ には，対応するパイプラインが暗号化ブロックを取り込んだときのみ「1」が入力される（たとえば，パイプライン ③ に暗号化ブロックが取り込まれた場合には，その時点の S ＝「1」は同期回路 α ⑦ に送られる）．そして，この「1」はパイプラインと同期して同期回路 α 中を移動し，当該暗号化ブロックがパイプラインの最終フェーズに到達した時点で，S'_1，S'_2，S'_3，S'_4 信号のいずれかとして取り出される．トランスファゲート ⑭〜⑰ はそれぞれ，「$S'_1 = 1$ かつ $\mathrm{SCLK}_1 = 1$」，「$S'_2 = 1$ かつ $\mathrm{SCLK}_2 = 1$」，「$S'_3 = 1$ かつ $\mathrm{SCLK}_3 = 1$」，「$S'_4 = 1$ かつ $\mathrm{SCLK}_4 = 1$」のときにのみ，当該パイプラインの出力をキュー ② に通過させる．キュー ② はいずれかのトランスファゲートが開いているときのみ，その 4 画素分のデータを取り込む．この結果，復号されたデータのみが正しくキュー ② に格納される．

4.2.3 画素データの統合

4.2.1 項で，暗号化ブロックがいずれかのパイプラインに送られた場合には，その後，4 画素分の「0」データが同期回路 β ⑪，⑫ に送られることを述べた．同期回路 β ⑪，⑫ の働きにより，当該暗号化ブロックがパイプラインを通じて復号され，その復号結果がキュー ② に格納された時点で，4 画素分の「0」データのうちの 1 番目のデータがレジスタ ⑱，⑲ に格納

されることになる．したがって，その後段の OR ゲートによりキュー ② 内の復号結果が正しく RAMDAC に送られることになる．また，同期回路 β ⑬ により，この時点でその画素に対応するデータ R がレジスタ ⑳ に格納されているため，データ R も正しく統合される．

なお，すべてのトランスファゲート ⑭〜⑰ が閉じているときは，キュー ② にはクロック CLK に同期して 1 画素分の「0」データが入力される．したがって，暗号化されていない画素情報を RAMDAC に送る時点では，キュー ② からは「0」が出力されることになる．一方，暗号化されていない画素のデータ GB は同期回路 β ⑪，⑫ にそのまま送られるため，その時点におけるレジスタ ⑱，⑲ には当該画素のデータ GB が格納されている．したがって，やはりその後段の OR ゲートにより画素データ GB は正しく RAMDAC に送られる．同期回路 β ⑬ とレジスタ ⑳ により，データ R もこの時点で同様に正しく統合される．

5. 考　　察

5.1 暗号化方式

画素単位の暗号化においては，同一色の画素は同一の暗号化データに変換されてしまうことになり，その強度が懸念される．64 ビットを 1 ブロックとする暗号化を採用した場合，画素単位の暗号強度を向上させるためには，たとえば，

(1) 各画素 24 ビットに乱数 40 ビットを付加し，1 ブロックとする，
(2) 2 画素分 48 ビットに乱数 16 ビットを付加し，1 ブロックとする，
(3) 4 画素分の 2 原色成分（たとえば GB 成分）64 ビットを 1 ブロックとする，
(4) 8 画素分の 1 原色成分（たとえば B 成分）64 ビットを 1 ブロックとする，

などの方法が考えられる．

ここで，(1) や (2) のように乱数を付加する方法には画像ファイルのデータサイズが大きくなるという欠点が存在する．一方，(2)，(3)，(4) のように複数の画素を統合して 1 ブロックとする方法では，統合された画素が 1 つでも欠落してしまうとその暗号化ブロックの復号が誤ることになる．

本論文では，画像ファイルのデータサイズの肥大化を避け，かつ，統合される画素数が少ない上記 (3) の方法を採用した．なお，RAMDAC においては X 軸方向（水平方向）に各画素が走査され，D/A 変換が行われることを考慮し，X 軸方向に連続した 4 画素を 1 ブロックに統合している．

また，暗号強度の観点からは CBC モードや CFB モードの暗号化が推奨される．しかし，ブロック間の暗号化に連鎖関係が存在すると，1 ブロックが欠けただけでもそれ以降のすべての画素の復号が行えなくなるため，画素単位の暗号化には適用できない．本方式により適した暗号化方式に関しては今後とも検討を続けていく．

5.2 画像ファイルの圧縮

画像データを画素単位で暗号化した場合，画像データを不可逆圧縮することが不可能となる．画像データを不可逆圧縮してしまうと，それを完全に元に戻すことができず，暗号化データが破壊されてしまうからである．しかし，著作物画像を作成する著者の多くは画像劣化を招く不可逆圧縮を嫌う傾向が強い．すでに可逆圧縮技術の圧縮率を向上させる研究は鋭意進められており[6]，さらに，今後のブロードバンド化にともなって容量がある程度大きいファイルの送信も認められるようになると期待される．よって，近い将来においては，可逆圧縮された原画データがネットワーク経由で売買される時代がくるものと予想される．本論文は，本方式はそのような原画データを保護するための仕組みであるという立場に立っている．

画像の不可逆圧縮が不可能なため，本方式では画像データのファイル形式はビットマップ（BMP）形式とせざるをえない．ただしここで，OS はすべての画像ファイルを DIB 形式で取り扱い，グラフィックボードはこの DIB 形式の画像データを自らのグラフィックモード（ハイカラー/トゥルーカラー/フルカラー）に適合した精細度の BMP データに再変換して表示することを考慮しなければならない．すなわち，画像データの再変換により暗号化データが壊されることを避けるために，ユーザの使用する PC のグラフィックボードのモードに適合した BMP 形式にて画像データをファイルする．

5.3 画像の拡大・縮小

暗号化データの段階で画像を圧縮・縮小することはできない．しかし，現在の PC では圧縮・縮小などの画像の加工を行うための専用エンジン（ハードウェア）が用意されていることも多く，このエンジンに復号および再暗号化を行うための図 9 と同様のモジュールを付加すれば画像を各種加工することも可能となる．

5.4 識別フラグ

VRAM 上に構築された 1 画面分の画像データの中には，暗号化されている画像コンテンツ（著作物コンテンツ）と暗号化されていない画像コンテンツが混在

する．また，本論文では 4 画素分の GB 成分 64 ビットを 1 ブロックとして暗号化する方式が採用されている．したがって，各画素に「暗号化されている画素か否か」と「（暗号化されている画素の場合は）4 画素中の何番目の画素か」という 2 つの識別情報を与える必要がある．

画像ファイルのデータサイズの肥大化を抑えるためには，これら 2 つの識別情報を電子透かしとして各画素データ 24 ビット中に埋め込んでしまうという方法が考えられる．しかし，透かし情報の挿入によりオリジナルの画素データが変更されることになる．著作物画像を作成する多くの著者は自らの作品が忠実に表現されることを強く望んでおり，本論文では電子透かしによる識別情報の埋め込みは不適切であると判断した．

3.2 節で説明した方法であれば，1 ビットの識別フラグの付加により，上述した 2 つの識別情報を同時に与えることが可能であり，効率的である．この結果，VRAM の 1 画素が 25 ビットとなる．アプリケーションソフトウェアにおいては 1 画素が何ビットであろうともさほど問題とはならないと思われる．しかし，CPU から VRAM に画像データを送るバス幅や VRAM から RAMDAC に画像データを送るバス幅は 24 ビット（またはその倍数）に規定されていることも多い．その場合には 1 画素 25 ビットのデータは転送のスループットが低下するため，これに留意したシステム作りも重要となる．

5.5 鍵の保管

現段階では，暗号を解くための共通鍵はグラフィックボード製造時にメーカが復号機構内のセキュアレジスタ[5]に封印するという前提に立ち，暗号化コンテンツを安全に配信する方法を示した．将来的には，IC カード内に共通鍵を格納し，その共通鍵をユーザが適宜，使用する PC の復号機構にロードするという方式[7]へ改良することによって，より利便性や実用性が高まるだろう．

6. まとめ

本論文では，スクリーンキャプチャやメモリへの直接アクセスによる画像の不正コピーを防止する手段を探った．コンテンツを RAMDAC の直前で復号する動的復号型の表示方式を提案し，RAMDAC の高速動作に追従可能な復号機構を設計した．本方式によれば CPU の管理するいかなる記憶装置上にも著作画像のオリジナルデータは残らず，完全な不正コピーの防止が可能になる．

今後，引続き検討を重ね，動的復号型表示方式により適合した暗号化方式の開発を進める予定である．特に，本方式をオーバレイ表示方式（暗号化画像を別領域で管理しスーパーインポーズする）や DVI CPS と組み合わせることにより，より効率的かつ安全にディジタル画像の不正コピー防止システムを構築できる可能性がある．また，本方式の拡張にともない，これに容易に対応ができるように，本復号機構をプログラマブルデバイスにより実装することも有用であろう．

謝辞 本研究を行うにあたり，貴重なご意見をいただきました，（株）東芝佐野文彦氏，アイ・オー・データ機器（株）城之前伸一氏，吉田仁志氏に感謝いたします．

参考文献

1) DDWG: Digital Visual Interface. http://www.ddwg.org
2) Intel 社: DVI Content Protection System. http://www.intel.com
3) Alchemedia 社：Clever Content Viewer. http://www.alchemedia.com
4) 松井 充：ブロック暗号アルゴリズム MISTY，電子情報通信学会技術研究報告，ISEC96-11, pp.35–47 (1996).
5) 西垣正勝，井熊 徹，曽我正和，田窪昭夫：データのスクラッチングと動的復元によるバイナリープログラムの不正コピー防止方式，電子情報通信学会論文誌 A，Vol.J83, No.11, pp.1288–1299 (2000).
6) （財）新映像産業推進センター開発委員会次世代映像技術研究会：画像の完全可逆圧縮（ロスレス圧縮）方式の研究開発，平成 11 年度日本自転車振興会補助事業報告書 (2000).
7) 井熊 徹，西垣正勝，曽我正和，田窪昭夫：IC カードから CPU への秘密情報の送信，コンピュータセキュリティシンポジウム'99 論文集，pp.49–54 (1999).

(平成 12 年 11 月 28 日受付)
(平成 13 年 6 月 19 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年同大学院博士課程修了．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，現在に至る．博士（工学）．回路シミュレーション，ニューラルネットワーク，情報セキュリティ等に関する研究に従事．

小澤　卓也

平成10年静岡大学工学部情報知識工学科卒業．平成12年同大学大学院修士課程修了．現在，日本システムウェア株式会社ネットワークソリューション事業本部に勤務．在学中，情報セキュリティに関する研究に従事．

曽我　正和（正会員）

昭和33年京都大学工学部電子工学科卒業．昭和35年同大学大学院修士課程電子修了．昭和35年～平成8年三菱電機計算機製作所，情報電子研究所，本社開発本部．平成8年静岡大学情報学部教授，平成11年岩手県立大学ソフトウェア情報学部教授，現在に至る．博士（工学）．汎用計算機，制御用計算機，制御用システムの開発に従事．フォールトトレラントシステム，セキュリティシステムに関する研究に従事．

田窪　昭夫（正会員）

昭和17年生．昭和41年早稲田大学理工学部電気工学科卒業．昭和43年同大学大学院理工学研究科修士課程修了．同年三菱電機株式会社入社，平成10年静岡大学大学院博士後期課程修了．博士（工学）．モバイルコンピューティング，ネットワーク，セキュリティ等に興味を持つ．電気学会，IEEE，ACM各会員．