マルチメディア通信と分散処理　97－2
コンピュータセキュリティ　8－2
（２０００．３．２１）

動的復号型暗号方式による画像コンテンツの不正コピー防止

小澤　卓也†　　西垣　正勝††　　曽我　正和‡　　田窪　昭夫※
†静岡大学大学院理工学研究科　〒432－8011 浜松市城北３－５－１
††静岡大学情報学部情報科学科　〒432－8011 浜松市城北３－５－１
‡岩手県立大学ソフトウェア情報学部　〒020－0173 岩手県滝沢村滝沢字巣子 152－52
※三菱電機情報システム製作所　〒247-8520 鎌倉市上町屋 325
E-mail：nisigaki@cs.inf.shizuoka.ac.jp

あらまし：
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一つとして挙げられるのが、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、本研究では、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、動的復号型暗号方式を提案する。

キーワード：不正コピー防止、画像コンテンツ、スクリーンキャプチャ、動的復号

Copy Protection of Image Data by Dynamic Decryption

Takuya KOZAWA†　　Masakatsu NISHIGAKI††　　Masakazu SOGA‡　　Akio TAKUBO※
†Graduate school of Science and Engineering, Shizuoka University,
††Department of Computer Science, Faculty of Information, Shizuoka University
3-5-1 Johoku, Hamamatsu, 432-8011,Japan,
‡Faculty of Software and Information Science, Iwate Prefectural University,
Sugo 152-52, Takizawa, Iwate, 020-0173, Japan,
※Mitsubishi Electric Corp., 325 Kamimachiya, Kamakura, 247-8520, Japan
E-mail：nisigaki@cs.inf.shizuoka.ac.jp

Abstract：
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 displated. 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.

Keyword：Copy protection, Digital image, Screen capture, Dynamic decryption

第１章　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] が挙げられる。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 Viwer 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可能である。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言える。

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ツの復号をディスプレイ表示の直前に行う、動的復号型暗号方式を提案する。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。

第２章　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 はグラフィックスメモリ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 上にディスプレイ一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）、各画素毎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。

本研究では、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。従ってスクリーンキャプチャによって 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暗号方式と呼ぶこととする。

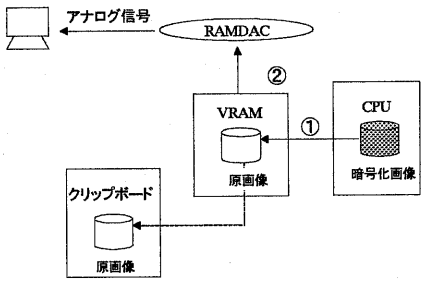

図１：現在の画像表示機構

第３章　動的復号型暗号方式

３．１　画素単位の暗号化

ディスプレイの一画面中に表示される画像データは、コンテンツ同士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が多い。従って、画像コンテンツ全体に対する暗号化や連鎖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。そこで本稿では、著作物画像の暗号化に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、１画素毎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。従って本方式においては、実装の際には、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)。しかし、この結果、一つの暗号化ブロックである４画素の中の１画素でも欠落してしまうと、その暗号化ブロック４画素分の復号結果が誤ることとなる。この対処策においては今後の課題とする。

なお、画素単位の暗号化を採用したため、画像データのファイル形式はビットマップ形式(BMP 形式)を採用せざるを得ない。ただしここで、OS は全ての画像ファイルを DIB 形式とし

て取り扱い、グラフィックボードはこのDIB形式の画像をBMP形式に再変換して表示するということを考慮しなければならない。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は、ファイルのBMP形式を利用者が使用するPCのグラフィックボード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）と同一に用意しておかなければならない。また、同様の理由で、暗号化データを非可逆圧縮することはできない。更に、暗号化データの段階で画像を拡大・縮小することは不可能である。これらに対しては今後の課題としたい。

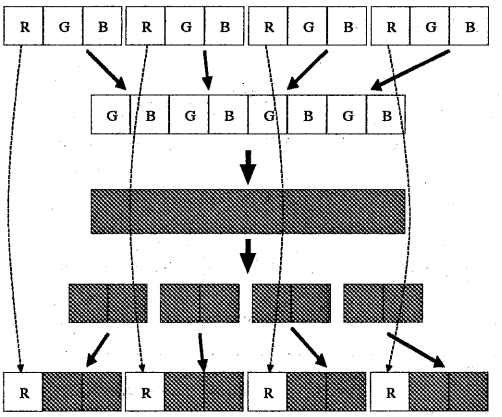

図2：4画素単位による画像の暗号化

3．2 著作物コンテンツの識別

VRAM内で構築された一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。

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、25ビットとすることを提案する。識別フラグに対しては、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画素には「0」がセットされる。また、著作物でない画像コンテンツの識別フラグには全ての画素において「0」がセットされる（図3）。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、画素情報が25ビットになることにより、VRAMのサイズやOSに変更を加える必要が生じる。

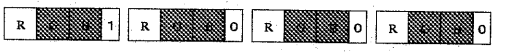

図3：識別フラグを追加した画素情報

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。ここではMISTY2暗号[4]を採用する。そして、復号機構をパイプライン化することで高速化を達成する。

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得るが、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。従って、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。従って本稿では、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。

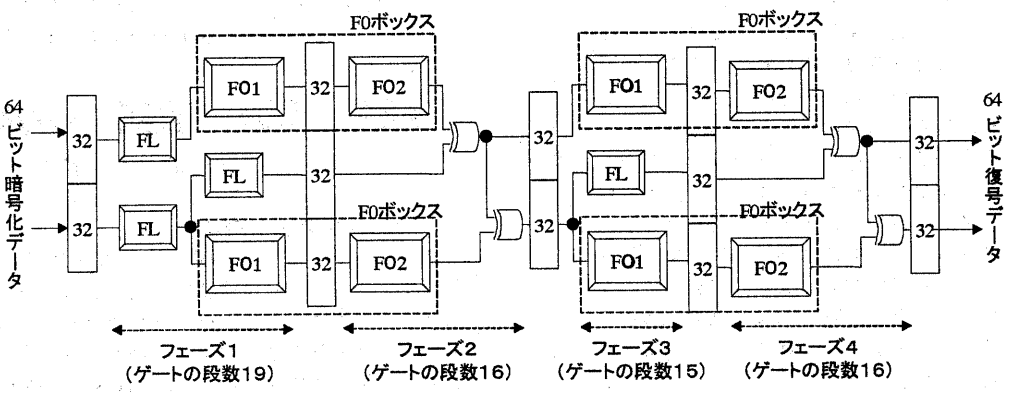

図4：パイプライン型復号機構

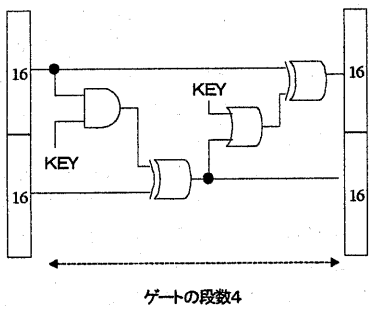

図5：FLボックス

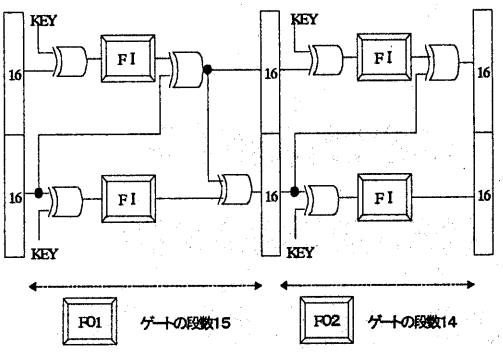

図6：FOボックス

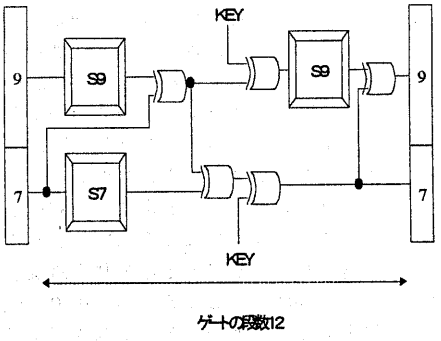

図7：FIボックス

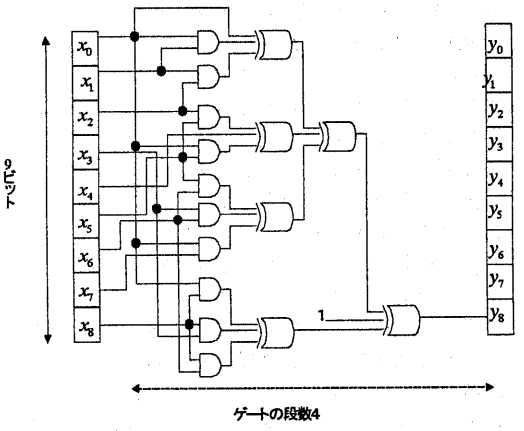

図8：S9ボックス（9ビット目の出力のみ）

第4章 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、復号によるオーバーヘッドがRAMDACのD/A変換の速度を落とすことがあってはならない。1024×768画素の画面を毎秒60フレーム表示する表示機構の場合、RAMDACは1画素分の画素情報のD/A変換をおよそ20ナノ秒で行っていることになる。つ

まり、各暗号化ブロックの復号は 20 ナノ秒以内に終わらせる必要がある。従って、パイプラインの1フェーズがこの条件を満たすような処理速度となるように復号回路を設計する。

4段 MISTY2 暗号化機構（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実装した。文献[4]では安全性と速度バランスを考慮し MISTY2 の暗号化機構を 12 段とすることを推奨している。本稿図 4 の復号機構は文献[2]の図 2 における 4 段分の暗号化機構に対応しているので、図 4 の復号機構を 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。更に、図 6 中の F I 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）。図 4 の復号機構の各フェーズ内に存在するゲートの段数の内、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 ゲート分の遅延時間は遅くとも 0.5 ナノ秒であると考えてよいと思われる。従って、本パイプラインの 1 フェーズの最大処理時間は 9.5 ナノ秒程度となり、先ほど挙げた条件を十分満たす。

4．2 復号機構

図 9 に本方式の復号機構を示す。

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、VRAM から 1 画素分づつ送られる画素情報を順次キュー①～④に積んでいく。4 画素分のデータ GB は各クロックごとに常にパイプラインに送られる。識別フラグ用のキュー②が「1000」の場合に、キュー③、④に格納されている 4 画素分のデータが一つの暗号化ブロックであると識別され、信号 S が「1」にセットされる。S が「1」のときのみ、4 画素分のデータ GB がパイプラインに送られた時点で、キュー③、④内のデータはキューから削除される（リセットされる）。一方で、信号 S、データ R,G,B は、キューを経由した後、1 画素づつ無条件に同期機構 α,β,γ に送られる。ここで、データ GB が暗号化データの場合には、同期機構 α には 4 画素分の 0 データが送られることに注意する。（0 データを送る必要性については 4．2．3 節で述べる。）

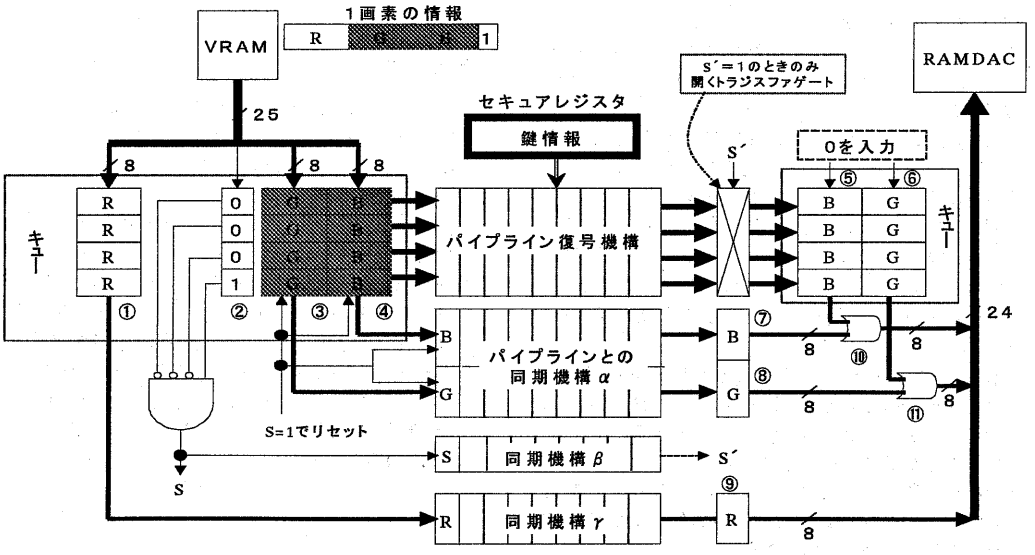

図 9：復号機構

4．2．2 パイプラインとの同期

本方式では色情報RGBのうち、データGBのみが暗号化されている。そのため、パイプラインを通過してきた復号データGBを対応するデータRと正しく結合させるには、データRの転送速度をデータGBがパイプラインを通過する速度と同じにしなければならない。そこで、パイプラインの処理速度と同期をとる機構α,β,γを用意し、ここを通過させることで、各データの同期を図る。また、暗号化されていないデータGBに対してもこの機構を通過させることで、暗号化されているデータGBと暗号化されていないデータGBの転送速度を一致させている。更に、識別信号Sに対してもこの機構を通過させる（その理由については4.2.3節で述べる)。パイプライン処理の実行にかかる全フェーズ数をN（図4～8のパイプラインではN=12）とした場合、同期機構α,β,γはN段のキュー（シフトレジスタ）により実装される。

4．2．3 画素情報の統合

まず、同期機構αから出力されるデータGBとパイプラインから出力されるデータGBの統合を考える。同期機構γの働きにより、信号SがS´に伝わった時点で、パイプラインにおけるデータGBの復号が完了したことが分かる。パイプラインからの出力は信号S´が「1」の場合のときのみキュー⑤、⑥に格納される。ここで、キュー⑤、⑥においては、信号S´が「0」の場合には常に0データが積まれるようになっている。すなわち、キュー⑤、⑥からは、著作物画像の復号データのみが順次その後段のOR回路⑩、⑪に送られ、それ以外の時には0が送られる。反対に、4.2.1節で示したように、同期機構αからレジスタ⑦、⑧を通じてOR回路⑩、⑪に送られるデータGBは、著作物画像である場合には0となる。従って、OR回路⑩、⑪によってパイプラインからのデータGBと同期機構αからのデータGBを統合することができる。

次に、これをデータRと結合する必要があるが、同期機構βの働きにより、データGBの統合が完了する時点で対応するデータRがレジスタ⑨に格納されることが分かる。よって、OR回路⑩、⑪の出力とレジスタ⑨からの出力をそのままRAMDACに送ってやれば、RGB全てのデータがそろうことになる。

第5章 まとめ

本研究ではスクリーンキャプチャや機械語レベルによるメモリへの直接アクセスといった高度なクラッキングによる画像の不正コピーを防止する手段を探った。

本方式ではECBモードにより暗号化を行っているため、暗号強度が高いとは言えない。しかしCBCモードのようにブロック間の暗号化に連鎖関係を与えると、1つの画素が欠けただけで全体の復号が行えなくなるという問題が発生してしまう。

本方式の発展形としてオーバーレイ表示方式を応用する方式や、冒頭に紹介したDVI CPSと本方式を組み合わせることで安全にVRAMからディスプレイへデータを転送する方式が考えられる。

本方式においては、ハードウェアやOSレベルでのシステム変更が必要となる。しかし、セキュリティ問題はネットワーク社会の発展に大きく関わる。ゆえに従来のシステムにとらわれず、セキュリティ指向のOSやハードウェア基盤の構築、そしてその基盤を活かしたシステムの設計が望まれるのではないだろうか。

謝辞

本研究を行うにあたり、貴重な御意見を頂きました、(株)東芝 佐野文彦氏、アイ・オー・データ機器（株）城之前伸一氏、吉田仁志氏に感謝致します。

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, 信学技報、ISEC96-11、PP.35-47(1996-07).

[5]井熊徹、曽我正和、西垣正勝、田窪昭夫：データの汚染と動的復元による実行形式プログラムの不正コピー防止方式,1999年暗号と情報セキュリティシンポジウム、PP.445-450 (1999-1).