2006－CG－125 (1)
2006／11／16

統計的解析に対して防御可能なLSBステガノグラフィ

杉原 佳次

京都大学大学院人間・環境学研究科

画像の最下位ビット (LSB) を用いたステガノグラフィは数多く存在している．一方，その埋め込みデータを検出する様々な手法も提案されており，特に有用とされているのは画像の統計的性質に注目して解析を行う手法である．本研究ではこれらの手法で埋め込みデータが検出されないようにする LSB ステガノグラフィの手法を提案する．埋め込みデータの検出を防ぐために，対象とする解析で用いられる統計量を埋め込み後に補正する．本手法ではグレイコードの性質を利用することで，画素値の変化を高々1に抑えながら既存の手法とは異なる形でデータを埋め込む．この方法により，データを埋め込んだ画素の約半数を統計量の補正に用いることができる．本研究では，3つの統計的解析を用いて検出できないように画像全体にデータを埋め込むことができることを示した．

An LSB Steganography Robust to Statistical Steganalyses

Sugihara Keiji

Graduate School of Human and Environmental Studies, Kyoto University

Many steganography techniques using least significant bits(LSB) for images have been presented for hiding secret information. At the same time, various steganalysis techniques for finding or analysing embedded data are proposed and statistical steganalyses are widely known as useful ones. This study presents a new LSB steganography method robust to them. In the method, statistical measures used in steganalyses are adjusted after embedding data. This method is based on the characteristics of graycode. Data are embedded in a different way from existing ones, which makes the change of each pixel value at most one. About half of the pixels where data are embedded can be used for adjustment of the measures. It was shown that the proposed method is robust to three major steganalyses even when data are embedded fully into images.

1. はじめに

ステガノグラフィとは，他人に気づかれない形でデジタルコンテンツに秘密情報を埋め込んで保存したり，特定の相手に伝える技術のことである．通信を行っていることがわかっても鍵を持たない第三者には解読できないようにするのが目的の暗号化とは異なり，ステガノグラフィの目的は通信の存在そのものを隠すことである．情報を埋め込むコンテンツとしては，画像や音声など冗長性の多いものがよく用いられている．

その中で静止画像に対するステガノグラフィについては，データ埋め込みによる視覚的変化をできるだけ小さく抑える必要がある．よく用いられる手法の1つとして，画素値やパレット画像のインデックスなどの値を表すビット列の LSB(Least Significant Bits) に対してデータを埋め込む LSB ステガノグラフィがある．

LSB ステガノグラフィの手法とともに，埋め込まれたデータの検出を行う手法も考案されている [1]．その中で有用とされているのが統計的性質に注目した解析手法である．これは，データ埋め込みによって変化する画像の統計的性質に注目し，それを表す統計量の解析によって埋め込みデータの存在やその長さを判定するというものである．例えば，RS Steganalysis[2] ではデータの埋め込みによって LSB がノイズ状に変化する様子を式で表して解析を行っている．他にも Sample Pair Analysis[3] や HCF を用いた解析 [4] などの手法が知られている．これらの手法で検出可能な埋め込みはステガノグラフィの目的を果たせていないといえる．

そこで，本研究ではこのような統計的解析によって埋め込みデータが検出されないようにする LSB ステガノグラフィの手法を提案する．本手法では，各解析手法で注目している統計的性質がデータの埋め込み前後で変化しなければ，その手法によってデータが検出されることがないことを利用する．各手法で用いられる統計量が埋め込み前後で変化しないようにデータの埋め込み後に統計量を補正することによって，その手

法に対する防御が可能となる．この補正は画素値の変更によって行うため，データを埋め込む際に画素値を調整する余地を残しておく必要がある．

本手法ではこの埋め込み方法を実現するために，計算機による実数計算 [5] などに用いられているグレイコードを利用する．グレイコードでは，差が1である2つの整数を表すコードは1ビットしか異ならない．グレイコードの性質を用いた処理によって，画素値の変化を高々1に抑えながら既存の手法とは異なる形でデータを埋め込んで，データを埋め込んだ画素の約半数について画素値を調整することができるようになる．そこで，それらの画素を用いて各手法で用いられる統計量を埋め込み前後で変化しないように補正することができる．本研究では，この手法が前述の3つの解析手法，およびそれらの解析を同時に対象とした防御が可能であることを実験により示した．

2. LSBステガノグラフィとその統計的解析

LSBステガノグラフィとは，画素値やパレット画像のインデックスなどの値のLSBに対してデータを埋め込む手法のことである．この手法はデータの埋め込み方法によって大きく2つに分類される．1つは画像のLSBを埋め込みデータのビット列で置き換えていく手法で，LSB replacementと呼ばれる．もう1つは画像のLSBが埋め込みデータのビット列と一致するように画素値を変化させる手法で，LSB matchingと呼ばれる．これらの手法においては，埋め込みによる画素値の変化は高々1であり，埋め込み後のLSBがデータのビット列と一致する．ただLSB matchingについては，画素値の変化によってLSB以外のビットが変化することもある．実際LSBステガノグラフィの重要な性質は，埋め込みによる値の変化がほとんどないことである．そこで，本報告では画素値の変化が高々1であるようにデータを埋め込む手法をLSBステガノグラフィと呼ぶこととする．

LSBステガノグラフィの手法とともに，埋め込まれたデータの検出やその長さの解析を行う手法も数多く考案されている．その中でも特に有用とされているのが統計的解析による手法である．本研究ではこのうち，LSB replacementに対する解析であるRS Steganalysis と Sample Pair Analysis，およびLSB matchingに対する解析として利用できるHCFを用いた解析を防御の対象として実験を行った．本節ではこれらの解析手法について概説する．

2.1. RS Steganalysis

本節では，RS Steganalysis（以下，RS）[2] と呼ばれるLSB replacementに対する統計的解析の手法について述べる．

まず初めに，画像全体を n 個ずつの画素の組に分ける．本研究では $n = 4$ として隣接画素の組を利用している．ある組 $G = (x_1, \cdots, x_n)$ について，

$$f(x_1, \cdots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|$$

と定義する．この関数 f は G がノイズに近い領域であるほど大きな値を取るように定義されている．

次に，flipping F を以下のように定義する．

$$\begin{aligned} F_1(x) &= \begin{cases} x+1 & x \text{ が偶数} \\ x-1 & x \text{ が奇数} \end{cases} \\ F_{-1}(x) &= F_1(x+1) - 1 \ \text{ for } \forall x \\ F_0(x) &= x \ \text{ for } \forall x \end{aligned}$$

これと $\{-1, 0, 1\}$ の n 個組からなるマスク $M = \{M(1), \cdots, M(n)\}$ を用いて定義される $F(G) = (F_{M(1)}(x_1), \cdots, F_{M(n)}(x_n))$ によってLSBへのノイズの付加による画素値の変化を表すことができる．なお，本研究では $M = \{0, 1, 1, 0\}$ を用いている．

ここで，これらの flipping F と関数 f を用いて，G を次の3つのグループのいずれかに分類する．

$$\begin{aligned} &\text{Regular groups:} && G \in R \Leftrightarrow f(F(G)) > f(G) \\ &\text{Singular groups:} && G \in S \Leftrightarrow f(F(G)) < f(G) \\ &\text{Unusable groups:} && G \in U \Leftrightarrow f(F(G)) = f(G) \end{aligned}$$

あるマスク M について，$G \in R$ となる G の（全集合数に対する）割合を R_M，$G \in S$ となる G の割合を S_M とする．このとき，一般的な画像については

$$R_M \cong R_{-M} \text{ かつ } S_M \cong S_{-M} \qquad (1)$$

が成り立つ．ところが，LSBへデータを埋め込むと R_M と S_M との差は小さくなり，全画素にデータを埋め込んだ場合に $R_M \cong S_M$ となる．それに対して，R_{-M} と S_{-M} との差はデータが長くなるにつれて大きくなることが知られている（図1）．

この性質を利用して，データの長さを推定する．画像全体のLSBに対する埋め込まれたデータの割合（以

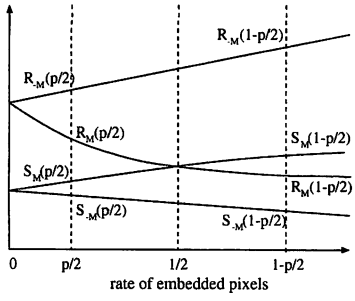

図 1: RS Steganalysis のダイアグラム

下，埋め込み率と呼ぶ）を p とする．このとき，データのビット列がランダムであれば埋め込み時に反転される画素の割合は $p/2$ と考えられるため，$R_M(p/2)$, $S_M(p/2)$, $R_{-M}(p/2)$, $S_{-M}(p/2)$ が求められる．また，埋め込み後の画像の全画素の LSB を反転させれば $R_M(1-p/2)$, $S_M(1-p/2)$, $R_{-M}(1-p/2)$, $S_{-M}(1-p/2)$ が求められる．これらの値と (1) より構成できる図 1 のようなダイアグラムから p の推定値を求めることができる．

2.2. Sample Pair Analysis

本節では，Sample Pair Analysis(以下，SPA)[3] と呼ばれる LSB replacement に対する統計的解析の手法について述べる．

まず，画素の組 (u,v) の集合 D_n, C_n を次のように定義する．なお本研究では，水平，垂直方向に隣接する全ての画素の組を用いることとしている．

$$\begin{aligned} D_n &= \{(u,v)|\ |u-v|=n\} \\ C_n &= \{(u,v)|\ |\lceil u/2\rceil - \lceil v/2\rceil|=n\} \end{aligned}$$

すると，D_{2m} は必ず C_m に含まれるのに対し，D_{2m+1} は C_m に含まれる部分と C_{m+1} に含まれる部分に分割できる．そこで，X_n, Y_n を $X_{2m+1} = D_{2m+1} \cap C_{m+1}$, $Y_{2m+1} = D_{2m+1} \cap C_m$ を満たす D_n の部分集合とする．このとき，

$$\forall m,\ |X_{2m+1}| \cong |Y_{2m+1}| \tag{2}$$

と考えられる．また，C_m は $X_{2m-1}, X_{2m}, Y_{2m}, Y_{2m+1}$ の 4 つの部分集合に分割することができる．

次に，これらの部分集合の濃度がデータの埋め込みによってどのように変化するかを考える．ある組

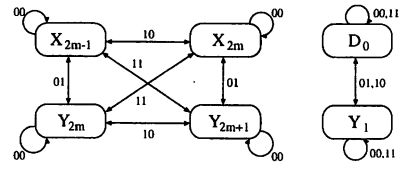

図 2: C_m についてのオートマトン

(u,v) について，埋め込みによって画素値に起こる変化は次の 4 通りである．

00) u も v も変化しない　01) v のみが変化する
10) u のみが変化する　11) u も v も変化する

C_m の部分集合について，これらの変化をモデル化したものが図 2 である．なお，定義より C_m の要素が埋め込みによって変化することはない．

データの埋め込み率を p とし，データのビット列がランダムであるとすると，画素値が変化する確率は $p/2$ と考えられる．よって，(2) と図 2 から p の推定値を求めることができる．

ここで，さらに正確な値を求めるには，ある集合 C_m に関するオートマトンを考えるよりもある範囲の m について結合させた集合 $\bigcup_{m=i}^{j} C_m$ を用いたほうがよい．なぜなら，

$$|\bigcup_{m=i}^{j} X_{2m+1}| \cong |\bigcup_{m=i}^{j} Y_{2m+1}| \tag{3}$$

という条件のほうが，(2) よりも弱い仮定になっているからである．このとき，i と j との差は大きいほうがよいため，本研究では $i=0, j=30$ としている．

2.3. HCF を用いた解析手法

本節では，LSB matching に対する統計的解析として利用できる Histogram Characteristic Function（以下，HCF）[4] を用いた解析手法について述べる．

まず原画像の画素値のヒストグラムを $h_c[n]$（n は画素値），埋め込み後の画素値のヒストグラムを $h_s[n]$ とする．また，データ埋め込みによって付加されるノイズの分布を表す確率関数を $f_\triangle[n] \equiv p(x_s - x_c = n)$ とする．ただし，x_c は埋め込み前の画素値，x_s は埋め込み後の画素値である．このとき，埋め込みの際に付加されるノイズが原画像と独立ならば以下の式が成り立つ．

$$h_s[n] = h_c[n] * f_\triangle[n]$$

ただし $*$ は畳み込み演算を表す．

ここで，これらの関数の離散フーリエ変換 (DFT) を考える．N を画素値集合の濃度（8 ビット濃淡画像なら $N = 256$）とするとき，

$$X[k] = DFT(x[n]) = \sum_{n=0}^{N-1} x[n] e^{-\frac{2\pi jnk}{N}}$$

と表すことにし，$f_\triangle(n), h_c(n), h_s(n)$ に対応する DFT をそれぞれ $F_\triangle[k]$, $H_c[k]$, $H_s[k]$ で表す．ヒストグラムの DFT のことを特に HCF と呼ぶ．すると，これらについて，

$$H_s[k] = F_\triangle[k] H_c[k]$$

が成り立つ．

ここで，HCF 上のエネルギー分布の測度として COM(Center of Mass) を導入し，埋め込みデータの有無の解析に用いる．COM は以下の式で表される．

$$C(H[k]) \equiv \frac{\sum_{k \in \mathcal{K}} k|H[k]|}{\sum_{i \in \mathcal{K}} |H[i]|}$$

ただし，$\mathcal{K} = \{0, \ldots, \frac{N}{2} - 1\}$ である．$\mathcal{K}$ をこのように定めるのは，DFT の後半の項が冗長であり解析には不要だからである．この HCF COM について，$k = (0, \ldots, \frac{N}{2} - 1)$ に対して $|F_\triangle[k]|$ が非増加である場合，

$$C(H_s[k]) \leq C(H_c[k])$$

が成り立つ．なお，一般的な LSB matching においては，$|F_\triangle[k]|$ は k について単調減少になる．

この性質を利用して，埋め込みデータの有無を判定する．その際には，データ埋め込みのない訓練用画像群の HCF COM と解析対象の画像の HCF COM を比較し，同じ群に含まれるかどうかを判定する．

3. 統計的解析に対して防御可能なデータ埋め込み

本節では，前節で述べたような統計的解析によって埋め込みデータが検出されないようにする LSB ステガノグラフィの手法について述べる．データが検出されないようにするために，対象とする解析で用いられる統計量が埋め込み前後で変化しないようにデータを埋め込んだ後に統計量の補正を行う．そこで，データを埋め込む際に画素値を調整する余地を残すようにする．本手法ではグレイコードの性質を用いた処理によってデータを埋め込む．これによって，データを埋め込んだ画素の約半数において画素値を調整することができる．以下，本手法で注目したグレイコードの性質ならびに具体的な処理の手順について述べる．

v	graycode	M_v	v	graycode	M_v
0	0 0 0 0	−	5	0 1 $\boxed{1}$ 1	2
1	0 0 $\boxed{0}$ 1	0	6	0 1 $\boxed{0}$ 1	1
2	0 0 $\boxed{1}$ 1	1	7	$\boxed{0}$ 1 0 0	0
3	0 $\boxed{0}$ 1 0	0	8	$\boxed{1}$ 1 0 0	1
4	0 $\boxed{1}$ 1 0	1	9	1 1 $\boxed{0}$ 1	2

図 3: グレイコード

3.1. グレイコードとその性質

グレイコードとは，差が 1 である 2 つの整数を表すコードが 1 ビットしか異ならないようなコードのことである．図 3 は 4 ビットで表現できる整数の一部を示している．

グレイコードでは，ある値 v を表すコードについて，その中で反転させたときに値が 1 しか変わらないビットが LSB 以外にもう 1 つ存在する（図 3 の四角で囲んだビットがこれにあたる）．v に関してこのビットは最上位ビットから数えて N_v 番目であるとする．このとき，v を表すコードの $N_v + 1$ 番目のビット以降は必ず $100\cdots$ となっている．

ここで，v を表すコードのうち N_v 番目のビットまでに含まれるビット 1 の数を M_v とすると，M_v は（コード全体に含まれているビット 1 の数）-1 である．v が 1 だけ変化するとき，v を表すコードのうち必ず 1 つだけビットの 0/1 が入れ替わるため，M_v の偶奇も v を 1 変化させるごとに入れ替わる．

3.2. データ埋め込みの手順

前節で述べたグレイコードの性質を用いて，画素値の変化を高々1 に抑えながら統計量を補正できる形でデータを埋め込む手順について述べる．

今，原画像の画素値 v について M_v の偶奇が埋め込みビット b の 0/1 と一致するようにデータを埋め込むと，埋め込み後の画素値 v' は

$$v' = \begin{cases} v & (M_v \text{の偶奇}) = b \\ v+1 \text{ or } v-1 & (M_v \text{の偶奇}) \neq b \end{cases}$$

	v	LSB	v'	
			$b=0$	$b=1$
1.	奇数	0	v or $v-1$	$v+1$
2.	偶数	0	$v-1$	v or $v+1$
3.	奇数	1	$v+1$	v or $v-1$
4.	偶数	1	v or $v+1$	$v-1$

表 1: 埋め込み後の画素値

となる．この変化は LSB matching と同じであるため，LSB matching に対する解析で用いられる統計量の補正が難しくなる．

そこで，本手法では全ての画素値を表すコードの LSB を 0 にした際の M_v の偶奇が埋め込みビットの 0/1 と一致するようにデータを埋め込む．こうすることで，埋め込みによる画素値の変化が LSB replacement とも LSB matching とも異なる形になる．具体的な処理手順は次の通りである．

まず，原画像の各画素を画素値 v の偶奇と v を表すコードの LSB の値によって 4 つに分類する．そして，v' を b の 0/1 に応じて表 1 のように決定する．

例えば 4 ビットのグレイコードの場合，画素値 $v=5$（コードは 0111）については，v が奇数で LSB=1 であるから，$b=0$ なら $v'=6$（コードは 0101）に，$b=1$ なら $v'=5$（コードは 0111）または 4（コードは 0110）にする．

データを取り出す際には，v' を表すコードの LSB を 0 にした値 v'' について $M_{v''}$ を計算し，その偶奇から b を決定する．

先ほどの例の場合，v' のコードの LSB を 0 にすれば，v' が 4 または 5 の場合は $v''=4$（コードは 0110）に，v' が 6 の場合には $v''=7$（コードは 0100）になる．$M_4=1, M_7=0$ であることから，$v'=4,5$ なら $b=1$，$v'=6$ なら $b=0$ と決定できる．

この例のように，v' が 2 通りある場合でもそこから得られる v'' は同じ値になる．また，b の値と $M_{v''}$ の偶奇が一致するように v' を決定していることから，この処理によって正しくデータを取り出すことができることがわかる．

この手法でデータを埋め込むと，全ての場合について $b=0$ または 1 のどちらかの場合に埋め込み後の画素値として利用できる値が 2 通り存在する．このような画素を変更可能画素と呼ぶ．埋め込みデータのビット列がランダムであるとすると，データを埋め込む画素の約半数が変更可能画素であると考えられる．これらの画素を用いて，データ埋め込みによる統計量を補正する．なお，埋め込みに用いない画素も補正に利用できるため，変更可能画素に加えておく．

補正の処理としては，各手法で用いられる統計量に関して，自然画像において成り立つとされている性質が保たれるように変更可能画素の画素値を変更する．この性質として RS であれば式 (1)，SPA であれば式 (3) が挙げられる．HCF を用いた解析については後述する．これらの解析手法を自然画像に適用した場合，データ埋め込み率の推定値 $\hat{p}$ はほぼゼロになる．よって，補正の処理を施すことでこの推定値の絶対値を小さく抑えることができる．なお，補正の閾値は $\hat{p}$ をもとに決定する．

なお，HCF を用いた解析の検出結果は訓練用画像の性質などに依存するため，全ての埋め込みデータが検出されないようにするのは極めて難しい．ただ，埋め込み前後の HCF COM の差がなくなれば，同一画像に関して埋め込みの有無によらず検出結果が同じになり，この場合には本手法による埋め込みを正しく検出できないと見なすことができる．そこで，HCF COM の値が埋め込み前の画像の値に近づくように補正を行うこととする．

4. 実験と評価

本節では，防御の対象とした 3 つの解析手法で用いられる統計量の補正の実験とその評価について述べる．さて本手法においては，データ埋め込みならびに統計量の補正のために画素値 v を v' に変更する際にデータを埋め込んだ変更可能画素の扱い方として次の 2 通りの方針が考えられる．

方針 1. データを埋め込む際には $v' \neq v$ である v' にしておき，補正時に必要に応じて $v'=v$ にする

方針 2. データを埋め込む際には $v'=v$ にしておき，補正時に必要に応じて $v' \neq v$ である v' にする

ここでは，それぞれの方針で実験を行った．

データ埋め込みの対象とする画像としては，Kodak PhotoCD PCD0992[6] で提供されている PNG 形式のカラー画像 24 枚（サイズ 768×512）と USDA NRCS Photo Gallery[7] で提供されている JPEG 形式のカラー画像 40 枚（サイズ 2100×1500）の計 64 枚の画

手法	方針	補正前		補正後	
		平均	最大	平均	最大
RS	方針 1	3.24	21.68	0.03	0.08
	方針 2	105.39	115.39	0.03	0.07
SPA	方針 1	2.62	13.32	0.20	0.97
	方針 2	109.46	124.11	0.08	0.21
HCF	方針 1	15.77	41.14	0.73	0.99
	方針 2	23.48	57.13	0.76	1.00

表 2: 実験結果（数値は %）

像を BMP 形式の 8 ビット濃淡画像（サイズ 768×512）に変換したものを用いた．

統計量の補正の閾値としては，RS および SPA については埋め込み率の推定値の絶対値を 1% とした．また HCF については，HCF COM の原画像との誤差の閾値を 1% とした．以下に実験の結果と評価を述べる．

方針 1，2 による比較

3 つの解析手法それぞれを防御の対象とし，埋め込み率 100% で実験を行った．表 2 は，RS および SPA によるデータ埋め込み率の推定値の絶対値 (%) と HCF COM の原画像との誤差 (%) の補正による変化を示している．これからわかるように，方針 1，方針 2 ともに，全ての画像について各統計量を閾値以内に補正することができた．ただし，方針 2 のほうが補正前の値が大きいため方針 1 に比べて処理に時間がかかる場合が多かった．これは方針 2 の補正前の画素値の変化が LSB replacement と同じ形であるためと考えられる．

3 つの手法を同時に対象にした場合

3 つの解析手法を同時に防御の対象とする実験を方針 1，方針 2 のそれぞれの手法について埋め込み率 100% で行った．統計量の補正の際には，全ての統計量が同時に閾値を下回るまで HCF，RS，SPA の順に補正の処理を行った．また，ある統計量の補正には他の統計量の補正に用いていない画素をできるだけ用いるようにした．

この場合でも 64 枚全ての画像について各手法の統計量を補正することができた．このことから，ある統計量の補正による画素値の変化は他の 2 つの統計量に影響を及ぼすが，この影響は処理を繰り返すごとに小さくなったと考えられる．

5. まとめと今後の課題

本研究では，統計的解析によって埋め込みデータが検出されないようにする LSB ステガノグラフィの手法を提案した．本手法ではグレイコードの性質を用いて，画素値の変化を高々1 に抑えながら既存の手法とは異なる形でデータを埋め込む．この処理によって，防御対象とする解析で用いられる統計量を埋め込み後に補正することができる．実際，RS，SPA ならびに HCF を用いた解析によって検出されないようにデータを埋め込むことができることを示した．

今後は他の解析に対する防御をさらに組み合わせることが考えられる．また，埋め込み後の LSB はデータ読み取りには利用しないため，その部分を補正に用いずに別のデータを埋め込むなどの応用も考えられる．

参考文献

[1] J.Fridrich and M.Goljan : Practical Steganalysis of Digital Images - States of the Art, in *Proc. SPIE Security Watermarking Multimedia Contents*, E.J.Delp III and P.W.Wong eds., Vol. 4675, pp. 1-13, (2002).

[2] J.Fridrich and M.Goljan and R.Du : Detecting LSB steganography in color and grayscale images, *IEEE Multimedia*, Vol. 8, No. 4, pp.22-28 (2001).

[3] S.Dumitrescu and X.Wu and Z.Wang : Detection of LSB Steganography via Sample Pair Analysis, *IEEE Transactions on Signal Processing*, Vol. 51, No. 7, pp. 1995-2007 (2003).

[4] J.J.Harmsen and W.A.Pearlman : Steganalysis of additive noise modelable information hiding, *Proc. SPIE Security Watermarking Multimedia Contents*, E.J.Delp III and P.W.Wong eds., Vol. 5020, pp. 131-142 (2003).

[5] H.Tsuiki : Real number computation with committed choice logic programming languages, *Journal of Logic and Algebraic Programming*, Vol. 64, pp.61-84 (2005).

[6] http://www.r0k.us/graphics/kodak .

[7] http://photogallery.nrcs.usda.gov .