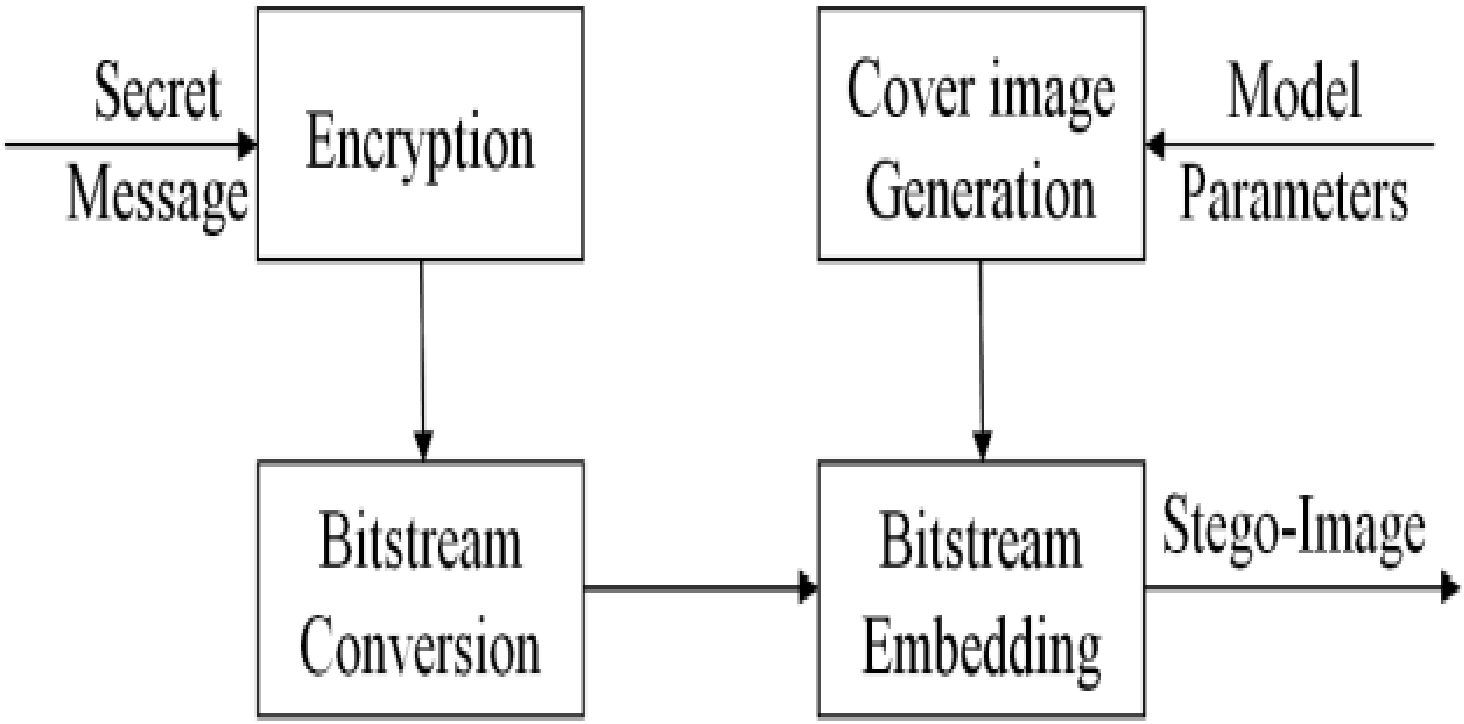
High-Capacity Steganography Using MRF-Synthesized Images

Chaur-Chin Chen[1,2] and Wei-Ju Lai[1]
Department of Computer Science[1]
Institute of Information Systems & Applications[2]
National Tsing Hua University, Hsinchu,Taiwan 30013
E-mail: cchen@cs.nthu.edu.tw

ABSTRACT

Steganography *refers to embedding information or secret message into media.* This paper presents a simple and secure high-capacity steganographic algorithm for information hiding. We synthesize a cover-image texture with four gray levels *32, 96, 160, and 224* of user-selected size based on a Markov Random Field (MRF) model. On the other hand, each byte of the secret information (secret message, image, etc.) is first encrypted based on an exponential modular arithmetic which is then partitioned into two 4-bit words. Each 4-bit word in [0,15] is inserted into the last four bits of a pixel in the selected *cover-image* to form a *stego-image*. The embedding capacity for an m by n cover-image could be as high as $(m \times n)/2$.

A Flowchart of Proposed Steganography



Algorithm (GIM) for Cover Image Generation

(1) For s=1 to MN, randomly assign a $g \in A$ for x_s to give an initial image x.

(2) For s=1 to MN Do

(a) Let $y_t = x_t$ for all $t \neq s$. Choose $g \in A$ at random and let $y_s = g$.

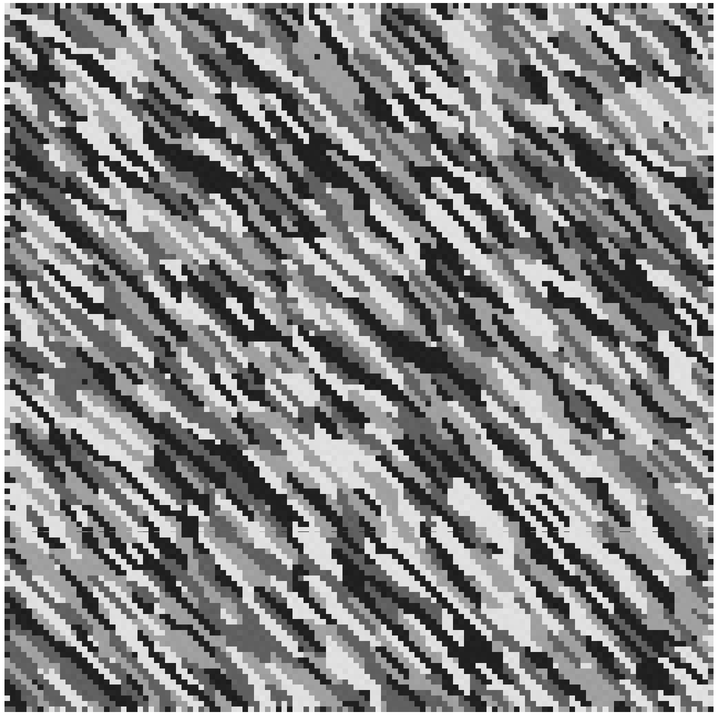
(b) Let $r = min\{1, P(y)/P(x)\}$, where P is as defined in eq. (1).

(c) $x \longleftarrow y$ with probability r.

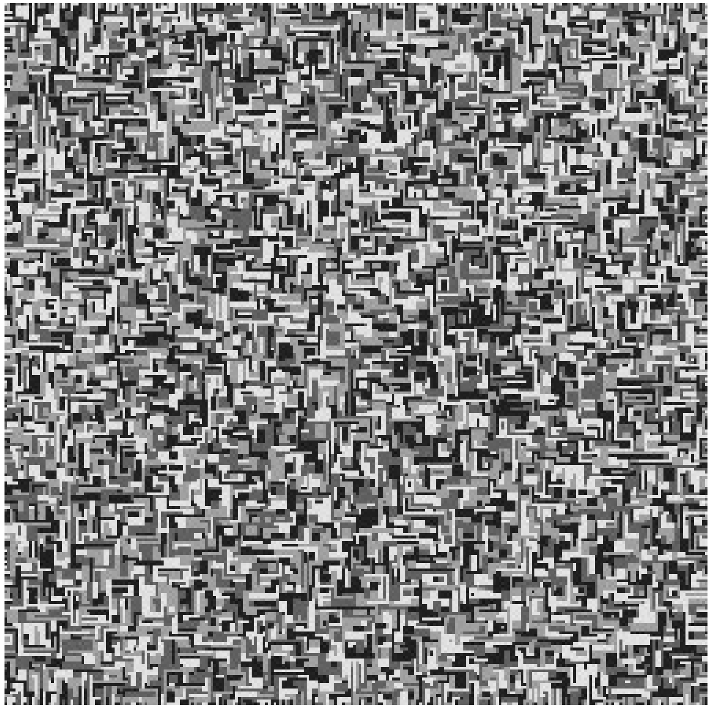
(3) Repeat step (2) until "*convergence*," is achieved, for example, in 50 iterations.

Cover Images Generated by Markov Random Model

θ=(1,1,1-1)



θ=(2,2,-1,-1)



Message Converted into Bitstream (1/3)

- Suppose a secret message ‘hide’ is to be embedded into a cover image consisted of pixels Pixel(1), Pixel(2), ….,Pixel(K). Each Pixel(j) has one of the values

$32 = 00100000_2$, $96 = 01100000_2$,

$160 = 10100000_2$, $224 = 11000000_2$

For example,

Pixel(1)=96, Pixel(2)=32, Pixel(3)=160, etc.

Message Converted into Bitstream (2/3)

1. h,i,d,e = 104,105,100,101 in ASCII code
2. A permutation is done on {0,1,2,…255} by $y+1=g^{x+1}$ mod p=257, so that x could be transformed into y, and vice versa.
3. Take g=83, then (104,105,100,101) will be transformed into (159,172,217,103)
4. 159=10011111_2 is splitted as 1001 & 1111

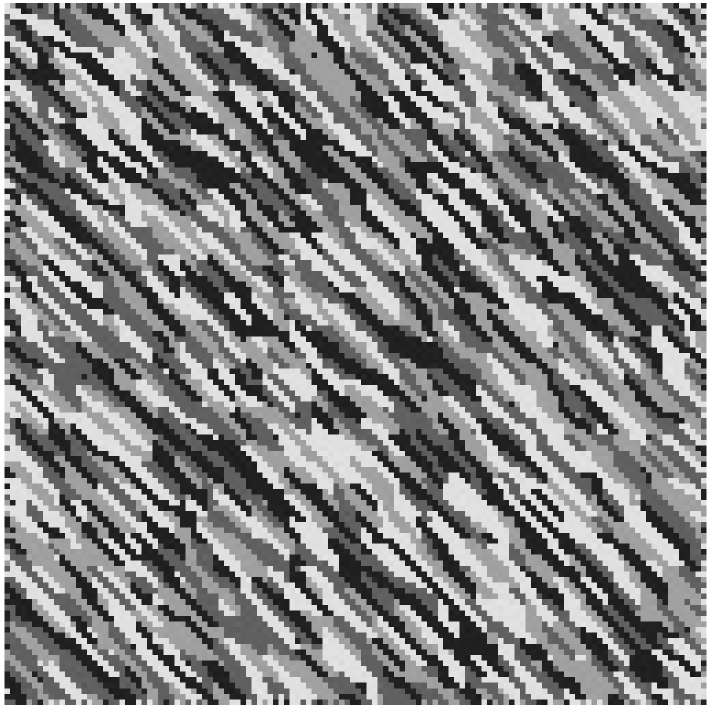
Message Converted into Bitstream (3/3)

1. The ASCII code for h is 104 which is converted to 159=10011111 and is further processed as 1001 and 1111
2. Q(1)=Pixel(1)+00001001
3. Q(2)=Pixel(2)+00001111

The procedures continued until all of the message stored as a character sequence have been embedded into the cover image.

The Experiment

A 128x128 Cover Image



A Secret Message

Steve Jobs to 2005 graduates : 'Stay hungry, stay foolish'

Drawing from some of the most pivotal points in his life, Steve Jobs, chief executive officer and co-founder of Apple Computer and of Pixar Animation Studios, urged graduates to pursue their dreams and see the opportunities in life's setbacks—including death itself—at the university's 114th Commencement on Sunday in Stanford Stadium.

………….

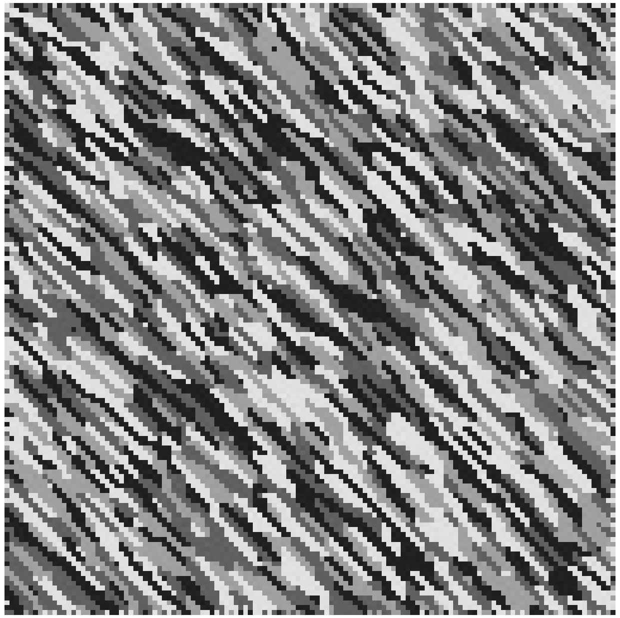
"I'm pretty sure none of this would have happened if I hadn't been fired from Apple," Jobs said. "I'm convinced that the only thing that kept me going was that I loved what I did."

………….

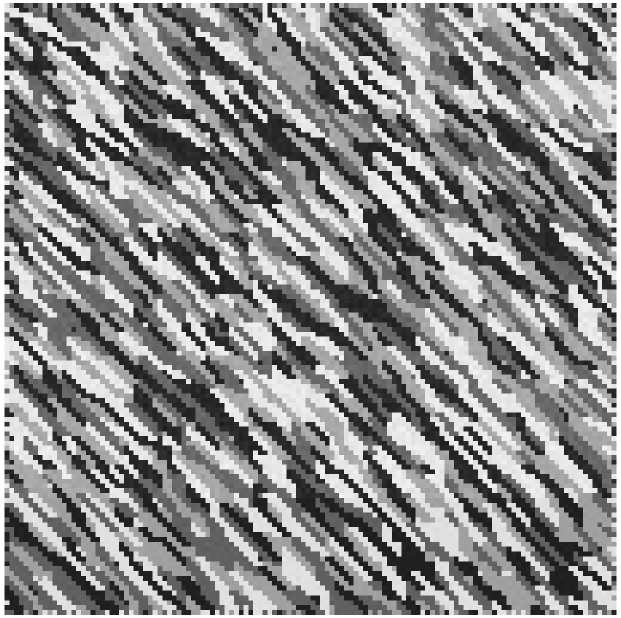
"I just think it's a remarkable accomplishment to get through this school," she said. "Just the challenge of being here."

A Cover Image and Stego Image

A 128x128 Cover Image



The Stego Image



Conclusion and Discussion (1/2)

(1)JPEG Images As Cover Images

A cover image of JPEG *available everywhere nowadays* is based on Discrete Cosine Transform (DCT) by ignoring the quantized 0 and 1 coefficients which occupy major percentage of an image and thus *shorten the embedding capacity.*

Conclusion and Discussion (2/2)

(2) MRF-Synthesized Cover Images

We propose using a synthesized cover image based on Markov Random Model which can generate a cover image to meet the requirement of message size. *This cover image provides high-capacity embedding rate. The available embedded capacity in our scheme is (mxn)/2 characters with user selected (m,n) for image (#rows, #columns)*

Textures Generated by Markov Random Field Models

Using Markov random fields (Mrf) to synthesize textures is a challenging task. We will review Mrf and give algorithms for synthesizing textures.

1 Background of the Markov Random Field

Let x, an $M \times N$ texture pattern, be represented as a matrix whose elements take values from the set $A = \{0, 1, ..., G-1\}$. Let $\Omega = \{x \mid x_t = x(i,j) \ \in \ A\}$, be the set of all possible texture patterns, and let $S = \{1, ..., MN\}$ be the sites of a matrix ordered by a raster scan. A Gibbs random field (Grf) is a joint probability mass function defined on Ω which satisfies

$$P(x) = e^{-U(x)}/Z, \tag{1}$$

where $U(x)$ is the energy function and $Z = \sum_{y \in \Omega} e^{-U(y)}$ is the partition function.

A Markov random field is a Gibbs random field whose probability mass function satisfies the following conditions.

(a) *Positivity*: $P(X = x) > 0$ for all $x \in \Omega$.

(b) *Markov property*: For all $t \in S$, $P(X_t = x_t | X_r = x_r, \ r \neq t) = P(X_t = x_t | X_r = x_r, \ r \in R_t)$,

where R_t is the ordered set of neighbors of site t.

(c) *Homogeneity*: $P(x_t | R_t)$ does not depend on a particular site t.

Figure 1 defines the relative sites and orders of neighbors of site t. A Grf and an Mrf are equivalent with respect to a specified neighborhood system.

t:-3	t:-2	t:+4
t:-1	t	t:+1
t:-4	t:+2	t:+3

(a)

2	1	2
1	t	1
2	1	2

(b)

Figure 1: The relative sites and orders of neighbors of site t.

A Gibbs random field is completely characterized by its energy function. In this paper, two commonly used Mrf models whose energy functions have the following form are introduced:

$$U(x) = \sum_{t=1}^{MN} F(x_t) \; + \; \sum_{t=1}^{MN} \sum_{r=1}^{c} \; H(x_t, x_{t:+r}), \tag{2}$$

where $H(a,b) = H(b,a)$ and c depends on the size of the neighborhood. For example, c = 2, 4 for 1st-order and 2nd-order neighborhoods, respectively. Two Mrf models are defined below.

1.1 Generalized Ising Model (GIM)

Let $A = \{0, 1, ..., G-1\}$; the F and H functions of (2) in the generalized Ising model are defined as $F(x_t) = \alpha_{x_t}$ and $H(x_t, x_{t:+r})= \theta_r I(x_t, x_{t:+r})$, where $I(a,b) = -1$ if $a = b$ and $I(a,b) = 1$, otherwise.

Simple derivation gives the conditional density:

$$P(x_t|R_t) = \exp[-\alpha_{x_t} - \sum_{r=-c}^{c} \theta_r I(x_t, x_{t:+r})] \; / \; \sum_{s \in A} \; \exp[-\alpha_s - \sum_{r=-c}^{c} \theta_r I(s, x_{t:+r})]. \tag{3}$$

An algorithm for simulating the generalized Ising model (GIM) is given below. The synthesized textures obtained based on GIM with the parameters $M = N = 128$ and $\theta = (1, 1, 1, -1)$ are shown in Figure 5(a).

Algorithm GIM

(1) For s=1 to MN, randomly assign a $g \in A$ for x_s to give an initial image x.

(2) For s=1 to MN Do

- **(a)** Let $y_t = x_t$ for all $t \neq s$. Choose $g \in A$ at random and let $y_s = g$.
- **(b)** Let $r = min\{1, P(y)/P(x)\}$, where P is as defined in eq. (1).
- **(c)** $x \longleftarrow y$ with probability r.

(3) Repeat step (2) until "*convergence,*" is achieved, for example, in 50 iterations.

Each of the four parameters of the 2nd-order GIM model is restricted to be between -2 and 2 to avoid the phase-transition phenomenon. In practice, this model assumes that a texture will consist of a small number of gray levels, for example, 8 or less. Each parameter determines a directionality; the larger the negative value of the parameter, the stronger the direction.

1.2 Gaussian Markov Random Field (Gmrf)

A Gmrf was first proposed by Besag as a model for analyzing crop yields in plant ecology. This model has also been used to model natural textures. Let $A = R$; the corresponding F and H functions of Gmrf in eq. (2) are defined as

$$F(x_t) = (x_t - \mu_t)^2/2\sigma^2, \quad H(x_t, x_{t:+r}) = -\theta_r(x_t - \mu_t)(x_{t:+r} - \mu_{t:+r})/\sigma^2. \tag{4}$$

Simple derivation gives the conditional density:

$$P(x_t|R_t) = \frac{1}{2\pi\sigma^2}\exp\left[\left(x_t - \mu_t - \sum_{-c}^{c}\theta_r(x_{t:+r} - \mu_{t:+r})\right)^2/2\sigma^2\right]. \tag{5}$$

The distribution of X under the Gmrf model is a multivariate normal distribution [1] with then block circulant covariance matrix B^{-1} given below:

$$f(x) = \frac{|B|^{1/2}}{(2\pi\sigma^2)^{MN/2}}\exp[-(x-\mu)^t B(x-\mu)/2\sigma^2]. \tag{6}$$

The matrix B is an $MN \times MN$ block circulant matrix with M^2 blocks of N^2 circulant matrices $B'_{ij}s$, defined as

$$B = \begin{bmatrix} B_{11} & B_{12} & \dots & B_{1M} \\ B_{1M} & B_{11} & \dots & B_{1,M-1} \\ \vdots & \vdots & \vdots & \vdots \\ B_{12} & B_{13} & \dots & B_{11} \end{bmatrix}. \tag{7}$$

For the 2nd-order neighborhood,

$$\begin{aligned} B_{11} &= \textit{circulant}\ (1, -\theta_1, 0, \dots, 0, -\theta_1), \\ B_{12} &= \textit{circulant}\ (-\theta_2, -\theta_3, 0, \dots, 0, -\theta_4), \\ B_{1M} &= \textit{circulant}\ (-\theta_2, -\theta_4, 0, \dots, 0, -\theta_3), \\ B_{1j} &= O \text{ for } 2 < j < M. \end{aligned}$$

The probability density (7) is valid only if B is positive definite, and it is identifiable if no different parameter sets lead to the same eigenvalues of matrix B. Sampling a Gmrf is nothing but sampling a multivariate normal distribution. However, in image analysis, the B matrix is of order $MN \times MN$, that is, 16384×16384, when $M = N = 128$, so the traditional method for simulating the multivariate normal distribution based on Cholesky decomposition is infeasible. An algorithm using the properties of block circulant matrices is given below. Let y be an $M \times N$ array, and assign the first row of matrix B of order $MN \times MN$ to an $M \times N$ matrix A by means of $A(i,j) = B(1,\ j + N \times (i-1))$. An algorithm for simulating Gmrf by adopting fast Fourier transform (FFT) is listed below. A synthesized texture based on a Gmrf model with the parameters $M = N = 128$, $\mu = 128$, $\sigma = 64$, and $\theta = (0.07, -0.32, 0.07, 0.12)$ is shown in Figure 5(b).

Algorithm Gmrf

(1) Generate an $M \times N$ array Y with each element $Y(i,j) \sim N(0, \sigma^2)$ being independent.

(2) $Y \longleftarrow$ apply 2D FFT on Y.

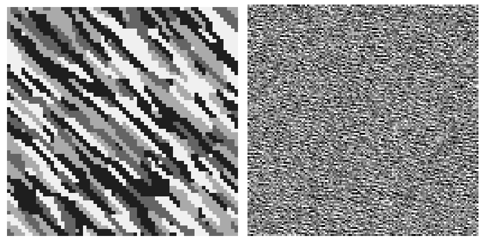
(3) $A \longleftarrow$ apply 2D inverse FFT on A (formed from the first row of matrix B).

(4) $Y(u,v) \longleftarrow Y(u,v)/\sqrt{A(u,v)},\ 0 \le u < M,\ 0 \le v < N$.

(5) $Y \longleftarrow$ apply 2D inverse FFT on Y.

(6) $Y + \mu$ is a realization.

This model is nothing but a multivariate normal distribution with the covariance matrix $\sigma^2 B^{-1}$ being a large block-circulant matrix. The parameter θ affects the directionality, and the parameter σ describes the spread of the gray values. It should be mentioned that the parameter θ must make the matrix B positive definite. It seems that this model tends to generate more textures as its order increases. However, the restriction of positive definiteness of matrix B results in the problem of parameter selection.



(a) (b)

Figure 2: The relative sites and orders of neighbors of site t.