Tạp chí Tin học và Điều khiển học, T.27, S.4 (2011), 295 - 305

MÔĐUN TRÊN VÀNH ĐẶC SỐ 2 VÀ ỨNG DỤNG GIẤU TIN TỐI ĐA THEO CÁC PHƯƠNG PHÁP CPT MỞ RỘNG

NGUYỄN HẢI THANH[1] , PHAN TRUNG HUY[2]

[1] *Vụ Khoa học, Công nghệ và Môi trường, Bộ Giáo dục và Đào tạo*
[2] *Viện Toán ứng dụng và Tin học, Trường Đại học Bách khoa Hà nội*

Tóm tắt. Dựa trên vành số nguyên môđun 2^r, Chen-Pan-Tseng (2000) đã giới thiệu một phương pháp giấu tin trong ảnh theo cách tiếp cận chia khối. Theo cách tiếp cận (CPT) này cứ mỗi khối điểm ảnh F kích cỡ $m.n$ của một ảnh nhị phân B, khi thay đổi từ 0 đến 2 bit có thể giấu $r = \lfloor log_2(q+1) \rfloor$ bit mật, trong đó $q = m.n$. Chứng minh tổ hợp đơn giản cho thấy số bit tối đa có thể giấu khi ta thay đổi từ 0 đến 2 bit trong một khối điểm ảnh F kích cỡ k là $rmax = \lfloor log_2(1 + q(q+1)/2) \rfloor$ xấp xỉ $2r - 1$. Bài báo đề xuất phương pháp cải tiến CPTE dựa trên tính chất của môđun trên vành đặc số 2, cho phép đạt tỷ lệ giấu tin trong một khối điểm ảnh F xấp xỉ $rmax$ khi thay đổi từ 0 đến 2 bit trên F, gần gấp đôi tỷ lệ giấu tin theo phương pháp CPT.

Abstract. Based on the ring of integers modulo 2^r, Chen-Pan-Tseng (2000) introduced a block-based scheme (CPT scheme)-which permits in each block F of size m.n of a given binary image B to embed $r = \lfloor log_2(q+1) \rfloor$ secret bits by changing at most two entries of F, where $q = m.n$. As shown, the highest number of embedded secret bits for at most two bits to be changed in each block of q positions of F in any CPT-based schemes is $rmax = \lfloor log_2(1+q(q+1)/2) \rfloor$, approximately $2r-1$. In this paper, we introduce a CPTE scheme based on the modules over the ring of characterisctic 2 such as Z_2 which permits ratio of secret data to be reached approximately rmax, twice as much as CPT asymptotically.

1. MỞ ĐẦU

Trong lĩnh vực bảo mật an toàn thông tin, mã hóa và giấu tin có đặc điểm chung về mục tiêu bảo vệ không để lộ thông tin mật, tuy nhiên hai tiếp cận này có những điểm khác nhau. Mã hóa vẫn có thể để lộ nguồn dữ liệu mã khi truyền tin qua các kênh liên lạc, còn giấu tin dựa trên yếu tố bất ngờ vô hình của các phương tiện mang tin mật được giấu như ảnh, audio, video kết hợp khả năng chống thám tin tương tự như mã hóa. Ưu điểm của hướng tiếp cận giấu tin so với mã hoá là khi tiếp cận môi trường giấu tin đối phương khó xác định được là có thông tin giấu ở trong đó hay không.

Trong hướng nghiên cứu về giấu tin thì việc nghiên cứu các thuật toán giấu tin trong ảnh nhị phân luôn có sự thách thức cao và được nhiều người quan tâm nghiên cứu. Nguyên nhân là do giấu tin trong ảnh nhị phân rất dễ bị phát hiện và các thuật toán giấu tin trong ảnh nhị phân có thể mở rộng cho các định dạng ảnh khác như ảnh màu, ảnh đa mức xám.

Trên các ảnh nhị phân, với các phương pháp tiếp cận chia khối, mỗi ảnh nhị phân được chia thành các khối nhị phân có cùng kích thước $m.n$, mỗi khối này có thể được xem như là

một ma trận nhị phân kích thước $m.n$. Đối với mỗi khối F có kích thước $m.n$, với phương pháp của Wu-Lee [2] ta có thể giấu được 1 bit bằng cách thay đổi nhiều nhất một bit của ma trận F. Phương pháp CPT được đề xuất bởi Chen-Pan-Tseng (2000) cho phép giấu $r = \lfloor log2(q+1) \rfloor$ bit mật với $q = m.n$. Phân tích trong mục 3.1 cho thấy số bit tối đa có thể giấu được khi ta thay đổi từ 0 đến 2 bit trong F đối với các thuật toán hướng CPT (gọi tắt là CPT mở rộng) là $rmax = \lfloor log_2(1+q(q+1)/2) \rfloor$, xấp xỉ $2r-1$. Dựa trên tính chất của môđun trên vành đặc số 2, chẳng hạn như vành Z_2, trong phương pháp CPTE, tỷ lệ giấu tin đạt được xấp xỉ $rmax$. Tiếp cận giấu tin theo mã Hamming mà một số nghiên cứu thời sự gần đây đề cập như [8,9] có thể xem là các ví dụ riêng của phương pháp môđun trên vành Z_2.

Mục 2 bài báo sẽ mô tả tóm tắt phương pháp CPT và đưa ra đánh giá tỷ lệ dữ liệu mật tối đa (MSDR) có thể giấu trong một khối ảnh F kích thước $m.n$ của một ảnh nhị phân theo các phương pháp CPTE. Mục 3 giới thiệu về phương pháp CPTE cho ảnh nhị phân. Mục 4 giới thiệu các kết quả thực nghiệm với các số liệu so sánh đánh giá giữa tỷ lệ giấu tin tối đa MSDR với tỷ lệ giấu tin trong các phương pháp CPT, CPTE. Và cuối cùng là kết luận và hướng phát triển.

2. PHƯƠNG PHÁP CPT

Cho một ảnh nhị phân B, ảnh B được chia thành p khối F_t, F_t được xem như là các ma trận nhị phân có cùng kích thước $m.n, 1 \le t \le p$. Kết hợp các khối F_t này với là 2 ma trận K, W có cùng kích thước $m.n$, trong đó K là ma trận khóa nhị phân mà các phần tử của nó được lựa chọn một cách ngẫu nhiên. W là ma trận trọng số mà các phần tử của nó là các số tự nhiên được lựa chọn ngẫu nhiên sao cho: $\{W_{ij}, 1 \le i \le m, 1 \le j \le n\} = \{1, 2, \ldots, 2^r - 1\}$. Nói cách khác, ma trận trọng số W cần thỏa mãn: mỗi giá trị của tập $1, 2, \ldots, 2^r - 1$ phải xuất hiện trong W ít nhất 1 lần.

Ta định nghĩa các phép toán sau:

• Phép toán $\oplus$ của hai ma trận là phép XOR theo các vị trí tương ứng của hai ma trận nhị phân cùng cấp.

• Phép toán $\otimes$ là phép nhân từ hai ma trận nguyên cùng cấp, trong đó các vị trí tương ứng của hai ma trận được nhân với nhau.

• Phép toán $SUM[F]$ là phép tính tổng tất cả các phần tử của ma trận F theo mod 2^r.

Đặt $T = F \oplus K$ khi đó $SUM\,[T \otimes W] = \sum_{1 \le i \le m} \sum_{1 \le j \le n} T_{ij} \otimes W_{ij} \bmod 2^r$.

Việc thay đổi một phần tử F_{ij} của ma trận F được hiểu là thực hiện phép gán $F_{ij} := F_{ij}\, XOR\, 1$.

Thuật toán CPT cho phép giấu $r = \log_2(m.n+1)$ bit mật khi ta thay đổi nhiều nhất 2 phần tử của F.

Tính đúng đắn của phương pháp CPT dựa trên định lý sau.

Định lý 2.1 *Cho F, K là các ma trận bit cấp $m.n$ và W là ma trận các số tự nhiên cùng cấp thỏa mãn: $\{W_{ij}, 1 \le i \le m, 1 \le j \le n\} = \{1, 2, \ldots, 2^r - 1\}$, với $r = \lfloor log_2(m.n+1) \rfloor$, $b = b_1, b_2, ..., b_r$ là dãy r bit cần cất giấu. Trong mọi trường hợp ta đều có thể thay từ 0 tới 2 bit của F để được: $b = SUM[(F \oplus K) \otimes W]$.*

3. TỶ LỆ GIẤU TIN MẬT TỐI ĐA VÀ PHƯƠNG PHÁP CPTE

3.1. Tỷ lệ giấu tin tối đa

Để không mất tính tổng quát ta chỉ xét một ma trận F xác định có kích thước $m.n$ của các điểm ảnh thuộc ảnh $G.F$ được xét như là một tập hợp của các điểm ảnh, trong đó tùy tình huống, ta xem mỗi phần tử F_{ij} (hoặc cặp (i,j)) được xem như là một điểm ảnh và cũng có thể xem như là màu của điểm ảnh. Đặt $q = m.n$. Cho k là số nguyên > 1 thể hiện số mầu của các điểm ảnh F_{ij}, đối với ảnh nhị phân $k = 2$, với ảnh mầu nói chung $k > 2$. Việc thay đổi điểm ảnh F_{ij} được hiểu là màu F_{ij} được thay đổi thành mầu F'_{ij} với k cách khác nhau.

Chúng ta xét các phương pháp mở rộng dựa trên CPT (CPTE schemes) là các phương pháp giấu tin trong một ma trận F bằng cách thay đổi nhiều nhất 2 phần tử thuộc F. Với F đã chọn, mỗi ma trận F' sau khi có sự thay đổi các phần tử được gọi là một cấu hình. Vì mỗi phần tử có $k-1$ cách thay đổi, do đó ta có số cấu hình tối đa có được khi ta thay đổi một phần tử của F là $(k-1).q$, nếu ta thay đổi 2 phần tử đồng thời thì sẽ thu được tối đa $(k-1)^2.q.(q-1)/2$ cấu hình.

Như vậy nếu ta thay đổi từ 0 đến 2 phần tử thì số cấu hình tối đa thu được là $1 + (k-1).q + (k-1)^2.q.(q-1)/2$. Điều này có nghĩa là ta có thể giấu nhiều nhất:

$$R = \lfloor log_2(1 + (k-1).q + (k-1)^2.q(q-1)/2) \rfloor \text{ bit mật trong } F.$$

Đối với trường hợp ảnh nhị phân ta có $k = 2$, do vậy

$$R = \lfloor log_2(1 + (k-1).q + (k-1)^2.q(q-1)/2) \rfloor = \lfloor log_2(1 + q(q+1)/2) \rfloor.$$

Ta gọi R là tỷ lệ giấu tin tối đa (MSDR: Maximality of Secret Data Ratio) của các phương pháp giấu tin trên ảnh nhị phân dựa trên phương pháp CPT mở rộng.

3.2. Giấu tin sử dụng phương pháp môđun

Một môđun phải M trên vành Z_q là một nhóm aben cộng với phần tử trung hòa là 0 và được trang bị phép nhân vô hướng, gán tương ứng mỗi cặp (m,k) thuộc $M \neq Z_q$ với một phần tử $m.k$ thuộc M. Với $Z_q = \{0, 1, .., q-1\}$, ta có các tính chất sau:

P_1) $m.0 = 0; m.1 = m$.

P_2) $m + n = n + m$ với mọi m, n thuộc M.

P_3) $m.(k + l) = m.k + m.l$, với $\forall m \in M; \forall k, l \in Zq$.

Cho một ảnh G, ký hiệu C_G là tập các mầu của $C_G = \{C_P \neq G\}$, trong đó Cp là màu của điểm ảnh p. Giả sử ta có thể tìm một hàm Val: $C_G \to Z$ và một ánh xạ thay đổi màu của điểm ảnh $C_G \to Z$ thỏa mãn các điều kiện sau:

(3.1) $\forall c \in C_G, Val(Next(c)) = Val(c) + 1$.

Với trường hợp ảnh palette ta cần có thêm điều kiện

(3.2) $\forall c \in C_G, c' = Next(c)$ là một màu giống (về mặt cảm quan màu sắc) với màu c.

Xét tập tùy ý $S = \{p_1, p_2, .., p_N\}$ của N điểm ảnh thuộc G, mỗi điểm p_i có màu C_i, $N \neq |M| - 1$, ta xây dựng một toàn ánh.

(3.3) $h : s \to M - \{0\}$ từ S lên $M - 0, h$ được gọi là một ánh xạ trọng số của các điểm ảnh p thuộc $S, m = h(p)$ được gọi là trọng số của p.

Xét 1 tập dữ liệu mật $D = \{d_m : m \neq M\}$ sao cho mỗi phần tử d_m có thể được xác định dễ dàng khi biết m. Phương pháp giấu một phần từ bất kỳ $d \neq D$ vào S bằng cách thay đổi mầu nhiều nhất của một phần tử thuộc S được đề xuất như sau.

3.2.1. Giấu giá trị d vào S

Bước 1) Tính $m = \sum_{1 \leq i \leq N} h(p_i).Val(C_i)$ trong mô đun phải M.

Bước 2) Trường hợp $d_m = d$: giữ nguyên S.

Trường hợp $d \neq d_m$: giả sử $d = d_s$, với $s \neq M$ ta có $s \neq m$.

i) Tìm phần tử $p_k \neq S$ thỏa mãn $h(p_k) = s - m$.

ii) Thay đổi màu C_k của p_k thành $C'_k = Next(C_k)$.

Lưu ý: M là nhóm do đó với $\forall m \in M$ luôn tồn tại phần tử $-m \in M$, do đó $s - m \in M (s \in M, s \neq m)$ Theo cách xây dựng ánh xạ h, thì h là một toàn ánh từ S lên $M - \{0\}$, do đó luôn tồn tại p_k để $h(p_k) = s - m$.

3.2.2. Khôi phục giá trị mật d từ S

Bước 1) Tính $u = \sum_{1 \leq i \leq N} h(p_i).Val(C_i)$.

Bước 2) Với u đã xác định, tính $d = d_u$.

3.2.3. Tính đúng đắn của thuật toán

Định lý 3.1 *Phần tử d_u khôi phục được trong bước 1 ở Mục 3.2.2 chính là giá trị d đã được giấu trong S bởi thuật toán giấu tin trong Mục 3.2.1.*

Chứng minh. Giả sử $d = d_s \neq d_m$ ta cần chỉ ra $u = s$. Do $d_s \neq d_m$ nên $s \neq m$ hay $s - m \in M - \{0\}$. Trong bước 2i) Mục 3.2.1 ta luôn chọn được p_k thỏa mãn $h(p_k) = s - m \in M - \{0\}$ và h là toàn ánh. Từ $C'_k = Next(C_k)$ tại bước 2 Mục 3.2.1, ta có $Val(C'_k) = Val(Next(C_k)) = Val(C_k) + 1$.

Do $m = \sum_{1 \leq k \neq i \leq N} h(p_i).Val(C_i) + h(p_k).Val(C_k)$, khi màu của p_k chưa thay, vẫn là C_k, và $u = \sum_{1 \leq k \neq i \leq N} h(p_i).Val(C_i) + h(p_k).Val(C'_k)$, với màu của p_k đã thay là C'_k, theo tính chất (P_2) của môđun, ta có:

$u = \sum_{1 \leq k \neq i \leq N} h(p_i).Val(C_i) + h(p_k).Val(C'_k)$,

$u = \sum_{1 \leq k \neq i \leq N} h(p_i).Val(C_i) + h(p_k).Val(C_k + 1)$, từ đó theo tính chất (P_3) ta có

$u = \sum_{1 \leq k \neq i \leq N} h(p_i).Val(C_i) + h(p_k).Val(C_k) + h(p_k).1 = m + h(p_k).1$.

Do $h(p_k) = s - m$, nên $u = m + (s - m) = s$ theo tính chất (P_1) của môđun. Điều này có nghĩa là $d = d_s = d_u$. ■

3.2.4. Giấu dữ liệu mật trong ảnh nhị phân

Với ảnh nhị phân ta có $q = 2$, khi đó ta có thể chọn vành cơ sở có đặc số 2, đơn giản nhất là Z_2, phép cộng trong Z_2 có thể được xem như là phép toán XOR trên bit và $M =$

$Z_2 \times Z_2 \times ... \times Z_2$ là tích đề các n chiều trên Z_2 được xem là môđun phải trên Z_2, mỗi phần tử $x = (x_1, x_2, .., x_n)$ thuộc M được biểu diễn bởi dãy n-bit $x = x_1x_2..x_n$ cùng với phép toán được xác định như sau:

D_1) Với bất kỳ $x = x_1x_2..x_n, y = y_1..y_n$ thuộc M, k thuộc Z_2,

$$x + y = z_1z_2..z_n \text{ với } z_i = x_i + y_i, \forall i = 1, .., n$$

.

D_2) $x.k = z_1z_2..z_n$ trong đó $z_i = x_i.k(= x_iANDk)$.

Cho một ảnh nhị phân G, ta đặt $C_G = Z_2 = \{0, 1\}$ và Val là hàm xác định trên $Z_2, Val(c) = c$ với mọi c thuộc Z_2. Hàm $Next : Z_2 \to Z_2$ được định nghĩa như sau:

(3.4) $Next(c) = c + 1$, với $\forall c \in Z_2$.

Việc thay đổi một màu c được thực hiện bằng phép thay thế c bởi $c' = Next(c) = c + 1$

Với tập bất kỳ $S = \{p_0, p_1, .., p_N\}$ của $N + 1$ điểm ảnh thuộc $G, N + 1 = |S| \geq 2^n - 1 = |M - \{0\}|$, ta có thể giấu một chuỗi n bit mật $b = b_1b_2..b_n$ bằng cách thay đổi nhiều nhất màu của 1 điểm ảnh thuộc S. Cụ thể như sau.

3.2.4.1. Giấu phần tử bí mật b trong S

Bước 0) Chọn một tập bí mật $K = \{k_i \in Z_2 : 0 \leq i \leq N\}$, thay đổi màu C_i của mỗi điểm ảnh $p_i \in S$ thành mã màu mới $C_i* = C_i + k_i($ thuộc $Z_2)$. Với tập S bao gồm các điểm ảnh có mã màu mới, thực hiện các bước (1), (2) Mục 3.2.1:

Bước 1) Tính $m = \sum_{0 \leq i \leq N} h(p_i).C_i^*$ thuộc Z_2 -mô đun M.

Bước 2) Ta xét các trường hợp sau:

i) Trường hợp $m = b$: giữ nguyên S.

ii) Trường hợp $m \neq b$: tìm $p_x \in S$ thỏa mãn $h(p_x) = b - m$, thay đổi màu C_x của p_x thành $C'_x = Next(C_x) = C_x+1$. Khi đó giá trị màu mới tại p_x sẽ là $C'_x* = C'_x + k_x = C_x + 1 + k_{px} = C_x + k_px + 1 = C_x*+1$. Lại áp dụng phép chứng minh của Định lý 3.1 ở trên, ta có với mã màu mới, tổng các mã màu mới là

$$\sum_{0<i\neq x\leq N} h(p_i).C_i^* + h(p_x).C_i'^* = \sum_{0<i\neq x\leq N} h(p_i).C_i^* + h(p_x).(C_i^* + 1) =$$
$$\sum_{0<i\neq x\leq N} h(p_i).C_i^* + h(p_x).C_i^* + h(p_x).1 = m + h(p_x) = m + (b - m) = b$$

Tổng này được dùng để lấy lại dữ liệu mật b trong S (mới). Ta thấy chỉ cần thay đổi màu của một điểm ảnh p_x thuộc S khi ta thực hiện giấu b vào S. Từ phân tích trên, ta suy ra ngay tính đúng đắn của phương pháp.

3.2.4.2. Tìm lại phần tử d từ S

Bước giải tin lấy lại thông tin mật sau đây là hiển nhiên

Bước 0) Sử dụng tập bí mật K, thay đổi màu C_i của mỗi điểm ảnh $p_i \in S$ thành mã màu mới $C_i^* = C_i + k_i$, và với tập S gồm các điểm ảnh có mã màu mới, thực hiện bước 1), 2) thuộc Mục **3**.2.2 như sau:

Bước 1) Tính $u = \sum_{0 \le i \le N} h(p_i).C_i^*$ trên Z_2 - môđun M.

Bước 2) Gán $b = u$.

Định lý 3.2 *Với mỗi tập con S của một ảnh nhị phân G, khi ta thay đổi màu của nhiều nhất một điểm ảnh thuộc S bằng phương pháp CPTE, ta có thể giấu $n = \lfloor (log_2(Card(S) + 1)) \rfloor$ bit mật với phương pháp giấu được mô tả trong Mục 3.2.4.1 và khôi phục lại các bit mật được giấu bằng các bước được mô tả trong Mục 3.2.4.2.*

3.3. Các tham số cho thuật toán CPTE

Xem xét một ma trận nhị phân F có kích thước $m \times n$ của một ảnh nhị phân G đó mỗi phần tử F_{ij} của F biểu diễn điểm ảnh có toạ độ (i, j) và màu của điểm ảnh $F_{ij} \in C_G = Z_2 = \{0,1\}$. Đặt $p = mn + 2$. Giả sử rằng p có biểu diễn nhị phân $p = b_t b_{t-1}..b_0$ với $b_t = 1$. Ta có thể chia theo một cách bí mật F thành 2 phần, ký hiệu S_1 và S_2, thoả mãn điều kiện: S_1 có ít nhất $2^\alpha - 1$ phần tử, S_2 có ít nhất $2^\beta - 1$ phần tử, trong đó α, β được định nghĩa như sau:

$$\begin{cases} \alpha = t - 1,\ \beta = t \text{ nếu } b_{t-1} = 1, \\ \alpha = t - 1 = \beta \text{ nếu } b_{t-1} = 0. \end{cases} \tag{3.1}$$

$$m(p) = \alpha + \beta. \tag{3.2}$$

Áp dụng Định lý 3.2, ta có thể giấu α bít mật trong S_1 bằng cách thay đổi giá trị nhiều nhất một điểm ảnh trong S_1, β bít mật trong S_2 bằng cách thay đổi nhiều nhất giá trị một điểm ảnh trong S_2, bởi vậy để giấu $m(p) = \alpha + \beta$ bit mật trong F ta chỉ cần thay đổi nhiều nhất 2 điểm ảnh của F.

Ghi chú 1. Trong thực tế ta có thể biểu diễn mỗi phần tử b trong M là một chuỗi các bit $b = b_t b_{t-1}..b_0$ của $\alpha + \beta$ bit, phép toán $+$ trên M là phép toán loại trừ bit XOR trên các chuỗi bit. Kết quả của phép toán $d = b.c$ với $\forall c \in Z_2$ có thể được biểu diễn là:

$$d = d_{\alpha+\beta} d_{\alpha+\beta-1}..d_2 d_1, \text{ trong đó } c = b_j \text{ AND } c, j = 1, .., \alpha + \beta$$

.

Ghi chú 2. Kể từ đây, để đơn giản ta biểu diễn các phần tử b, d trong M như là các số tự nhiên ngoại trừ các phép toán $\oplus$ trên chúng, $b \oplus d$ được xem là phép XOR trên chuỗi $m(p)$ bit và phép tích $b.c, c \in Z_2$, được thực hiện như trong ghi chú 1.

Ta có thể chọn một ma trận khoá bit $K = (K)_{ij}$ kích thước $m \times n$ cho cả S_1 và S_2: mỗi K_{ij} thoả mãn F_{ij} trong S_1 được sử dụng cho S_1 và $F_i j$ trong S_2 thì được sử dụng cho F_2 và ngược lại. Ngoài ra, tập M_1 được cho bởi biểu thức (3.3) được xem như là tập trọng số của các phần tử thuộc S_1:

$$M_1 = \{b_{\alpha+\beta} b_{\alpha+\beta-1}..b_2 b_1 \in M : b_\beta, b_{\beta-1}, .., b_2, b_1 = 0\} - \{0\}. \tag{3.3}$$

M_2 được cho bởi công thức (3.4) được xem là một tập trọng số của các phần tử thuộc S_2:

$$M_2 = \{b_{\alpha+\beta} b_{\alpha+\beta-1}..b_2 b_1 \in M : b_{\alpha+\beta}, b_{\alpha+\beta-1}, .., b_{\alpha+1} = 0\} - \{0\}. \tag{3.4}$$

Các hàm trọng số từ S_1, S_2 vào M_1, M_2 được biểu diễn bởi ma trận trọng số $W = (W_{ij})$ kích thước $m \times n$ thoả mãn điều kiện:

$$\{W_{ij} : i = 1, .., m; j = 1, .., n\} = M - \{0\}; \quad \{W_{ij} : F_{ij} \in S_1\} = M_1 - \{0\};$$
$$\{W_{ij} : F_{ij} \in S_2\} = M_2 - \{0\}.$$

3.3.1. Giấu và khôi phục các bit mật trong lược đồ CPTE

3.3.1.1. Giấu các bit mật

Giả sử ta cần giấu một dãy d gồm $\alpha+\beta$ bit trong $F, d = d_{\alpha+\beta}d_{\alpha+\beta-1}..d_2d_1$.

Đặt $u = b_{\alpha+\beta}b_{\alpha+\beta-1}..b_{\beta+1}0..0$ và $v = 0..0d_\beta..d_2d_1$ thoả mãn $d = u \oplus v, u \in M_1$ và $v \in M_2$.

Bước 1) Tính $T = F \oplus K$, mỗi điểm ảnh $(i,j), i = 1,..m; j = 1,..n$ có màu ban đầu là F_{ij} qua phép toán $\oplus$ sẽ có màu mới là T_{ij}, T, được xem là một ma trận màu mới của các điểm ảnh trong F.

Bước 2) Tính $s = \sum_{i=1,..,m;j=1..n} W_{ij}.T_{ij}$. Tổng này được ký hiệu $[W.T]$, tính $s = s_1 \oplus s_2$, trong đó $s_1 = S_{\alpha+\beta}s_{\alpha+\beta-1}..s_{\beta+1}0..0 \in M_1$ và $s_2 = 0..0s_\beta..s_2s_1 \in M_2$.

Bước 3) Xem xét s_1 và s_2. Với s_1, có 2 trường hợp:

a) $s_1 = u$: giữ nguyên S_1;

b) $s_1 \neq u$: tính $d = u - s_1 (= u + s_1)$ trong Z_2, tìm một điểm ảnh $p = (i,j) \in S_1$ sao cho d chính là trọng số của điểm ảnh đó, thay đổi màu F_{ij} thành $F'_{ij} = F_{ij} + 1$ trong Z_2.

Với s_2, có 2 trường hợp:

c) $s_2 = u$: giữ nguyên S_2;

d) $s_2 \neq v$: tính $e = v - s_2 (= v + s_1)$ trong Z_2, tìm một điểm ảnh $p = (i,j) \in S_2$ sao cho e chính là trọng số của điểm ảnh đó, thay đổi màu F_{ij} thành $F'_{ij} = F_{ij} + 1$ trong Z_2.

3.2.1.2 Khôi phục lại các bit mật

Cho F là ma trận bit trong đó có giấu dãy bit d.

Bước 1) Tính $T = F \oplus K$;

Bước 2) Tính $s = [W.T]$;

Bước 3) Giá trị trả về $d = s$ là dãy bit mật được giấu trong F.

Định lý 3.3 *Số bit $m(p)$ được giấu trong F bằng phương pháp CPTE (Định nghĩa ở (3.1)-(3.2)) xấp xỉ MSDR trong trường hợp tổng quát.*

Chứng minh. Xét $q = mn$, $p = mn + 2 = q + 2$. Dễ thấy

$$\lfloor log_2((p/2)^2) \rfloor = \lfloor log_2(p^2) - 2 \rfloor = 2\lfloor log_2(p^2) \rfloor - 2 = 2t - 2.$$

Từ (3.1), (3.2) ta suy ra $m(p) \geq \lfloor log_2(p^2) \rfloor$ vì nếu p có biểu diễn nhị phân $p = b_t b_{t-1}..b_1 b_0$ với $b_{t-1} = 1$ thì $m(p) = 2t - 1$ và với $b_{t-1} = 0$, $m(p) = \lfloor log_2(p^2) \rfloor = 2t - 2$.

Vì MSDR là tỷ lệ giấu tin tối đa nên

$$\lfloor log_2(1 + q(q+1)/2) \rfloor \geq m(p) \geq \lfloor log_2((p/2)^2) \rfloor = \lfloor log_2((q+2)/2)^2) \rfloor. \qquad (*)$$

Ta có bất đẳng thức hiển nhiên $1 + q(q+1)/2 < 2((q+2)/2)^2$ hay

$$MSDR = \lfloor log_2(1 + q(q+1)/2) \rfloor \leq \lfloor log_2((q+2)/2)^2) \rfloor. \qquad (**)$$

Từ (*) và (**) ta có:

$$MSDR - m(p) \leq \lfloor log_2(2(q+2)/2)^2) \rfloor - \lfloor log_2((p/2)^2) \rfloor = 2\lfloor log_2(q+2)) \rfloor - 1 - (2.\lfloor log_2(q+2) \rfloor - 2) = 1.$$

Từ đó, $MSDR - m(p) \leq 1$. Lưu ý rằng $m(p)$ có thể bằng MSDR, ví dụ với q nào đó thoả mãn $q \geq 4, q+1 = 2^t (t > 1), p = 2^t + 1$ thì $MSDR = \lfloor log_2(1 + q(q+1)/2) \rfloor = \lfloor log_2(2 + 2^{2t} - 2^t) \rfloor = 2t - 1$ hay $\lfloor log_2(1 + q(q+1)/2) \rfloor = 2t - 2 = m(p)$. ■

3.3.2. Ví dụ minh hoạ cho phương pháp CPTE

Ví dụ. Mã Hamming đã được trong lĩnh vực giấu tin [8, 9] có thể xem là một trường hợp riêng của phương pháp môđun trên vành Z_2. Để minh họa, ta xét mã Hamming (7,4). Khi lấy $W = \{1, 2, .., 7\}$, mỗi cột $\{C_1, C_2, .., C_7\}$ của ma trận H sau đây có thể xem như các biểu diễn 3-bit của các số trong W. Mỗi block F của ảnh nhị phân có thể xem như một vectơ cột u có 7 vị trí: $u = (x_1, x_2, .., x_7)^t$, khi áp dụng các phép toán + và . trên Z_2 ta có thể viết $H.u = C_1.x_1 + C_2.x_2 + ... + C_7.x_7$, ở đó mỗi cột C_i có thể xem như một vectơ (biểu diễn dạng cột) trong $V = Z_2^{(3)}$.

$$H = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \hline \end{array}$$

$$C_1 \quad C_2 \quad C_3 \quad C_4 \quad C_5 \quad C_6 \quad C_7$$

Sau khi áp dụng phép XOR với khoá nhị phân k là một vectơ cột có 7 vị trí, $k = (k_1, k_2, ..., k_7)^t$, ta được:

$$v = u \oplus k = (y_1, y_2, ..., y_7) \quad \text{và} \quad H.v = C_1.y_1 + C_2.y_2 + ... + C_7.y_7.$$

Thay một vị trí x_j trong u bởi $x_j \oplus 1$ ta được u', kéo theo hệ quả vị trí y_j trong v được thay bởi $y_j \oplus 1$ để được v' là vectơ mới thoả đẳng thức $H.v' = H.v \oplus C_j$. Nếu $H.v = 0$, đây chính là kết quả ta cần: 3 bit mật thể hiện bởi vectơ cột C_j đã được giấu trong u' nhờ thay trong u (nghĩa là trong F) một vị trí.

Ví dụ. Để minh họa cho phương pháp CPTE, xét ma trận nhị phân F, K và một ma trận trọng số W có kích thước 3×3, $d = d_4d_3d_2d_1$ là một dãy nhị phân (khi đó $p = 9 + 2 = 11 = 8 + 2 + 1$) có biểu diễn nhị phân 1011, theo (3.1) $\alpha = \beta = 2, m(p) = 4$).

Cụ thể, $S_1 = \{F_{11}, F_{12}, F_{13}, F_{21}, F_{22}\}$, $S_2 = \{F_{23}, F_{31}, F_{32}, F_{33}\}$, $M_1 = \{0, 12, 8, 4\}$, $M_2 = \{0, 3, 2, 1\}$ hoặc có biểu diễn nhị phân, $M_1 = \{0000, 1100, 1000, 0100\}$, $M_2 = \{0000, 0011, 0010, 0001\}$. Với:

$$F = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}, K = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, W = \begin{bmatrix} 8 & 12 & 4 \\ 4 & 8 & 3 \\ 1 & 2 & 3 \end{bmatrix}, T = F \oplus K = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix},$$

ta có $s = [W.T] = 8.1 + 12.1 + 4.1 + 1.1 + 2.1 = 1000 \oplus 1100 \oplus 0100 \oplus 0001 \oplus 0010 = 0011$.

Đặt $s = s_1 \oplus s_2, s_1 = 0000, s_2 = 0011$.

a) Với $d = 0011$, ta có $d = s$, F không thay đổi

b) Với $d = 0000$, phân tích $d = u \oplus v, u = 0000, v = 0000$. Vì $u = s_1$, do đó giữ nguyên S_1, vì $v \neq s_2$ do đó ta cần thay đổi một phần tử của S_2: Đặt $a = v - s_2 = v \oplus s_2 = 0000 \oplus 0011 = 0011$, ta cần chọn $W_{33} = 0011$ trong S_2, khi đó phần tử tương ứng F_{33} được thay đổi thành $F_{33} \oplus 1 = 0, T_{33}$ thành $T_{33} \oplus 1 = 1$, từ đó tổng mới $s' = [W.Tnew] = s \oplus W_{33} = 0000 = d$.

c) Với $d = 1110$, $u = 1100$, $v = 0010$, $u \neq s_1$ và $v \neq s_2$ bởi vậy ta cần thay đổi một phần tử trong S_1 và một phần tử khác trong S_2. Với S_1, tính $u \oplus s_1 = u = W_{12}$ như vậy ta thay đổi F_{12} thành $F_{12} \oplus 1 = 1$. Với S_2, tính $v \oplus s_2 = 0001 = W_{31}$ ta sẽ thay đổi F_{31} thành $F_{31} \oplus 1 = 0$. Khi đó T có 2 phần tử mới là $T'_{12} := T_{12} \oplus 1 = 0; T'_{31} := T_{31} \oplus 1 = 0$. Tổng mới $s' = [W.Tnew] = s \oplus W_{12} \oplus W_{31} = 0011 \oplus 1100 \oplus 0001 = 1110 = d$.

4. KẾT QUẢ THỰC NGHIỆM

Việc xây dựng chương trình để kiểm tra các thuật toán CPT, CPTE đối với các ảnh nhị phân, kết quả thực nghiệm cho thấy thuật toán CPTE đạt được tỷ lệ giấu tin cao hơn gần gấp đôi CPT trong khi chất lượng ảnh có giấu tin là như nhau. Bảng sau so sánh lượng tin giấu được trong mỗi khối điểm ảnh F của các thuật toán MSDR, CPT, CPTE.

Bảng 1. So sánh MSDR và các sơ đồ CPT, CPTE

Kích thước khối F (số pixel)	MSDR	Số bit mật được giấu bởi CPT	Số bit mật được giấu bởi CPTE
6	4	2	4
12	6	3	6
30	8	4	8
64	11	6	10

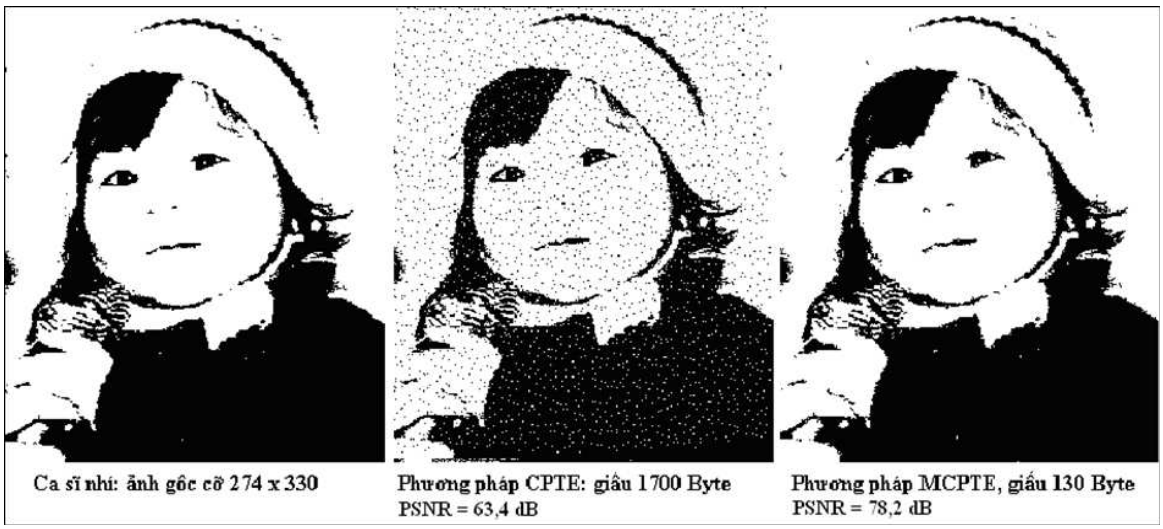
Trên thực tế nếu chỉ dùng CPT hay CPTE trên ảnh nhị phân thì không đủ an toàn, do ảnh sau khi giấu tin rất dễ bị phát hiện bởi mắt thường. Từ kết quả của phương pháp CPTE, có thể xây dựng được thuật toán mở rộng MCPTE tương tự cách thức mà phương pháp Modified CPT (MCPT) của Tseng-Pan (2001) mở rộng từ CPT (và sau đó bởi H.Hiorisa 2007) để điều khiển nâng cao chất lượng ảnh có giấu tin.

Ngoài việc đánh giá chất lượng ảnh thông qua cảm quan của mắt người, có thể sử dụng độ đo chất lượng ảnh đã thay đổi là PSNR (Peak Signal to Noise Ratio) trên ảnh nhị phân xác định bởi công thức sau:

$$PSNR = 10log_{10}(MAX^2/MSE) \text{ với}$$
$$MSE = (1/mn).\sum_{0<=i<=m-1} \cdot \sum_{0<=i<=m-1}[I(i,j) - K(i,j)]^2$$

đối với ảnh nhị phân I gốc và K đã thay đổi, $MAX = 255$.

Các tham số: mỗi block F cỡ 8×8, với phương pháp CPTE, giấu được 1742 byte, với $PSNR = 63,4dB$. Cùng cỡ PSNR này, với chất lượng ảnh giấu như nhau, phương pháp CPT giấu được 1044 byte. Do tăng chất lượng giấu tin chống phát hiện, phương pháp MCPTE giấu được 130 byte, với $PSNR = 78,2dB$. Cùng với chất lượng theo PSNR, phương pháp MCPT chỉ giấu được 95 byte. Để tăng chất lượng ảnh minh họa và khuôn khổ bài báo, ở đây chúng tôi chỉ đưa vào các ảnh xử lý theo CPTE, MCPTE. Trong dãy ảnh nhị phân minh họa dưới đây, ba ảnh bao gồm: ảnh gốc (ca sĩ nhí), ảnh đã giấu tin theo CPTE, ảnh đã giấu tin theo phương pháp MCPTE.



5. KẾT LUẬN

1) Các kết quả thực nghiệm cho thấy, trong hầu hết các trường hợp, tổng số bit có thể giấu được bởi thuật toán CPTE lớn gần gấp đôi so với thuật toán CPT và xấp xỉ với MSDR. Đối với bài toán giấu tin trong ảnh, một trong những thách thức đối với các thuật toán giấu tin là làm sao đạt được tỷ lệ giấu tin cao nhưng không làm giảm chất lượng của ảnh. Thuật toán MCPTE cho phép giấu tối đa $2r-2$ bit trong một khối điểm ảnh nhị phân F, nhiều gấp 2 lần so với phương pháp của Tseng-Pan (chỉ giấu được $r-1$ bit) trong khi chất lượng ảnh là tương đương.

2) Các ứng dụng khác: thuật toán CPTE có thể dễ dàng được mở rộng cho các ảnh palette (bảng màu) như ảnh GIF, ảnh BMP 8 bpp,... trong trường hợp ta cần chống các phương pháp tấn công phát hiện ảnh có giấu tin mật hay không, đặc biệt các phương pháp dựa trên histogram (xem ví dụ phận tích trong [6]: nếu tỷ lệ anpha của số các điểm ảnh được giấu tin trên tổng số điểm ảnh của một ảnh palette G nhỏ hơn 0.1, khi đó rất khó có thể đánh giá được G có chứa dữ liệu mật hay không). Áp dụng CPTE với mỗi palette, ta có thể đạt được một tỷ lệ alpha nhỏ với trong khi tổng số bit được giấu là đủ lớn cho các ứng dụng thực tế. Trong trường hợp, mỗi ảnh trong bảng màu có k "màu giống nhau" với $k > 2$, sử dụng các tính chất trong 3.1, 3.2 ta có thể giấu nhiều hơn số bit mật trong mỗi khối F của ảnh, chẳng hạn với ảnh 256 mức xám, có thể xét $k = 16$ (là 1/16 của 256 mức xám), khi đó Z_{16} sẽ thay cho Z_2 để đạt tỷ lệ giấu tin cao hơn nữa. Chi tiết những vấn đề này sẽ là nội dung phát triển của các công trình tiếp theo.

TÀI LIỆU THAM KHẢO

[1] Y.Chen, H.Pan, Y.Tseng, A secure of data hiding scheme for two-color images, *IEEE Symposium on Computers and Communications*, (2000).

[2] M.Y.Wu, J.H.Lee, Anovel data embedding method for two-color fascimile images, *Proceedings of international symposium on multimedia information processing*, Chung-Li, Taiwan, R.O.C,

1998.

[3] Negar Sadat Mirsattari, Parisa Haghani, Mansour Jamzad, Feature watermarking in digital documents for retrieval and authentication, *11th.International CSI Computer Conference CSICC 2006*, Iran, 2006.

[4] Y.-C. Tseng and H.-K. Pan, Secure and invisible data hiding in 2-color images, *Proceedings of INFOCOM 2001*, 2001 (887–896).

[5] HIOKI Hirohisa, A modified CPT scheme for embedding data into binary images, *Proc. of Pacific Rim Workshop on Digital Steganography 2003*, (Jul. 2003) 32-44.

[6] Xinpeng Zhang and Shuozhong Wang, *Analysis of Parity Assignment Steganography in palette Images*, R. Khosla et al. (Eds.): KES 2005, LNAI 3683, pp. 1025-1031, 2005. Springer-Verlag, Berlin- Heidelberg (2005).

[7] Nguyễn Hải Thanh, Phan Trung Huy, *Fast and near Optimal Parity Assignment in Palette Images with Enhanced CPT Scheme, LNCS/LNAI, 5991*, Springer, 2010 (pp.455–459) ISSN 0302-9743.

[8] C.C. Chang, T.D. Kieu, Y.C Chou, A high payload steganographic scheme based on (7,4) hamming code for digital images, *Electronic commerce and cecurity 2008 symposium* 2008 (16-21).

[9] Cheonsick Kim, Dongkyoo Shin, and Dongil Shin, *Data Hiding in a Halftone Image Using Hamming Code (15,11), ACIIDS 2011, LNAI 6592*, Springer-Verlag, Berlin Heidelberg, 2011 (372–381).

Nhận bài ngày 16 - 9 - 2011
Nhận lại sau sửa ngày 15 - 11 - 2011