MỘT GIẢI PHÁP MỚI CHIA SẺ BẢO MẬT THÔNG TIN

A NEW SOLUTION TO CONFIDENTIAL DATA SHARING

Võ Phước Hưng[1]

Tóm tắt

Bài báo đề xuất một giải pháp mới trong trong việc chia sẻ bảo mật thông tin, mỗi thông tin chia sẻ được xem là ảnh số, dựa trên lược đồ ngưỡng đầu tiên được đề xuất bởi Adi Shamir vào năm 1979. Tuy nhiên, để tăng cường tính bảo mật cho thông tin khi được lưu trữ hay chia sẻ trên môi trường mạng, phần thông tin ấy sẽ được mã hóa dựa trên hệ mật mã Hill. Kết quả tiến trình mã hóa sẽ áp dụng vào lược đồ ngưỡng-(t, n) đa thức Shamir để chia thành n mảnh nhỏ phân cho người dùng đầu cuối. Chỉ có thể tái hiện lại thông tin nếu có sự hợp tác của ít nhất t mẫu tin đã phân chia.

Từ khóa: chia sẻ bảo mật, mã hóa, mật mã học.

Abstract

This paper proposes a solution to confidential data sharing based on the intinial threshold histogram published by Adi Shamir in 1979. However, in order to enhance the confidentiality of information to be stored or shared on network, the data need to be encrypted based on the Hill cryptography. After that, the result of the cipher text will be shared with n end-user based on Shamir's polynomial (t, n)-threshold histogram. Only can the information be recovered when the collaboration of any t or more of n authorized participants.

Keywords: confidential sharing, encryption, cryptography.

1. Giới thiệu

Tốc độ phát triển mạnh mẽ của hạ tầng mạng Internet cùng giá thành các thiết bị máy tính và mạng máy tính ngày càng giảm đã làm một cuộc cách mạng trong giao thức xử lý thông tin và truyền tải thông tin. Việc lưu trữ, xử lý thông tin bằng các thiết bị tính toán (PC, laptop, smartphone, tablet, camera…) và chia sẻ chúng qua môi trường mạng ngày càng trở nên phổ dụng. Sự phát triển của mạng Internet ở Việt Nam được xem là nền tảng, động lực cho sự phát triển thương mại điện tử, giáo dục, y tế… Tuy nhiên, như chúng ta biết, Internet là một hệ thống mạng mở, toàn cầu, trong đó môi trường truyền thông thông tin được xem là không an toàn. Trong khi yêu cầu của người dùng mỗi khi tiếp nhận cũng như truyền tin là phải an toàn và chính xác. Vì vậy, việc lưu trữ và truyền tải dữ liệu phải được giữ bí mật đối với người không được phép là một yêu cầu bắt buộc của người thiết kế hệ thống thông tin.

Việc bảo mật thông tin được đặt ra từ rất sớm, chẳng hạn trong (Liu C.L 1968) đưa ra vấn đề: Có 11 nhà khoa học cùng làm chung một dự án bí mật, họ mong muốn rằng toàn bộ hồ sơ của dự án được lưu giữ trong một cái hộp. Hộp này chỉ có thể mở ra nếu như có sự hợp tác đủ ít nhất 6/11 nhà khoa học. Vậy hỏi, số ổ khóa và chìa khóa ít nhất mà mỗi nhà khoa học đề cập trên cần phải có là bao nhiêu? Không khó để có lời giải cho bài toán này là mỗi nhà khoa học phải mang theo 462 ổ khóa và 252 chìa khóa. Tuy nhiên, ngày nay, đây là một lời giải không thực tế, và nó sẽ tăng theo lũy thừa khi số lượng nhà khoa học tham gia cùng dự án tăng lên.

Năm 1979, (A. Shamir) đề xuất một phương pháp để giải quyết bài toán nêu trên gọi là chia sẻ bí mật (secret sharing). Secret sharing là phương pháp chia sẻ thông tin bí mật thành hai hay nhiều phần (share/shadow), mà mỗi phần sẽ do một người nắm giữ. Và thông tin bí mật ấy chỉ có thể khôi phục khi có sự hợp tác của tối thiểu một số lượng người đã định trước. Một cách logic, mỗi phần chia là một phần của thông tin, nhưng phần thông tin đó là vô nghĩa nếu như chúng đứng riêng lẻ.

Chia sẻ bí mật là một giải pháp quan trọng trong lĩnh vực bảo mật thông tin, là kỹ thuật cho phép tạo ra nhiều bóng tin (shadow data) hay còn gọi là thông tin chia sẻ (shared data) của thông tin gốc mà mỗi bóng tin là hiển thị thông tin không có giá trị. Tuy nhiên, khi tập hợp đủ số lượng thông tin chia sẻ cần thiết thì thông tin gốc ban đầu sẽ được phục hồi. Bài báo này sẽ tập trung nghiên cứu giải pháp chia sẻ bí mật thông tin mà mỗi thông tin gốc ở đây được xem là một tập tin hình ảnh (image). Ảnh thông tin bí mật (secret image) sẽ được mã hóa trước khi phân mảnh. Điều này giúp tăng cường tính bảo mật cho ảnh thông tin cần giữ bí mật.

[1] *Thạc sĩ, Trường Đại học Trà Vinh*

2. Cơ sở lý thuyết

2.1. Tập các số nguyên (Set of Integers)

- Tập hợp các số nguyên, được ký hiệu là **Z**, là tập các số nguyên (không chứa số phân số) có miền xác định từ -∞ đến +∞

Z = {…, -2, -1, 0, 2, …}

- Tập các số dư nguyên, được ký hiệu là $\mathbf{Z}_n$, là kết quả của phép toán modulo với *n*.

Khi đó $\mathbf{Z}_n$ = {0, 1, …, *n*-1}

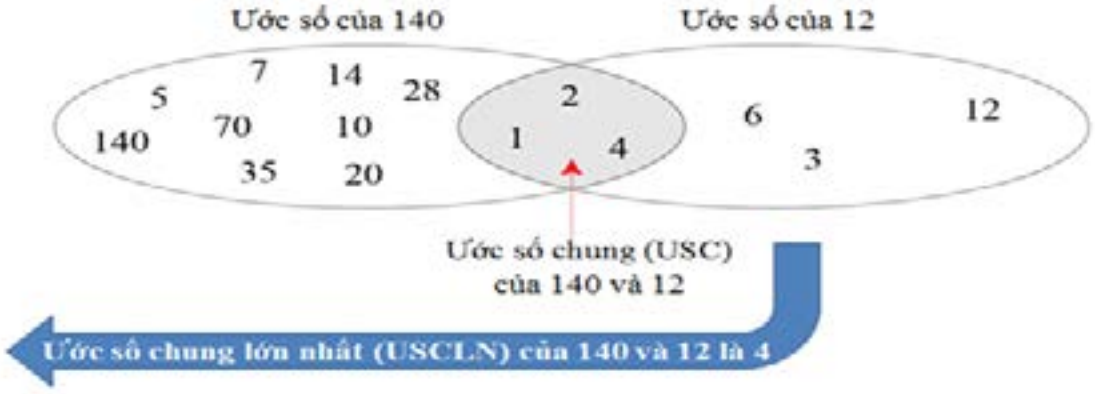
Ví dụ: ©

Z_2 = {0, 1}; Z_6 = {0, 1, …, 5} ; Z_{11} = {0, 1, …, 10}

2.2. Thuật toán Euclid [William Stalling]

Hai số nguyên dương *a* và *b* có thể có nhiều ước số, nhưng chỉ có một số chung là lớn nhất.

Ví dụ:



Như vậy, tìm USCLN của 2 số *a* và *b* là liệt kê tất cả ước số của mỗi số *a* và *b*, sau đó tìm tập giao USC của 2 số và rút ra USCLN cùa 2 số *a* và *b*. Rõ ràng với cách này là không thực tế khi 2 số *a*, *b* lớn. Thật may mắn, cách đây hơn 2000 năm, nhà toán học tên là Euclid đã phát triển một thuật toán có thể giúp ta tìm USCLN của 2 số nguyên dương. Thuật toán Euclid để tìm USCLN(*a*,*b*) có thể được mô tả như sau:

```
USCLN(a,b)
{    r1=a; r2=b;
          While (r2>0)
          {        q=⌊a/b⌋;
                   r=r1-q*r2;
                   r1=r2; r2=r;
          }
          return r1;
}
```

2.3. Nghịch đảo nhân (Multiplicative Inverse)

Trong tập Z_n, hai số *a* và *b* được gọi là nghịch đảo nhân của nhau nếu:

$$a \times b \equiv 1 \pmod{n}$$

Ví dụ:

Nếu giá trị modulus *n* = 10, thì nghịch đảo nhân của 3 trong Z_{10} là 7, vì:

$$(3 \times 7) \bmod 10 = 1$$

2.4. Mật mã Hill [William Stalling]

Mật mã Hill do nhà toán học người Mỹ tên là Lester S. Hill đề xuất năm 1929. Ý tưởng của giải thuật mã hóa Hill là lần lượt lấy *m* ký tự liên tiếp trong bản rõ (Plaintext) để thay thế bởi *m* ký tự mã hóa. Tiến trình thay thể được xác định bởi *m* phương trình tuyến tính.

Quá trình mã hóa Hill (Encoded Hill Cipher)

Giả sử *m*=3, ta có hệ 3 phương trình tuyến tính như sau:

$$\begin{cases} c_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod n \\ c_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod n \\ c_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod n \end{cases} \quad (1)$$

hay

$$(c1\ c2\ c3) = (p1\ p2\ p3)\begin{pmatrix} k11 & k12 & k12 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix} \bmod n$$

hay C = E(P,K) = PK (mod *n*); trong đó E là hàm

mã hóa, P là ký tự rõ, K là ma trận khóa, C là mật mã.

Quá trình giải mã Hill (Decoded Hill Cipher)

P' = D(K, C) = CK^{-1} mod n = PKK^{-1} = PI = P,

Trong đó: $\mathbf{K^{-1}}$ là ma trận nghịch đảo của ma trận **K**,

I là ma trận đơn vị.

2.5. Lược đồ ngưỡng Shamir

Khái niệm chia sẻ bí mật đầu tiên được giới thiệu vào năm 1979 bởi Shamir [1] và được gọi là lược đồ ngưỡng (t, n); trong đó n là số thành viên tham gia vào hệ thống, t là số thành viên tối thiểu (ngưỡng) cùng tham gia để phục hồi thông tin mật. Lược đồ Shamir dựa trên hàm đa thức bậc $t-1$ được định nghĩa như sau:

$$f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \bmod p \quad (2)$$

để mã hóa chia sẻ bí mật s thành n mảnh/phần chia (shadow/share), ký hiệu là $s_1, s_2, \ldots, s_n$, với p là số nguyên tố và các hệ số $a_1, a_2, \ldots, a_{t-1}$ được lựa chọn ngẫu nhiên sao cho $a_i \in [0, p-1]$. Chọn n số nguyên $x_1, x_2, \ldots, x_n$ khác nhau từng đôi một, tương trưng cho n thành phần tham gia vào hệ thống. Các phần chia $s_1, s_2, \ldots, s_n$ được tính $s_i = f(x_i)$, với $i = \overrightarrow{1..n}$. Khi đó mỗi thành phần tham gia vào hệ thống được chia sẻ cặp (x_i, s_i).

s chỉ có thể được khôi phục khi tập hợp đủ ít nhất t phần chia (share) (có ít nhất t cặp (x_i, s_i)) và áp dụng vào đa thức nội suy Lagrange:

$$f(x) = \sum_{i=1}^{t} \left(s_i \times \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)} \right) \bmod p \quad (3)$$

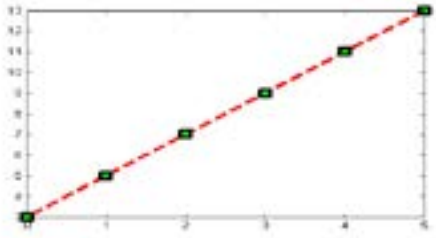
Ví dụ:

Lược đồ ngưỡng (t, n)=(2,3) với giá trị bí mật s=3, chọn p=11, từ (2), ta có:

$f(x)$ = 3+2x mod 11.

Nếu ta chọn x_1=1, x_2=2, x_3=3, $f(1)$=1, $f(2)$=2, $f(3)$=3, theo đó 3 phần chia tương ứng là: (1,5), (2,7), (3,9).

Thật ra chúng là những điểm trên đồ thị (Hình 1) của phương trình $f(x)$ = 3+2x mod 11.



Hình 1: Đồ thị f(x)=3+2x

Để khôi phục lại giá trị bí mật s, ta phải tập đủ ít nhất 2 phần trong 3 phần chia. Chẳng hạn, ta có 2 phần chia: (1,5) và (2,7).

Từ công thức (3):

$$f(x) = s_1 \frac{(x - x_2)}{(x_1 - x_2)} + s_2 \frac{(x - x_1)}{(x_2 - x_1)}$$

ta được:

$$f(x) = 5\frac{(x-2)}{(1-2)} + 7\frac{(x-1)}{(2-1)} = -5(x-2) + 7(x-1) = 3 + 2x$$

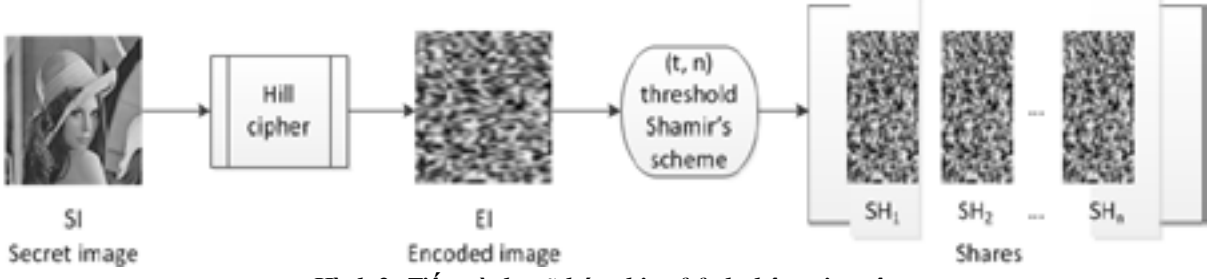
suy ra, s=3.

3. Giải pháp đề xuất

Một hệ mật mã luôn bao gồm hai tiến trình: mã hóa và giải mã. Giải pháp chia sẻ bảo mật thông tin với phần thông tin được xem là ảnh số đề xuất trong nghiên cứu này bao gồm tương ứng hai tiến trình như vậy: (1) tiến trìnhmã hóa chia sẻ ảnh thông tinmật (ảnh bí mật – Secret image) và (2) tiến trình khôi phục ảnh thông tin (Recovered image).

3.1. Tiến trình mã hóa chia sẻ ảnh thông tin mật

Trong tiến trình này, để tăng tính bảo mật cho ảnh bí mật (SI – secret image) cần chia sẻ, ta mã hóa SI dựa trên phương pháp hóa Hill, với ma trận vuông khóa K cấp (2×2) được lựa chọn ngẫu nhiên sao cho có tồn tại ma trận nghịch đảo K^{-1} theo modulo cường độ điểm ảnh. Như sơ đồ được mô tả trong Hình 2, ảnh thu được sau khi được mã hóa là EI sẽ áp dụng lược đồ ngưỡng (t, n) của Shamir. Theo cách này, ảnh EI sẽ phân chia thành n mảnh khác nhau ký hiệu là $SH_1, SH_2, \ldots, SH_n$.



Hình 2: Tiến trình mã hóa chia sẻ ảnh thông tin mật

Chi tiết của tiến trình này có thể được mô tả như sau:

a. *Giai đoạn mã hóa ảnh thông tin mật*

Bước 1: Chia ảnh đa cấp xám gồm có 256 cấp xám (ảnh xám) SI với kích thước (m×n) thành những khối (blocks) gồm 2 điểm ảnh (pixel) theo nguyên tắc trái-phải-trên-dưới. Nếu SI là ảnh màu true-color, ta tách lớp ảnh SI thành 3 lớp (layer) SI_R, SI_G, SI_B và thực hiện từng lớp ảnh như một đa cấp ảnh xám.

Bước 2: Lấy lần lượt từng khối 2 điểm ảnh (p_1, p_2) áp dụng vào công thức (1) với modulo 256 (giá trị mỗi điểm ảnh xám là 8 bits), tạo thành công thức mã hóa ảnh như sau:

$$\begin{aligned} p_1' &= (k_{11}p_1 + k_{12}p_2) \bmod 256 \\ p_2' &= (k_{21}p_1 + k_{22}p_2) \bmod 256 \end{aligned} \quad (4)$$

Với p_1' và p_2' là những điểm ảnh bị mã hóa (encoded pixel); k_{11}, k_{12}, k_{21}, k_{22}, là những khóa dùng để mã hóa theo phương pháp Hill.

Ví dụ: Giả sử ta có ma trận điểm ảnh SI như sau:

Bảng 1: Ma trận ảnh SI

42	60	93	103	83	84
41	51	91	108	84	83
43	51	86	106	79	74
41	54	85	98	70	68
38	49	82	95	71	73
39	51	82	93	73	74

Khóa được chọn là:

$$K = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix},$$

- Khối ảnh đầu tiên để mã hóa là $(p_1, p_2) = (42,60)$

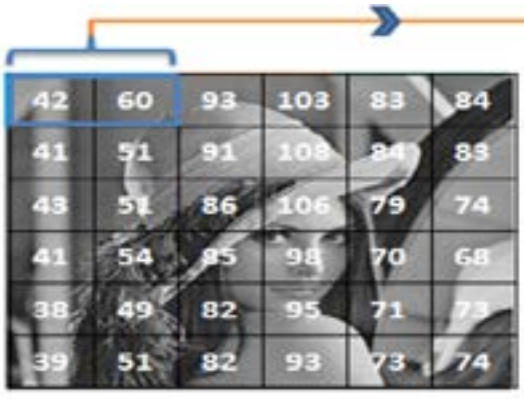
$$p_1' = (5\times42 + 8\times60) \bmod 256$$

$$p_2' = (17\times42 + 3\times60) \bmod 256$$

Áp dụng vào (4):

Ta có: $p_1' = 178$ và $p_2' = 126$.

Tiếp tục lấy những khối ảnh kế tiếp để mã hóa, cuối cùng ta nhận được ảnh mã hóa **EI** như hình 3.



(SI)

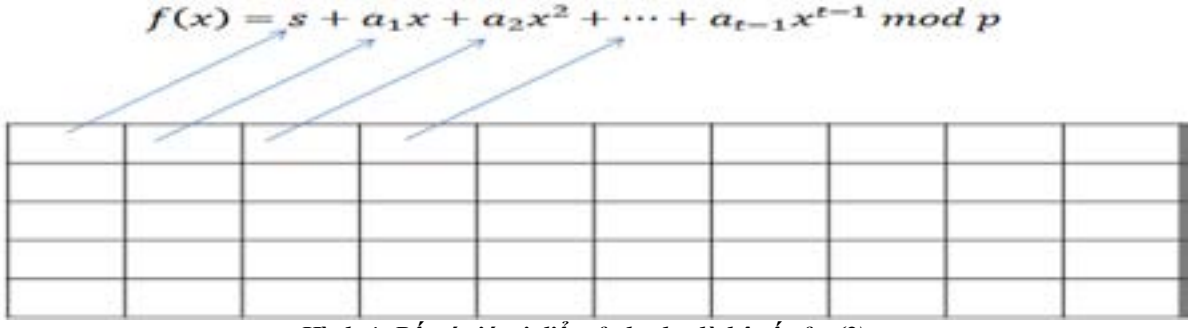
178	126	9	98	63	127
101	82	39	79	60	141
111	116	254	244	219	29
125	91	185	203	126	114
70	25	146	143	171	146
91	48	130	137	189	183

(EI)

Hình 3: Ảnh mã hóa EI từ SI

b. *Giai đoạn chia sẻ*

Như được mô tả ở Hình 2, sau khi mã hóa ảnh SI, ta thu được ảnh mã hóa EI. Tiếp theo của tiến trình này là chia sẻ ảnh mã hóa EI thành những phần chia (shares) dựa trên lược đồ ngưỡng (t, n) của Shamir. Trong giai đoạn này, chúng tôi xem giá trị các pixels như các hệ số $\{s, a_1, a_2, \ldots, a_{t-1}\}$ của đa thức (2) như Hình 4 và số nguyên tố $p = 251$ là số nguyên tố lớn nhất nhỏ hơn 255 (giá trị lớn nhất của điểm ảnh xám) [Hung P. Vo].



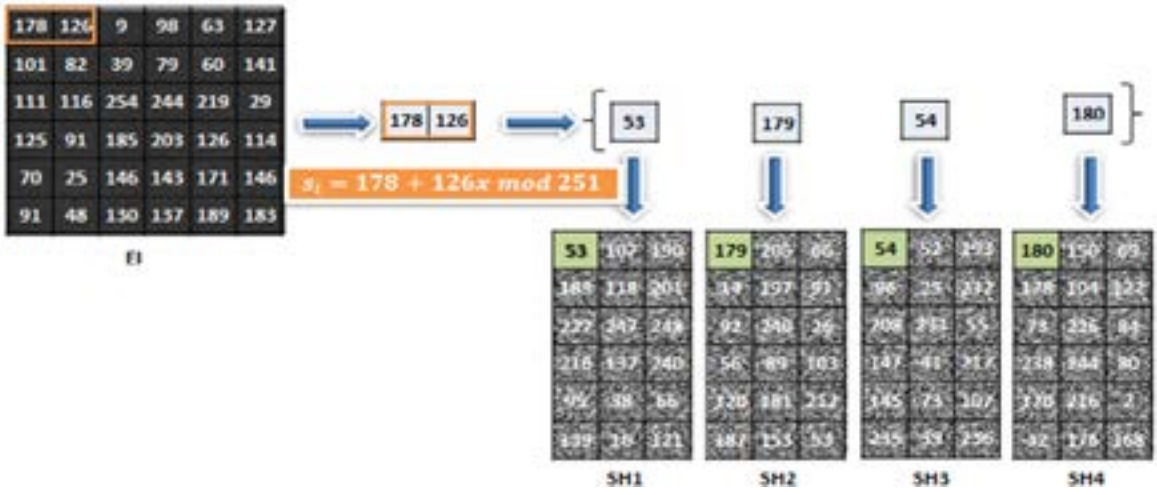
Hình 4: Bố trí giá trị điểm ảnh như là hệ số của (2)

Theo đó, ảnh EI kích thước (m×n) sẽ bị chia thành (m×n)/t khối, mỗi khối có t điểm ảnh tương ứng với các hệ số $\{s, a_1, a_2, \ldots, a_{t-1}\}$ của công thức (2). Và kết quả đa thức này ta thu được n giá trị $s_1=f(x_1)$, $s_2=f(x_2)$, …, $s_n=f(x_n)$, trong đó x_1, x_2, …, x_n được định ngẫu nhiên (xem như mã số của từng thành phần tham gia vào hệ thống) và khác nhau từng đôi một. Các giá trị s_1, s_2, ..s_n phân bố một cách tương ứng vào n ảnh chia sẻ (shadow image) ký hiệu là: SH_1, SH_2, …, SH_n. Và kích thước mỗi ảnh chia sẻ bằng 1/t kích thước ảnh EI.

Để mô tả giai đoạn chia sẻ ảnh, ta tiếp ví dụ ở phần trên (Hình 3), với ngưỡng (2, 4), có nghĩa là t=2, n=4. Như vậy hàm đa thức được thiết lập như sau đối với cặp điểm ảnh đầu tiên (178, 126):

$$f(x) = (178 + 126x) \bmod 251 \quad (5)$$

Chọn ngẫu nhiên 4 giá tri x khác nhau, tượng trưng mã số của bốn (n=4) thành viên tham gia vào hệ thống và thay vào (5), chẳng hạn x={1, 2, 3, 4}. Kết quả là ta nhận được 4 điểm chia sẻ (1, 53); (2, 179); (3, 54); (4, 180). Bốn điểm chia sẻ này trở thành điểm ảnh đầu tiên của mỗi 4 ảnh chia sẻ SH_1, SH_2, SH_3, SH_4. Điểm ảnh thứ 2 của mỗi ảnh chia sẻ SH_i (i=1..4) được tính tương tự như trên. Hình 5 mô tả chi tiết tiến trình chia sẻ ảnh dựa trên lược đồ ngưỡng Shamir.

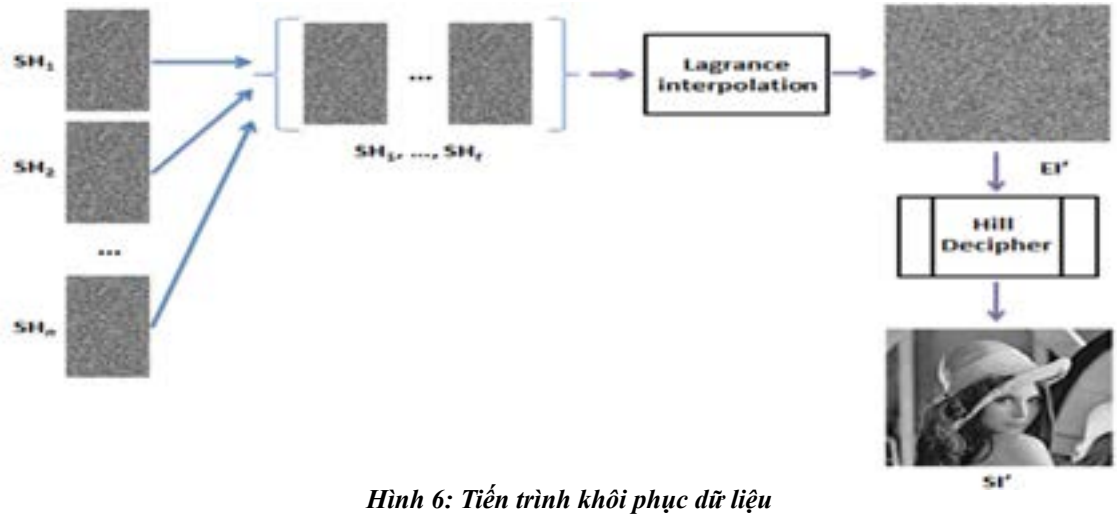


Hình 5: Giai đoạn chia sẻ ảnh

Mỗi ảnh chia SH_i có kích thước bằng 1/2 kích thước của ảnh EI, trong đó không ảnh SH_i nào hiển thị thông tin của ảnh gốc.

3.2. Tiến trình khôi phục ảnh thông tin

Tiến trình khôi phục dữ liệu được thực hiện ở phía người nhận, có nghĩa là dữ liệu sau khi được mã hóa, chia sẻ sẽ gửi cho n người nhận qua phương tiện truyền thông. Tiến trình này bao gồm hai giai đoạn: khôi phục và giải mã dữ liệu, tiến trình có thể được tóm tắt như Hình 6. Giai đoạn thứ nhất kết nối t ảnh chia sẻ dựa trên đa thức nội suy Lagrance, tiếp theo giai đoạn giải mã theo phương pháp Hill. Chi tiết của tiến trình được trình bày như sau:



Hình 6: Tiến trình khôi phục dữ liệu

a. *Giai đoạn khôi phục ảnh*

Đối với lược đồ (t,n)-ngưỡng của Shamir, thông tin được phục hồi là sự hợp tác của t thành phần tham gia vào hệ thống; hay nói cách khác, phải tập hợp đủ ít nhất bất kỳ t ảnh chia sẻ của n mẫu chia. Khi đó ảnh mã hóa EI' được khôi phục 100% chính xác bởi đa thức nội suy Lagrance, công thức (3).

Từng bước của giai đoạn mô tả như sau:

Bước 1: Lấy điểm ảnh đầu tiên chưa được sử dụng của mỗi t ảnh chia sẻ.

Bước 2: Áp dụng t điểm ảnh này vào đa thức (3) để tìm các hệ số $a_0, a_1, \ldots, a_{t-1}$. Khi đó các hệ số $a_0, \ldots, a_{t-1}$ sẽ tương ứng với các điểm ảnh của ảnh mã hóa EI'.

Bước 3: Lặp lại bước 1 và bước 2 cho đến khi tất cả các điểm ảnh của t ảnh chia sẻ được thực hiện.

b. *Giai đoạn giải mã ảnh*

Dùng phương pháp giải mã Hill đối với ảnh mã hóa EI' để giải mã ảnh bí mật theo các bước được mô tả như sau:

Bước 1: Chia ảnh mã hóa EI' thành từng khối 2 điểm ảnh theo quy tắc trái-phải-trên-dưới.

Bước 2: Lấy lần lượt từng cặp điểm ảnh $(p_1^{EI'}, p_2^{EI'})$.

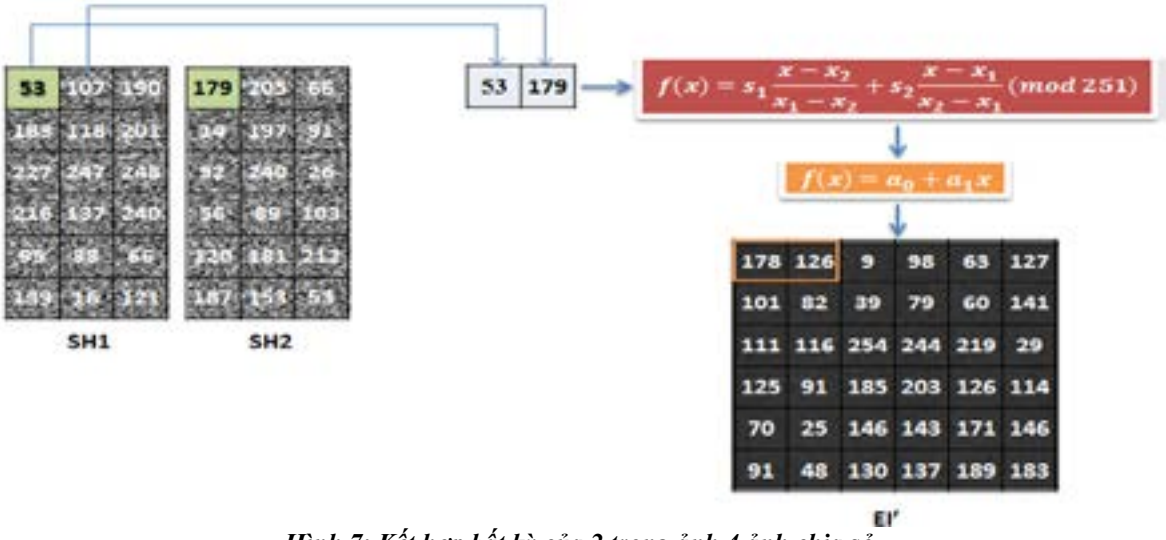
Bước 3: Áp dụng hàm giải mã Hill đối với 2 vừa lấy ở bước 2.

$$\begin{pmatrix} p_1^{SI'} \\ p_2^{SI'} \end{pmatrix} = \begin{pmatrix} p_1^{EI'} \\ p_2^{EI'} \end{pmatrix} K^{-1} \bmod 256$$

trong đó K^{-1} là ma trận nghịch đảo của K.

Bước 4: Lặp lại từ bước 2 đến 3 cho đến khi tất cả khối điểm ảnh được giải mã.

Để diễn giải cho tiến trình khôi phục và giải mã ảnh thông tin gốc, ta sử dụng ví dụ bên trên, Hình 5. Giả sử 2 trong 4 ảnh chia sẻ được chọn là SH1 và SH2 để hợp tác cùng khôi phục ảnh theo lược đồ ngưỡng (2, 4) của Shamir. Hình 7 mô tả giai đoạn khôi phục ảnh.



Hình 7: Kết hợp bất kỳ của 2 trong ảnh 4 ảnh chia sẻ

- Lấy lần lượt từng điểm của mỗi ảnh chia sẻ (SH1, SH2), kết hợp nhau để khôi phục lại ảnh mã hóa EI'. Như vậy cặp điểm ảnh đầu tiên của ảnh mã hóa EI' được phục hồi qua cặp điểm ảnh (1,53) và (2,179) và đa thức nội suy Lagrance (3):

$$f(x) = s_1 \frac{x-x_2}{x_1-x_2} + s_2 \frac{x-x_1}{x_2-x_1} (mod\ 251)$$

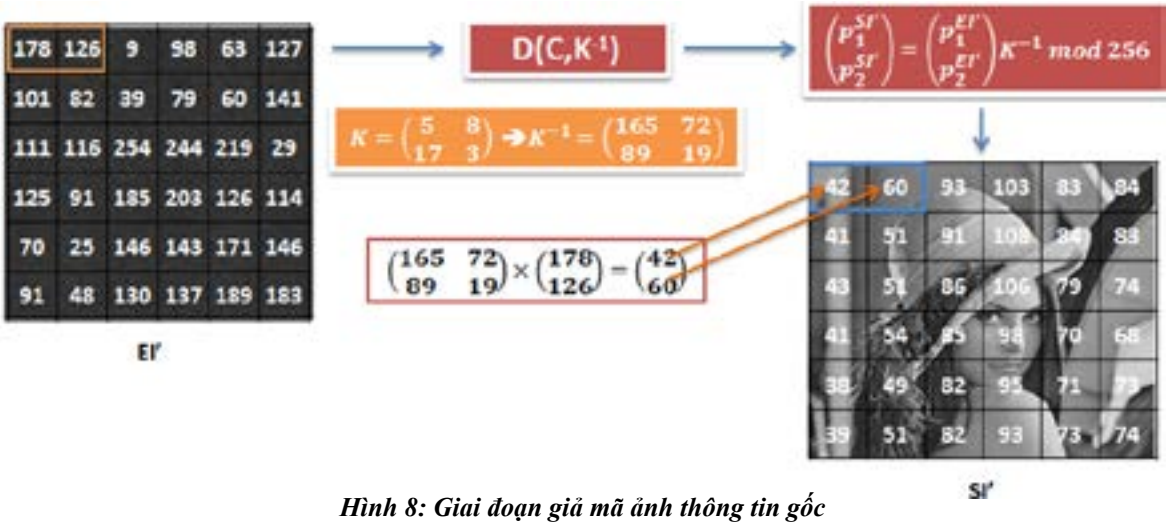
$$\rightarrow f(x) = 53\frac{x-2}{1-2} + 179\frac{x-1}{2-1} (mod\ 251) = (-73 + 126x)\ mod\ 251$$

$$= 178 + 126x$$

➔ cặp điểm ảnh thứ nhất của EI' là $(p_1^{EI'}, p_2^{EI'})$ =(178, 126).

Tiến trình khôi phục ảnh EI' được tiếp tục cho đến khi tất cả điểm ảnh của 2 ảnh chia sẻ SH1 va SH2 được thực hiện.

- Sau khi nhận được ảnh mã hóa EI', ta phải giải mã để có được ảnh thông tin mật ban đầu. Hình 8 trình bày sơ đồ giải mã ảnh thông tin dựa trên hệ mật mã Hill.

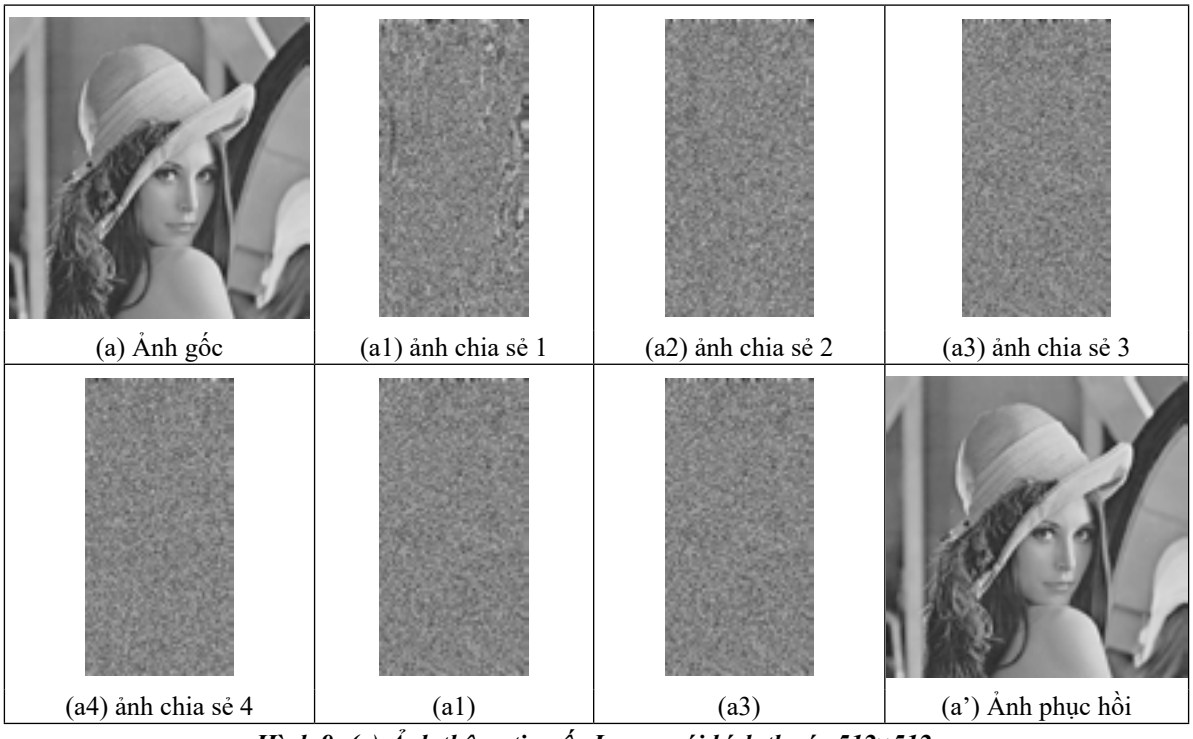


Hình 8: Giai đoạn giả mã ảnh thông tin gốc

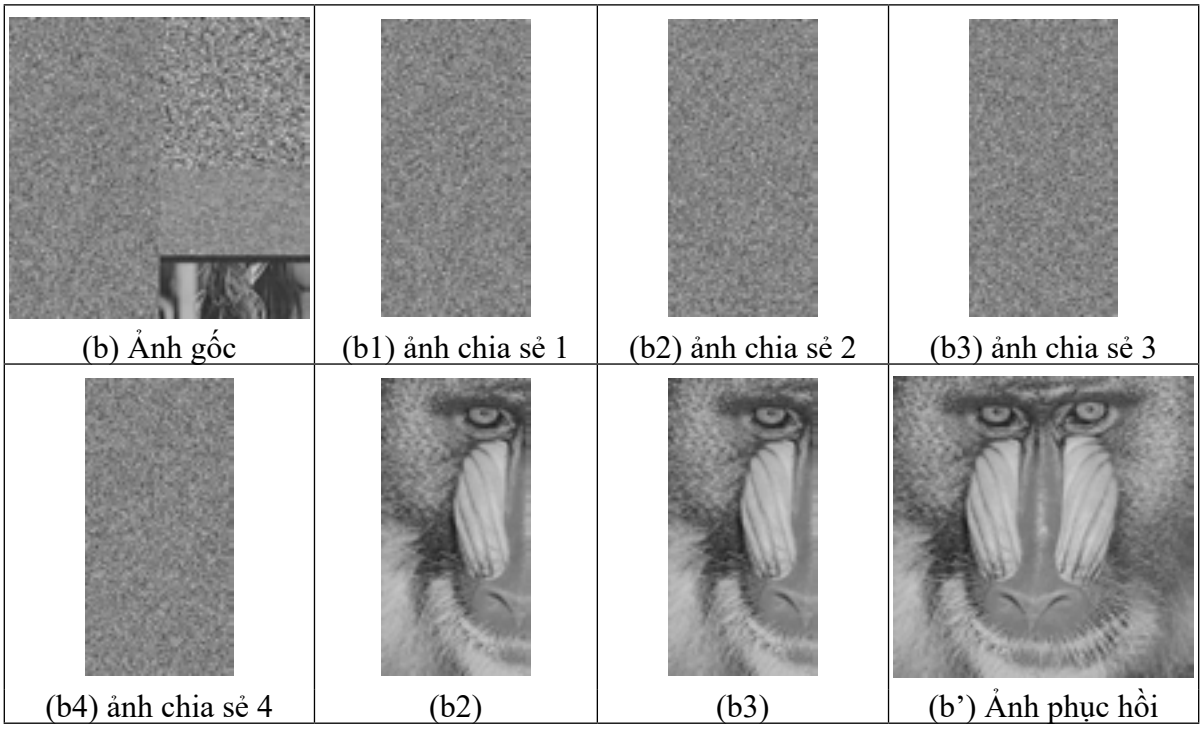
4. Kết quả thực nghiệm

Để chạy thực nghiệm chương trình, chúng tôi xây dựng một bộ sưu tập với trên 100 ảnh với kích thước 512×512 với hai thể loại ảnh chính là ảnh xám (gray-scale image) và ảnh màu RGB (true-color image). Tuy nhiên, trong bài báo này, chúng tôi chỉ ghi nhận lại một số kết quả để chứng minh cho giải pháp được đề xuất phần 2.

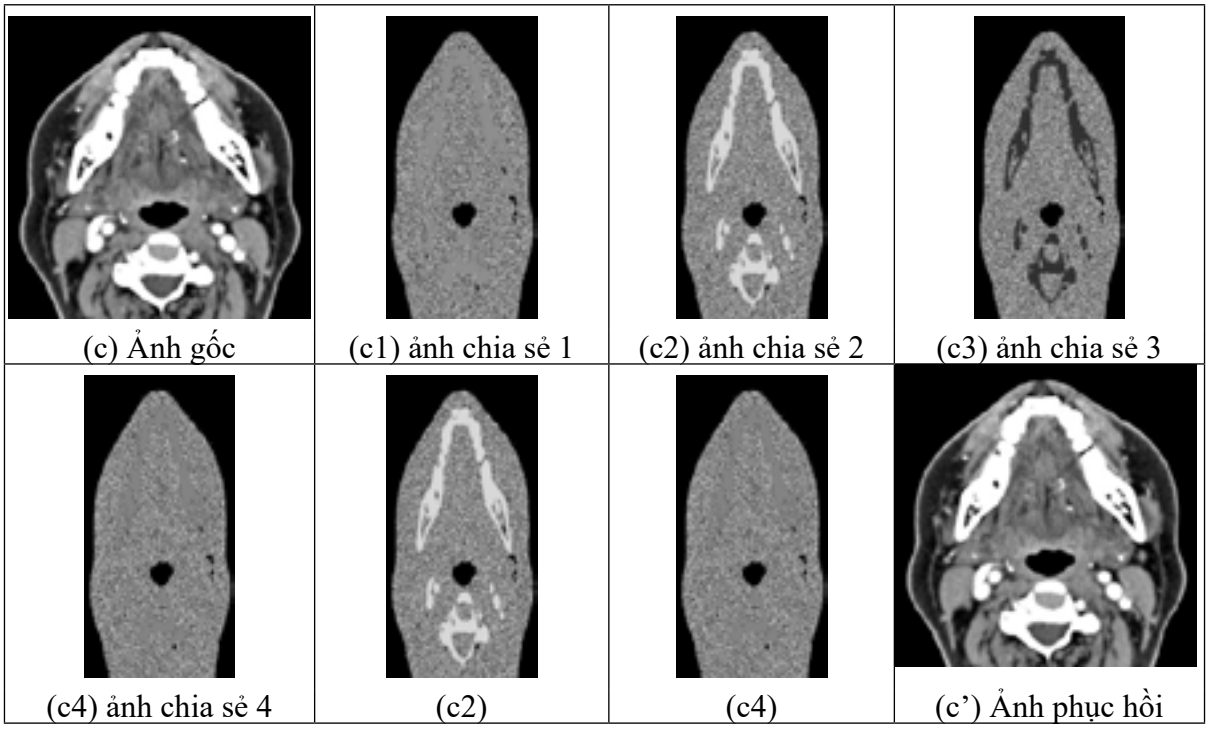
Trong phần một của thực nghiệm này, chúng tôi chỉ ghi nhận kết quả của một số ảnh xám được sử dụng để mã hóa bằng phương pháp Hill với tập khóa (k_{11}, k_{12}, k_{21}, k_{22}) tương ứng theo thứ tự là (5, 8, 17, 3), và chia sẻ theo lược đồ ngưỡng (2, 4) của Shamir. Các kết quả được thể hiện như ở các Hình 9, 10 và 11.



Hình 9: (a) Ảnh thông tin gốc Lenna với kích thước 512×512, (a1) ->(a4) bốn ảnh chia sẻ với kích thước (512×256), (a') ảnh phục hồi từ 2 ảnh (a1) và (a3).

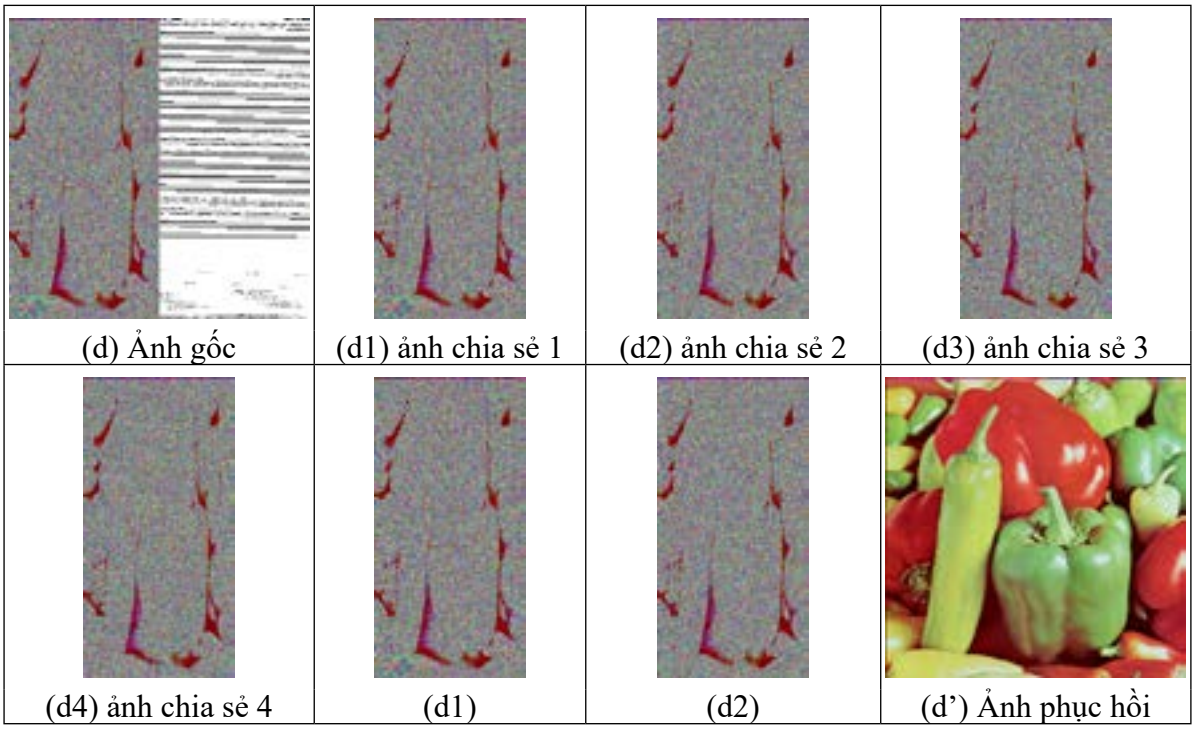


Hình 10: (b) Ảnh gốc Baboon với kích thước 512×512, (b1) ->(b4) bốn ảnh chia sẻ với kích thước (512×256), (b') ảnh phục hồi từ 2 ảnh (b2) và (b3).

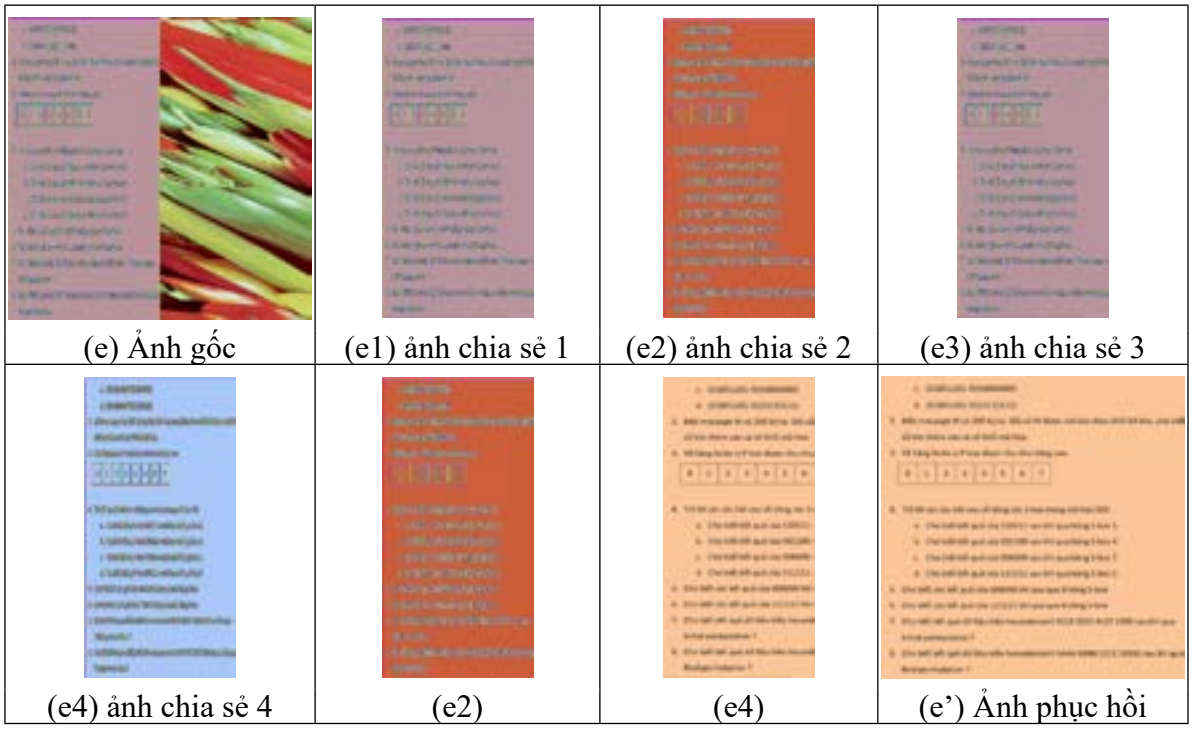


Hình 11: (c) Ảnh gốc Medicine với kích thước 512×512, (c1) ->(c4) bốn ảnh chia sẻ với kích thước (512×256), (c') ảnh phục hồi từ 2 ảnh (c2) và (c4).

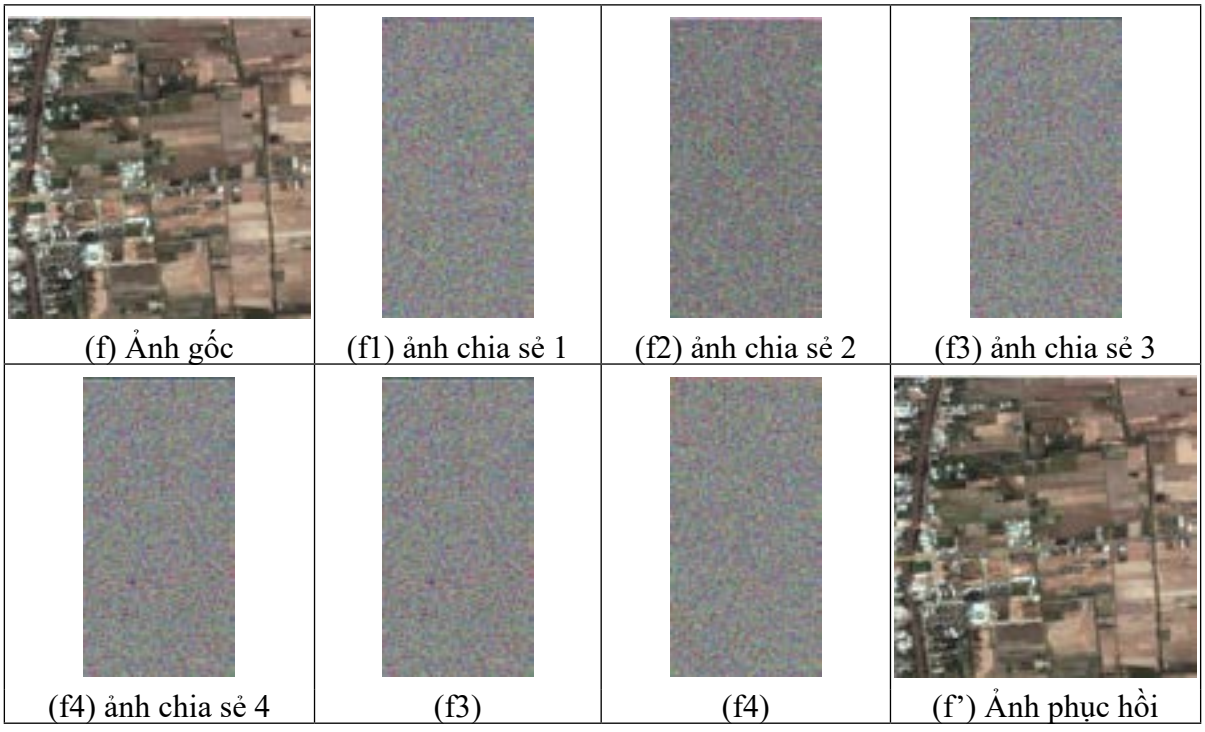
Tiếp theo, ở phần hai của thực nhiệm, báo cáo lược ghi một vài kết quả trên tập ảnh màu RGB. Các kết quả lần lượt được thể hiện qua các Hình 12, 13 và 14.



Hình 12: (d) Ảnh gốc Pepper với kích thước 512×512, (d1) ->(d4) bốn ảnh chia sẻ với kích thước (512×256), (d') ảnh phục hồi từ 2 ảnh (d1) và (d2).



Hình 13: (e) Ảnh gốc Text với kích thước 512×512, (e1) ->(e4) bốn ảnh chia sẻ với kích thước (512×256), (e') ảnh phục hồi từ 2 ảnh (e2) và (e4).



Hình 14: (f) Ảnh gốc TVUmap với kích thước 512×512, (f1) ->(f4) bốn ảnh chia sẻ với kích thước (512×256), (f') ảnh phục hồi từ 2 ảnh (f3) và (f4).

5. Kết luận

Chúng tôi áp dụng phương pháp mã hóa Hill vào ảnh bí mật trước khi áp dụng lược đồ ngưỡng Shamir vào việc chia sẻ ảnh. Ma trận khóa của phương pháp Hill có thể ghép vào chương trình hoặc truyền tải riêng trên kênh bí mật nhằm tăng độ phức tạp đối với việc thám mã.

Đối với thuật toán chia sẻ ảnh theo ngưỡng (*t*, *n*), nếu muốn khôi phục ảnh bí mật, ta phải xây dựng $\frac{m\times n}{t}$ đa thức theo dạng:

$$f_i(x_0) = a_0^i + a_1^i x_0 + \cdots + a_{t-1}^i x_{t-1}^i (mod\ 251)$$

cho ảnh có kích thước (*m*×*n*). Mỗi đa thức có *t* biến số $a_0^i, a_1^i, \ldots, a_{t-1}^i$.

Như vậy việc lựa chọn ngưỡng *t* là tùy thuộc và hệ thống của chúng ta cần có sự hợp tác của bao nhiêu người để khôi phục lại ảnh gốc trong tổng số *n* người tham gia hệ thống. Tuy nhiên, với việc lựa *t* càng lớn và không vượt quá *n* thì số lượng đa thức bậc *t*−1 sẽ giảm và khi đó độ phức tạp tính toán của mỗi đa thức sẽ tăng theo.

Giải pháp đề xuất chia sẻ ảnh thông tin mật thành nhiều ảnh nhỏ với ngưỡng (2, 4), như theo các kết quả thực nghiệm, mỗi ảnh chia sẻ chỉ bằng ½ ảnh thông tin gốc ban đầu, điều này giúp tăng tốc độ truyền tải dữ liệu qua môi trường Internet. Hơn nữa, trong quá trình lưu trữ hay truyền thông nếu có xảy ra mất bất kỳ ảnh chia sẻ nào, ta vẫn có thể phục hồi ảnh gốc thông qua bất kỳ hai ảnh chia sẻ.

Tài liệu tham khảo

A. Shamir. 1979. "How to share a secret".*Communications of the ACM*, Vol. 22, no.11, pp. 612–613.

Hung P. Vo. 2013. "A user-friendly image sharing scheme using JPEG-LS prediction and LSB matching function", *International journal of Modern Engineering research (IJMER),* Vol.3, Issue.1, pp. 139-148.

Liu C.L. 1968. "Introduction to Combinatorial Mathematics". *McGraw-Hill, New York.*

William Stalling. "*Cryptography and Network Security Principles and Practice*", 5th Edition.