NGHIÊN CỨU MÔ HÌNH GIẤU THÔNG TIN TRONG MÔI TRƯỜNG THƠ

RESEARCH MODELS OF HIDING INFORMATION IN THE POEMS ENVIRONMENT

Ninh Văn Thọ[1,*]

DOI: http://doi.org/10.57001/huih5804.2024.125

TÓM TẮT

Hiện nay với sự phát triển mạnh mẽ của công nghệ thông tin trên toàn cầu Intenet là một lĩnh vực không thể thiếu đối với cuộc sống hiện đại, nó đã làm thay đổi tư duy và cách tiếp cận của con người với mọi lĩnh vực khoa học kỹ thuật. Trong đó bảo mật về quá trình trao đổi thông tin trên không gian mạng là vấn đề hết sức cấp bách và cần thiết, bởi vì những thông tin trên mạng Intenet dù ở dạng lưu trữ hay truyền tải đều phải được an toàn và bảo. Vậy trong bài báo này tác giả sử dụng phương pháp mã hóa thông tin giải mã thông tin dựa vào môi trường thơ và là thơ lục bát.

Từ khóa*: Giấu thông tin, khôi phục thông tin, thơ, thuật toán, khóa.*

ABSTRACT

Currently with the strong development of information technology globally, Internet is an indispensable field for modern life, it has changed people's thinking and approach to all fields of science. technical study. In particular, the security of the process of exchanging information in cyberspace is a very urgent and necessary issue, because the information on the Internet, whether stored or transmitted, must be safe and protected. So, in this paper, the author uses the method of encoding information to decode information based on the poetic environment and hexagonal poetry.

Keywords*: Hiding information, retrieve information, algorithms, poems, keys.*

[1]Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

[*]Email: nvtho@uneti.edu.vn

Ngày nhận bài: 10/8/2023

Ngày nhận bài sửa sau phản biện: 26/12/2023

Ngày chấp nhận đăng: 25/4/2024

1. GIỚI THIỆU

Hiện nay có nhiều cách để bảo mật thông tin, tuy nhiên trong nghiên cứu này, tác giả sử dụng phương pháp giấu thông tin trong môi trường văn bản. Lượng thông tin đã được số hóa cùng với thông tin văn bản tức là người sử dùng đã giấu thông tin cần được bảo mật vào một đối tượng dữ liệu khác. Tức là môi trường giấu thông tin sao cho sự biến đổi của môi trường sau khi giấu tin khó có thể phát hiện ra và sau đó người sử dụng có thể lấy lại được các thông tin đã giấu khi cần thiết.

Phương pháp giấu thông tin là phương pháp mới đang được nghiên cứu và phát triển, được xem như công nghệ chìa khóa trong vấn đề bảo mật hiện nay để xác nhận được thông tin và ứng dụng để bảo đảm an toàn và bảo mật thông tin.

Đối với nghiên cứu này, tác giả xây dựng các thuật toán mã hóa thông tin và giải mã thông tin sử dụng môi trường là bài thơ lục bát.

Trong thơ lục bán là thể loại thơ đặt trưng truyền thống của Việt Nam, là loại thơ theo luật mà các thể thức tập trung trong một khổ với số từ cố định. Với một bài thơ thể lục bát là tập hợp của nhiều câu lục bát mỗi câu thường ngắt nhịp theo hai tiếng, độ dài bài thơ là không giới hạn, điều này rất phù hợp và thuận lợi cho việc mã hóa thông tin. Thông tin sẽ được mã hóa và truyền đi dưới dạng một bài thơ nên phương thức truyền là rất đa dạng. Phương pháp truyền có thể theo cách cổ điển như văn bản giấy hoặc phương pháp hiện đại như phương tiện truyền thông số. Trong điều kiện không thể truyền file thì việc truyền qua phương tiên thông tin đại chúng như phát thanh cũng có thể được. Khả năng này có thể áp dụng vào những hoàn cảnh đặc biệt như trong chiến tranh, khi mà các đường truyền số bị mất liên lạc hay dễ bị ngăn chặn.

Cấu trúc của bài báo gồm: Phần 1 là giới thiệu chung; phần 2 trình bày một số khái niệm về giấu thông tin và cấu trúc chung của thể loại thơ lục bát; phần 3 trình bày các thuật toán tìm khóa, thuật toán mã hóa thông tin và thuật toán giải mã thông tin; phần 4 là kết luận và định hướng nghiên cứu tiếp theo

2. CÁC KHÁI NIỆM CƠ BẢN

Trong phần này bài báo sẽ đưa ra một số định nghĩa về giấu thông tin dựa theo tài liệu [7].

Định nghĩa 1: Giấu thông tin

Giấu thông tin sử dụng phương pháp nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác và gọi là môi trường nhúng thông tin.

Kỹ thuật giấu thông tin chủ yếu hướng vào hai mục đích sau đây: Một là bảo mật cho dữ liệu được đem giấu, hai là bảo mật cho chính đối tượng được dùng để giấu thông tin. Trong đó khuynh hướng giấu tin mật tập trung vào kỹ thuật giấu tin sao cho lượng thông tin đem giấu được nhiều nhất và khó phát hiện được đối có được giấu tin bên trong hay không.

Các hệ thống giấu tin mật có thể chia thành ba loại như sau:

Định nghĩa 2: Giấu tin thuần túy *(Pure Steganography*)

Một bộ 4 $\sigma(C, M, D, E)$, trong đó C là tập các phương tiện chứa thông tin cần giấu, M là tập thông điệp cần giấu với $|C| \geq |M|$, $E: C \times M \rightarrow C$ là một hàm nhúng thông điệp M vào phương tiện chứa C và $D : C \rightarrow M$ là hàm giải mã thông tin sao cho D(E(c,m)) = m với mọi $m \in M$, $c \in C$ được gọi là một hệ *Pure Steganography*.

Định nghĩa 3: Giấu tin dùng khóa bí mật (*Secret Key Steganography)*.

Một bộ 5 $\sigma(C, M, K, D_k, E_k)$, trong đó C là tập các phương tiện chứa thông tin cần giấu, M là tập thông điệp cần giấu với $|C| \geq |M|$, $E_k: C \times M \times K \rightarrow C$ là một hàm nhúng thông điệp M vào phương tiện chứa C sử dụng khóa K và $D_k: C \times K \rightarrow M$ là hàm giải mã thông tin sao cho $D_k(E_k(c,m,k),k) = m$ với mọi $m \in M$, $c \in C$ và $k \in K$ được gọi là một hệ *Secret Key Steganography*.

Định nghĩa 4: Giấu tin dùng khóa công khai *(Public Key Steganography*)

Hệ giấu tin mật khóa công khai sử dụng hai khóa là khóa bí mật và khóa công khai. Khóa công khai được lưu trong cơ sở dữ liệu công cộng. Được sử dụng trong quá trình mã hóa thông tin. Còn khóa bí mật được sử dụng trong quá trình giải mã thông tin.

Định nghĩa 5: Giấu tin mật (*Steganography*)

Giấu tin mật là che giấu những thông điệp bên trong những thông tin khác mà không ảnh hưởng đến chất lượng của thông tin gốc và tránh bị nghi ngờ.

2.1. Các đối tượng trong bài toán giấu tin

***Bản tin mật*:** là bản tin được nhúng vào bản tin môi trường và là thông tin cần được bảo mật tùy theo từng kỹ thuật thông tin này được bảo mật ở các mức độ khác.

Đặc điểm: không giới hạn kiểu định dạng và kích thước của bản tin tùy thuộc vào yêu cầu bảo mật và lĩnh vực ứng dụng của thông tin.

Bản tin môi trường: là bản tin hay đối tượng được dùng để chứa bản tin mật. Bản tin môi trường thường có đặc điểm dữ liệu của nó phải lớn so với dữ liệu bản tin cần giấu.

Bản tin kết quả: là bản tin hay đối tượng chứa bản tin môi trường sau khi đã nhúng bản tin cần giấu.

Bản tin kết quả thường có kích thước dữ liệu không khác so với kích thước dữ liệu bản tin môi trường.

Khoá: là đối tượng mà nhờ nó người ta có thể tách được bản tin cần giấu ra khỏi bản tin môi trường.

Tuỳ thuộc vào kỹ thuật giấu tin mà khoá có thể là các dạng khác nhau, chúng có thể là một số nguyên hoặc tập các số nguyên hoặc một file...

2.2. Cấu trúc và đặc điểm của thể thơ lục bát [1]

Về câu chữ

Bài thơ thể lục bát là tập hợp các của các câu thơ lục bát, một câu lục bát gồm câu lục (6 tiếng) và câu bát (8 tiếng). Trong câu thơ nhịp thường được ngắt theo hai tiếng (nhịp chẵn) nhưng cũng có trường hợp đặc biệt mỗi nhịp là ba tiếng với câu lục và bốn với câu bát.

Gieo vần phối điệu

Thể thơ lục bát vừa gieo vần chấn vừa gieo vần lưng. Tiếng cuối của câu lục gieo vần xuống tiếng 6 của câu bát, tiếng nói cuối của câu bát lại gieo vần xuống tiếng 6 của câu lục tiếp theo.

Về phối điệu

Trong bài thơ lục bát yêu cầu các tiếng chẵn thì phải tuân theo đúng niên luật. Luật phối điệu như sau:

Câu 6		O	B	O	T	O	B	
Câu 8		O	B	O	T	B	O	B

Trong đó:

B: Thanh bằng

T: Thanh trắc

O: Thanh tự do (bằng hoặc trắc)

Thể thơ lục bát ngoài các luật điệu trên còn có thêm luật trầm bổng tức là tiếng thứ 6 và tiếng thứ 8 của câu bát mặc dù đều là thanh bằng nhưng có sự chuyển đổi từ âm trầm (thanh huyền) sang âm bổng (thanh không). Luật gieo vần và phối điệu như trên làm cho bài thơ lục bát nhịp nhàng và chặt chẽ.

3. PHƯƠNG PHÁP GIẤU THÔNG TIN TRONG THƠ LỤC BÁT

Khi giấu một lượng thông tin (là một văn bản tiếng Việt) vào một bài thơ lục bát nhằm mục đích truyền tin mật cho nên các yêu cầu được đặt ra một cách tự nhiên là:

Thứ nhất: một người bất kỳ khó lòng phát hiện một bài thơ lục bát nào đó có bị giấu thông tin hay không.

Thứ hai: mỗi bài thơ được giấu tin có một thông tin nào đó được gọi là "*khoá giấu tin*". Khoá giấu tin phải thỏa mãn điều kiện sau:

(k.1) Nếu biết được khoá giấu tin thì một người bất kỳ cũng dễ dàng tìm lại thông tin được giấu từ văn bản giấu thông tin.

(k.2) Nếu không biết được khoá giấu tin thì khó lòng tìm được thông tin được giấu.

Để đáp ứng yêu cầu thứ nhất ta thấy rằng việc giấu tin chỉ có thể được thực hiện như sau:

Thứ nhất: phải dùng phương pháp thay thế các "từ", vì phương pháp này không làm thay đổi cấu trúc của bài thơ (gồm số chẵn các câu với lần lượt là câu 6 từ, câu 8 từ).

Thứ hai: Các từ được thay thế không được phép là các từ thứ sáu trong mỗi câu thơ để tránh sự vi phạm luật gieo vần của thơ lục bát.

Thứ ba: Các câu thơ có thay từ vẫn đảm bảo là "*câu tiếng Việt có nghĩa*".

Để giảm thiểu sự "*lộ*" (theo nghĩa bị phát hiện là bài thơ có giấu tin) do việc thay thế, chúng ta giới hạn số từ được giấu trong mỗi câu thơ, cụ thể là trong mỗi câu thơ chỉ nên thay thế cùng lắm là một từ.

Đối với yêu cầu thứ hai, theo như lý thuyết Shannon, thì độ "*khó*" đối với người không có khoá giấu tin là tỷ lệ thuận với độ "*lớn*" của không gian khoá nếu việc sử dụng khoá là ngẫu nhiên. Nói một cách khác là độ phức tạp để tìm lại được thông tin khi không có khoá giấu tin chính là kích thước của không gian khóa.

3.1. Tiêu chuẩn nhận biết một khoá giấu tin

Một khoá giấu tin cho một bản tin n từ vào một bài thơ lục bát 14m từ (2m câu) là một bộ n số nguyên khác nhau $K = (j_0, j_1,\ldots, j_{n-1})$ với $0 \le i_j < 14m$.

Tuy nhiên một bộ n số nguyên khác nhau $K = (j_0, j_1,\ldots, j_{n-1})$ với $0 \le i_j < 14m$ bất kỳ nói chung chưa chắc đã là khoá giấu tin bởi vì không thỏa mãn các điều kiện (đk.1) và (đk.2). Kết quả sau đây cho ta điều kiện để một bộ số nguyên $(j_0, j_1,\ldots, j_{n-1})$ thoả mãn (đk.1) và (đk.2).

Mệnh đề 3.1. Cho bộ n số nguyên khác nhau $(j_0, j_1,\ldots, j_{n-1})$ với $0 \le i_j < 14m$.

Khi đó

(1) Điều kiện (đk.1) được thỏa mãn khi và chỉ khi với mọi $i = 0 \div n-1$ ta có

$$j_i \# 5, 11 \pmod{14} \quad (1)$$

(2) điều kiện (đk.2) được thỏa mãn khi và chỉ khi với mọi $i = 1 \div n-1$ ta có

$$\text{hoặc } j'_i \text{ div } 14 \neq j'_{i-1} \text{ div } 14 \quad (2)$$

Nếu $j'_i \text{ div } 14 = j'_{i-1} \text{ div } 14$ thì $j'_i \bmod 14 > 5$

$$\text{và } j'_{i-1} \bmod 14 < 5 \quad (3)$$

$j'_0, j'_1, \ldots, j'_{n-1}$ được sắp xếp theo thứ tự tăng dần của tập$\{j_0, j_1,\ldots, j_{n-1}\}$.

Chứng minh

Rõ ràng các từ thứ 6 trong các câu của một bài thơ lục bát sẽ có chỉ số thứ tự trong toàn bài thơ là $j \# 5, 11 \pmod{14}$ nên điều kiện (đk.1) là tương đương với các vị trí được giấu thoả mãn điều kiện trong công thức trong công thức (3). Trong công thức (4) cho biết hai từ được giấu có vị trí liền nhau thuộc hai cặp câu thơ lục bát khác nhau.

Do đó vị trị giấu của hai từ này nằm ở hai câu thơ khác nhau. Trong trường hợp ngược lại thì điều kiện của công thức (1-3) là tương đương với từ giấu ở vị trí j'_{i-1} phải thuộc câu 6, còn từ giấu ở vị trí j'_i phải thuộc câu 8 do đó chúng phải ở hai câu thơ khác nhau. Hay nói cách khác là điều kiện (đk.2) cũng được thỏa mãn điều phải chứng minh.

Bài toán 3.1: giấu bản tin gồm n từ tiếng Việt vào một bài thơ lục bát gồm 2m câu thơ bằng phép thay thế từ thoả mãn hai điều kiện sau:

(đk.1) Mỗi câu thơ chỉ được giấu không quá 1 từ.

(đk.2) Các từ được thay thế không được phép là các từ thứ sáu trong mỗi câu thơ.

Khoá giấu tin cho bài toán 3.1

Cho bản tin n từ $T = t_0 t_1 \ldots t_{n-1}$ trong đó t_i là một từ tiếng Việt $(i = 0 \div n-1)$ cần được giấu trong bài thơ lục bát gồm 2m câu (tức là có 14m từ) $L = l_0 l_1 \ldots l_{14m-1}$.

Trong đó:

l_j là một từ tiếng Việt $(j = 0 \div 14m-1)$

D là bài thơ sau khi đã được giấu tin

Theo phương pháp thế từ ta có D cũng đúng 14m từ tức là:

$$D = d_0 d_1 \ldots d_{14m-1} \quad (4)$$

Khi đó ta có $d_j = l_j$ nếu j không phải là vị trí của từ được giấu và $d_j = t_i$ nếu j là vị trí giấu từ t_i.

Ký hiệu $(j_0, j_1,\ldots, j_{n-1})$, trong đó j_i là vị trí từ trong bài thơ giấu từ t_i, rõ ràng việc biết D và bộ $(j_0, j_1,\ldots, j_{n-1})$ sẽ dễ dàng thu lại thông tin theo công thức sau.

$$T = d_{j_0} d_{j_1} \ldots d_{j_{n-1}} \quad (5)$$

Như vậy bộ n số nguyên $(j_0, j_1,\ldots, j_{n-1})$ thu được có thể đóng vai trò khoá giấu tin.

Ngược lại, nếu $L = l_0 l_1 \ldots l_{14m-1}$ là bài thơ lục bát 2m câu dùng để giấu thông tin $T = t_0 t_1 \ldots t_{n-1}$ bởi khoá $K = j_0 j_1 \ldots j_{n-1}$ thì các từ của bài thơ được giấu tin $D = d_0 d_1 \ldots d_{14m-1}$ sẽ được xác định theo công thức sau:

$d_j = l_j$ nếu $j \neq j_i$ với mọi $i = 0 \div n-1$

và $d_j = t_i$ nếu $j = j_i$ $(j = 0 \div 14m-1)$ (6)

Nhận xét: các công thức (2) và (1) chính là cơ sở cho các thuật toán mã hóa thông tin và và giải mã thông tin từ khóa $(j_0, j_1,\ldots, j_{n-1})$.

3.2. Các thuật toán mã hóa thông tin giải mã thông tin đã giấu

Thuật toán 3.1. Thuật toán giấu tin

Input: T, L và $K = (j_0, j_1,\ldots, j_{n-1})$.

Trong đó: T là bản tin cần giấu gồm n từ,

L là bài thơ lục bát gồm 2m câu thơ $(n \le 2m)$,

K là khoá giấu tin.

Output: D là bài thơ lục bát thu được từ L có giấu tin T theo khoá K.

1. Chia T và L theo đơn vị từ $T = t_0 t_1 \ldots t_{n-1}$,

$L = l_0 l_1 \ldots l_{14m-1}$.

2. Tính d_j $(j = 0 \div 14m-1)$ theo công thức (3-6)

Lấy $D = d_0 d_1 \ldots d_{14m-1}$.

3. Output = D.

Thuật toán 3.2. Thuật toán khôi phục lại tin sau khi giấu

Input: D và $K = (j_0, j_1,\ldots, j_{n-1})$.

Trong đó:

D là bài thơ lục bát có giấu tin gồm 2m câu thơ $(n \le 2m)$

K là khoá giấu tin.

Output: T là tin được giấu trong D theo khoá K.

1. Chia D theo đơn vị từ $D = d_0d_1...d_{14m-1}$.

2. Tính T theo công thức (3-5)

3. Output = T.

Thuật toán 3.3. Thuật toán tìm khoá giấu tin

Input: n, m là các số nguyên dương.

Output: $(j_0, j_1, ..., j_{n-1})$ là khoá giấu tin.

1. $i \leftarrow 0$, $TapCam \leftarrow \{\ \}$

2. $c \leftarrow random(2m)$

3. Nếu $c \in TapCam \cup \{c\}$, quay lại bước 2

4. $TapCam \leftarrow TapCam \cup \{c\}$

5. Nếu c chẵn $v \leftarrow random(5)$.

Ngược lại $v \leftarrow random(7)$.

6. Nếu $(v > 4)$ $v \leftarrow v + 1$

7. $j_i = 14(c \text{ div } 2) + 6(c \text{ mod } 2) + v$

8. $i \leftarrow i + 1$

9. Nếu $(i < n)$, quay lại bước 2

10. Output = $(j_0, j_1, ..., j_{n-1})$.

3.3. Xác định lượng không gian khoá giấu tin

Giả sử ký hiệu $A_k(n, m)$ là số các khoá có đúng k từ được giấu trong các câu 6 (đương nhiên n-k từ còn lại phải được giấu trong các câu 8) của bài thơ thì rõ ràng tổng số khoá có thể, ký hiệu là A(n, m), sẽ được tính theo công thức sau:

$$A(n, m) = \sum_{k_{min}}^{k_{max}} A_k(n, m) \quad (7)$$

Trong đó:

$$k_{min} = max\{0; n-m\} \text{ và } k_{max} = min\{m; n\}$$

(tương ứng là số từ tối thiểu và số từ tối đa mà các câu 6 có thể giấu).

Kết quả dưới đây cho ta công thức để tính các giá trị A_k.

Định lý 3.1: Nếu bản tin T có đúng $n \le 2m$ từ khác nhau thì với mọi $k_{min} \le k \le k_{max}$ ta có:

$$A_k(n, m) = 5^k 7^{(n-k)} m(m-1) \dots (m-k+1) m(m-1) \dots (m+n+k+1). (0 < k < n). \quad (8)$$

Trường hợp $n \le m$ thì $k_{min} = 0$, $k_{max} = n$ và ta có

$$A_0(n,m) = 7^n m(m-1)\dots(m-n+1) \quad (9)$$

$$A_n(n,m) = 5^n m(m-1)\dots(m-n+1) \quad (10)$$

Chứng minh

Theo thuật toán 3.3 thì để giấu từ đầu tiên vào các câu 6 ta có đúng m (tổng số câu 6 trong bài thơ) cách chọn một trong các câu 6 khác nhau mà trong câu 6 được chọn này lại có 5 vị trí từ khác nhau có thể giấu. Như vậy sẽ có 5m cách dấu khác nhau cho từ này.

Đối với từ thứ hai, do đã có một câu 6 giấu từ thứ nhất nên chỉ còn (m-1) cách chọn câu để giấu nó và vẫn tương ứng với 5 vị trí từ khác nhau ta sẽ có 5(m-1) cách giấu khác nhau cho từ thứ hai.

Như vậy, tổng số cách để giấu 2 từ vào các câu 6 sẽ là $5m5(m-1) = 5^2m(m-1)$. Và do đó số cách để giấu $k > 0$ từ vào các câu 6 sẽ là

$$5^k m(m-1)...(m-k+1) \quad (11)$$

Lập luận tương tự với việc giấu $(n-k) > 0$ từ vào các câu 8 ta sẽ có tổng số cách giấu là:

$$7^{(n-k)}m(m-1)\dots(m-n+k+1) \quad (12)$$

Như vậy nếu $0 < k < n$, tức là k và (n-k) đều lớn hơn 0, theo hai kết quả trên ta có ngay công thức (8).

Ngược lại nếu $k = 0$ thì $n - k = n$ và nếu $k = n$ thì $n - k = 0$ vậy số cách để giấu 0 từ vào các câu thơ chỉ có duy nhất một phương án đó là "không giấu gì cả" cho nên công thức (9) và (10) chính là các hệ quả tương ứng của công thức (12) và (13) điều phải chứng minh.

Định lý 3.2: Tổng số khoá cho việc giấu bản tin gồm n từ khác nhau vào bài thơ lục bát gồm 2m câu ($n < 2m$), ký hiệu là A(n, m), được xác định như sau:

Nếu $m < n$ thì:

$$A(n,m) = \frac{(m!)^2}{n!} \sum_{k=n-m}^{m} C_n^k 5^k 7^{n-k} \quad (13)$$

Ngược lại thì:

$$A(n,m) = \frac{(m!)^2}{n!}\left(12^n - (7^n + 5^n)\left(1 - \frac{1}{m!}\right)\right) \quad (14)$$

Chứng minh

Từ công thức (8) thì với mọi k ($0 < k < n$)ta có

$$A_k(n, m) = 5^k 7^{(n-k)} m(m-1)\dots(m-k+1)m(m-1) \dots (m+n+k+1).$$

$$= 5^k 7^{(n-k)} \frac{m!}{k!} \frac{m!}{(n-k)!}$$

$$= \frac{(m)^2}{n!} C_n^k 5^k 7^{n-k}$$

Trường hợp m < n

Khi đó $k_{min} = n - m$, $k_{max} = m < n$ nên ta có

$$A(n, m) = \sum_{k=n-m}^{m} A_k(n, m) = \frac{(m!)^2}{n!} \sum_{k=n-m}^{m} C_n^k 5^k 7^{n-k}$$

Trường hợp m ≥ n

Từ công thức (9) và công thức (10) thì

$A_0(n, m) = 7^n \frac{m!}{n!}, A_n(n, m) = 5^n \frac{m!}{n!}$ nên ta có

$$A(n, m) = \sum_{k-1}^{n-1} A_k(n, m) + (7^n + 5^n)\frac{m!}{n!}$$

$$= \frac{(m!)^2}{n!} \sum_{k=0}^{n} C_n^k 5^k 7^{n-k} - (7^n + 5^n)\frac{(m!)^2}{n!} + (7^n + 5^n)\frac{m!}{n!}$$

$$= \frac{(m!)^2}{n!}(5+7)^n - \frac{(m!)^2}{n!}(7^n + 5^n)(1 - \frac{1}{m!})$$

$$= \frac{(m!)^2}{n!}(12^n - (7^n + 5^n)(1 - \frac{1}{m!}))$$

Kết quả nghiên cứu: thông qua các nghiên cứu như trên ta xác định số khoá giấu tin theo bài toán của một số thông tin có số lượng từ khác nhau vào bài thơ lục bát có 40 câu thơ (m =20).

1. Số khoá giấu tin cho một bản tin 40 từ khác nhau là:

$A(40,20) = A_{20}(40,20) = 7^{20}5^{20} = 35^{20}$.

2. Số khoá giấu tin cho một bản tin 20 từ khác nhau là:

$$A(20,20) = \frac{(20!)^2}{20!}(12^{20} - (7^{20} + 5^{20})(1 - \frac{1}{20!})) > 20!(12^{20} - 7^{20} - 5^{20})$$

4. KẾT LUẬN

Dựa trên công trình nghiên cứu [2], trong bài báo này, tác giả đã chứng minh được tính đúng đắn của các thuật toán dựa theo các định nghĩa và định lý. Các thuật toán trên cũng đã được cài đặt chạy thử nghiệm và so sánh với các thuật toán phổ thông trước đây. Kết quả tính toán tính toán thực tế cho thấy các thuật toán này đều cho ta kết quả tốt hơn cả về chất và lượng. Dựa trên kết quả nghiên cứu phương pháp giấu thông tin trong môi trường văn bản với dung lượng lớn mang lại nhiều tiện ích cho người sử dụng mà vẫn đảm bảo tính an toàn cho thông tin. Ngoài ra bài báo còn nghiên cứu xây dựng thuật toán tối ưu về thời gian mã hóa và giải mã thông tin trên nhiều file văn bản trong cùng một thời điểm giúp người dùng tiết kiệm được thời gian công sức trong việc mã hóa thông tin.

Định hướng nghiên cứu tiếp theo là xây dựng các thuật toán giấu thông tin trong các môi trường khác để cải tiến quá trình xử lý về thời gian để xử lý nhiều file với dung lượng lớn một chách tối ưu nhất.

TÀI LIỆU THAM KHẢO

[1]. Nguyen Van Xuat, "Consider Vietnamese from the perspective of information technology", in *ITMATH'06*, Military Technical Academy, Hanoi, 2006,

[2]. Ashwini Palimkar, S. H. Patil, "Using SBR Algorithm To Hide The Data Into The JPEG Image," *International Journal of Security (IJS)*, 8, 2, 2014.

[3]. M. Swanson, M. Kobayashi, A. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", in *Procceding of the IEEE*, 86, 6, 1998.

[4]. M. Y. Wu, J. H. Lee, "A novel data embedding method for binary facsimile images," in *Proceedings of International Symposium on Multimedia Information Processing*, Chung-Li, Taiwan, 1998.

[5]. Pawlak Z, *Rough sets: Theoretical Aspects of Reasoning About Data*. Springer Dordrecht, 1991.

[6]. Peter Wayner, *Disappearing Cryptography: Information Hiding: Steganography and Watermarking (The Morgan Kaufmann Series in Software Engineering and Programming) 2nd Edition*. Morgan Kaufmann(MK), 2002.

[7]. R. Z. Wang, C. F. Lin, J. C. Lin, "Image hiding by LSB substitution and genetic algorithm", in *Proceedings of International Symposium on Multimedia Information Processing*, Chung-Li, Taiwan, 1998.

AUTHOR INFORMATION

Ninh Van Tho

University of Economics - Technology for Industries, Vietnam