Mathematical Researches
Print ISSN: 2588-2546
Online ISSN: 2588-2554
Kharazmi University
Homepage: https://mmr.khu.ac.ir/

An efficient improved steganographic scheme based on BCH syndrome coding

Reza Meshki-Sani[1], **Mohammad-Reza Rafsanjani-Sadeghi**[2]✉
Parvane Amirzade-Dana Samadyar[3]

1. Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran.
E-mail: r.msani74@aut.ac.ir
2. Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran.
✉E-mail: msadeghi@aut.ac.ir
3. Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran.
E-mail: pamirzade@gmail.com

Article Info

Article type:
Research Article

Article history:
Received:
22 July 2019
Received in revised form:
22 December 2020
Accepted:
4 January 2021
Published online:
31 December 2022

Keywords:
BCH coding,
Steganography,
Characteristic of the syndrome,
Syndrom coding,
Syndrom,
Invariant.

ABSTRACT

Introduction

After identifying the importance of steganography as a type of secure communication, the major effort of researchers in this field was to provide algorithms with low computational complexity and high embedding capacity. One of the essential principles of design of a secure steganographic schemes is minimizing the embedding impact. After introducing the matrix embedding (ME) method in steganography, it was noticed that the use of linear block codes would reduce the detectability of a steganography scheme, however, there were challenges such as high computational and spatial complexity as well as low embedding capacity. An approach to resolve such issue is search for different linear codes for the matrix embedding method. One of the most commonly used codes is BCH codes which we have also covered in this paper.

A more advanced form of ME is called MME, which changes more than one bit per cover but, increase the degree of freedom. In other words, more paths are provided to insert the message in the cover. Then the embedder chooses the best path by considering the conditions of the cover. This method reduces the distinguishability of the raw cover from the message carrier cover. Using steganography based on BCH codes, Schönfeld et al. found methods to increase the degree of freedom. They came up with a classic technique to find a corollary representation of BCH code.

However, their proposed method required to find polynomial roots in Galois Square and so this approach cannot be used in practical systems due to its high complexity. Later, with the aim of reducing complexity, a new steganography method was introduced using the BCH code generator polynomial which, despite a significant reduction in complexity, was not yet efficient enough to be used in practical systems.

Material and methods

In this paper we present a new stenographic scheme based on matrix embedding using syndrome coding. The proposed method embeds massage into cover by changing some coefficients of cover. In this scheme defining a number as characteristic of the syndrome, which is invariant with respect to the cyclic shift, we propose a new embedding algorithm based on BCH(n, k, 2) syndrome coding, without finding roots of quadratic and cubic polynomials in GF(2^m).

Results and discussion

We solve some test examples by using our proposed technique to demonstrate the efficiency, high accuracy and the simplicity of the present method, then compare the proposed method with some previous method. The numerical results reported in the tables indicate that the computational complexity of the proposed method is linear and space complexity is polynomial of size is just O(n^2), which demonstrate a sginificant improvement over the existing method.

Conclusion

This research provides the following conclusions:

- Defining a number as characteristic of the syndrome, which is invariant with respect to the cyclic shift, a new steganographic system, based on BCH(n,k,2) syndrome coding, is developed, without finding roots of quadratic and cubic polynomials in GF(2m).
- In order to implement proposed method, an efficient algorithm with polynomial complexity is designed.

How to cite: Meshki-Sani, R., Rafsanjani-Sadeghi, M. S., Amirzade-Dana Samadyar, P. (2022). An efficient improved steganographic scheme based on BCH syndrome coding. *Mathematical Researches*, 8 (4), 215-237.

Publisher: Kharazmi University

Mathematical Researches
Print ISSN: 2588-2546
Online ISSN: 2588-2554
Homepage: https://mmr.khu.ac.ir/

روش نهان‌نگاری بهبودیافته و کارا براساس بردار مشخصه کد BCH

رضا مشکی‌ثانی[۱]، محمد رضا رفسنجانی صادقی[۲]✉، پروانه امیرزاده دانا[۳]

۱. دانشکدهٔ ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران. رایانامه: r.msani74@aut.ac.ir
۲. نویسندهٔ مسئول، دانشکدهٔ ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران، رایانامه: msadeghi@aut.ac.ir
۳. دانشکدهٔ ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران. رایانامه: pamirzade@gmail.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۳۹۸/۰۴/۳۱
تاریخ بازنگری: ۱۳۹۹/۱۰/۰۲
تاریخ پذیرش: ۱۳۹۹/۱۰/۱۵
تاریخ انتشار: ۱۴۰۱/۱۰/۱۰

واژه‌های کلیدی:
کد BCH،
نهان‌نگاری،
بردار مشخصه،
بردار مشخصه کدهای BCH،
مشخصه بردار مشخصه.

چکیده

در این مقاله در ادامهٔ روش‌های نهان‌نگاری با استفاده از بردار مشخصهٔ کدهای BCH به ارائهٔ یک روش نهان‌نگاری دیگر با استفاده از بردار مشخصه کدهای $BCH(n, k, 2)$ می‌پردازیم. روش پیشنهادی، با تغییر بعضی از ضرایب پوشش به منظور صفر کردن بردار مشخصه ، پیام را داخل پوشش درج می‌کند. در این روش با تعریف یک عدد به عنوان مشخصه بردار مشخصه ، که نسبت به شیفت برداری پایا است، عمل نهان‌نگاری را براساس بردار مشخصه کدهای $BCH(n, k, 2)$ بدون نیاز به پیدا کردن ریشه‌های چندجمله‌ای‌های درجه دو و سه در میدان‌های گالوا انجام می‌دهیم. روش پیشنهادی برای کدهای $BCH(n, k, 2)$ دارای پیچیدگی محاسباتی خطی و فضایی چندجمله‌ای است و به صورت کارا قابل پیاده سازی در سیستم‌های عملی موجود است.

استناد: مشکی‌ثانی، رضا؛ رفسنجانی صادقی، محمد رضا؛ امیرزاده دانا، پروانه (۱۴۰۱). روش نهان‌نگاری بهبودیافته و کارا براساس بردار مشخصه کد BCH. *پژوهش‌های ریاضی*، ۸ (۴)، ۲۳۷-۲۱۵.

ناشر: دانشگاه خوارزمی

مقدمه

اخیراً نظریهٔ اطلاع سهم زیادی در پیشرفت نهان‌نگاری داشته است. یک تعریف کلی از نهان‌نگاری عبارت‌است از روشی برای پنهان کردن داده‌ها در بستر یک کانال ارتباطی امن به طوری که تشخیص وجود داده پنهان از دشمن سلب شود. رسانهٔ دیجیتالی که برای حمل پیام استفاده می‌شود را پوشش می‌نامند. عمل درج پیام بر روی پوشش باید به گونه‌ای باشد که در آن تغییر قابل احساسی ایجاد نشود، به عبارتی، بسیار طبیعی جلوه کند. عدم تشخیص‌پذیری پوشش خام از پوشش حامل پیام یکی از مهمترین اهداف برای طراحی یک طرح نهان‌نگاری امن است. وانگ[۱] و مولین[۲] نشان داده‌اند مادامی که درج کنندهٔ اطلاعات کاملی از نحوهٔ توزیع آماری پوشش داشته باشد نهان‌نگاری امن با احتمال تشخیص‌پذیری صفر امکان‌پذیر است [۱]. ثابت شده است که میزان تشخیص‌پذیری (توانایی تشخیص وجود یا عدم وجود پیام توسط دشمن) متناسب با تعداد تغییرات ناشی از درج (تعداد تغییراتی که درج کنندهٔ پیام به پوشش اعمال می‌کند تا پیام در پوشش درج شود) است [۲]. شاید یکی از اولین کاربردهای نظریه اطلاع در نهان‌نگاری مربوط به کشین[۳]باشد. او امنیت طرح های نهان‌نگاری را با استفاده از اختلاف کولبک لیبلر[۴] بین توزیع آماری پوشش خام و پوشش حامل پیام اندازه‌گیری کرد. او در روش خود طرح‌های نهان‌نگاری با اختلاف کولبک لیبلر صفر را کاملاً امن نامید. به عبارتی، هر چه شباهت بین خواص آماری پوشش حامل پیام و پوشش خام بیشتر باشد، توانایی دشمن در تشخیص وجود پیام کمتر می‌شود. چون برآورده کردن فرض‌های وانگ و مولین برای دست‌یابی به طرح‌های نهان‌نگاری امن کار دشواری است، ما عمده تلاش خود را در راستای طراحی الگوریتم‌های نهان‌نگاری صرف می‌کنیم که در فرایند درج کمترین تغییرات به پوشش اعمال شود و همچنین تغییرات در نقاط کم اهمیت پوشش (از نظر بازدهی تشخیص‌پذیری) ایجاد می‌شوند. در فرایند درج پیام در پوشش دو حالت زیر پیش می‌آید:

(آ) حالتی که مجاز به تغییر همهٔ مکان‌های پوشش هستیم.

(ب) حالتی که مجاز به تغییر بعضی از مکان‌های پوشش نیستیم (این مکان‌ها به مکان‌های قفل شده معروفند که درج‌کننده پیام از این مکان‌ها اگاهی دارد).

اخیراً نظریه کدگذاری با استفاده از کدهای همینگ[۵] [۳]، کد هایی دودویی BCH [۴]، [۵] و کدهای رید-سالمون[۶] [۶] و غیره به منظور طراحی طرح‌های امن نهان‌نگاری وارد حوزه‌ی نهان‌نگاری شده‌اند. وستفلد[۷] با استفاده از نظریهٔ کدینگ روشی

[۱] Wang
[۲] Moulin
[۳] Cachin
[۴] Kullback–Leibler
[۵] Hamming
[۶] Reed-Solomon
[۷] Westfeld

را بر مبنای حالت (آ) ارائه داد که به درج ماتریسی[۱] (ME) معروف است [۷]. در حالی که جسیکا فردریش[۲] و همکارانش به بررسی حالت (ب) پرداختند و الگوریتم کدگذاری کاغذ مرطوب[۳] را معرفی کردند. کدهای کاغذ مرطوب برای جلوگیری از تغییر مقدار عناصر در مکان‌های قفل شده در فرآیند درج طراحی شده‌اند. الگوریتم F_5 پیشنهاد شده توسط وستفلد اولین اجرا از مفهوم ME بود [۷]. اساس کار ME در الگوریتم F_5 به این شرح است که با استفاده از (n, k)- کد همینگ حداکثر یک بیت را از میان n بیت تغییر می‌دهد و $n-k$ بیت پیام را درج می‌کند. همان‌طور که واضح است، در مقایسه با روش LSB[۴] تعداد تغییرات را، به قیمت قربانی کردن ظرفیت درج، کم می‌کند. در این حالت لازم نیست همهٔ بیت‌های پوشش تغییر کند. شکل پیشرفته تری از ME به نام MME[۵] ارائه شده است، که در این روش بیشتر از یک بیت در هر پوشش تغییر می‌کند [۸]. در روش MEE تغییرات بیشتری در مقایسه با روش ME اعمال می‌شود، اما درجهٔ آزادی[۶] یا به عبارتی مسیرهای بیشتری به منظور درج پیام در پوشش فراهم می‌شود به این ترتیب درج‌کننده با در نظر گرفتن شرایط پوشش، بهترین مسیر را انتخاب می‌شود. این مسأله باعث کاهش تشخیص‌پذیری پوشش خام از پوشش حامل پیام می‌شود. شان فلد[۷] و وینکلر[۸] با استفاده از نهان‌نگاری برپایهٔ کدهای BCH روش‌هایی برای افزایش درجهٔ آزادی پیدا کردند [۴]. آنها یک روش کلاسیک برای پیدا کردن نمایندهٔ همدستهٔ[۹] کدهای BCH ارائه دادند اما، روش پیشنهاد شده توسط آنها نیاز به جستجوی کامل برای پیدا کردن ریشه‌های چندجمله‌ای در میدان گالوا داشت. این رویکرد به سبب پیچیدگی بالا قابل استفاده در سیستم‌های عملی نیست [۴]. بعدها با هدف کاهش پیچیدگی، یک روش جدید نهان‌نگاری با استفاده از چندجمله‌ای مولد کد BCH ارائه شد که، با وجود کاهش قابل ملاحظه پیچیدگی، نسبت به روش قبلی خود هنوز دارای کارایی لازم برای استفاده در سیستم‌های عملی نبود [۵]. در ادامهٔ تلاش‌ها برای کاهش پیچیدگی نهان‌نگاری، با استفاده از کدهای BCH، یک روش جدید نهان‌نگاری برپایهٔ کد $BCH(n, k, 2)$ ارائه شد این روش با به کارگیری دو لم و استفاده از دو حافظه از جستجوی کامل برای پیدا کردن ریشه‌های چندجمله‌ای درجهٔ دو و سه در میدان‌های گالوا جلوگیری می‌کند، در این طرح پیدا کردن نمایندهٔ همدسته با پیچیدگی محاسباتی خطی و فضایی چندجمله‌ای انجام می‌شود [۹]. در این مقاله ما با تعریف یک عدد به عنوان مشخصه بردار مشخصه که نسبت به شیفت برداری پایا است، با رویکردی جدید و متفاوت از روش‌های قبلی نهان‌نگاری بر پایهٔ کدهای BCH، الگوریتمی ارائه می‌دهیم که بر پایهٔ کد $BCH(n, k, 2)$ عمل نهان‌نگاری به صورتی ساده‌تر و با پیچیدگی محاسباتی خطی و فضایی چندجمله‌ای اجرا می‌کند.

در ادامه و در فصل ۰ به معرفی کدهای BCH خواهیم پرداخت. سپس در فصل ۰ روش نهان‌نگاری براساس کدگذاری

[۱] (Matrix embeding (ME))
[۲] J.ferdrich
[۳] Wet paper code (WPC)
[۴] Least significant bit
[۵] Modified matrix embeding
[۶] Degree of freedom (DOF)
[۷] Schönfeld
[۸] Winkler
[۹] Coset Leader

بردار مشخصه را بیان می‌کنیم. در فصل۰ به بیان ایدهٔ پیشنهادی خواهیم پرداخت. در فصل ۰ به ارائه یک مثال کامل از روش پیشنهادی خواهیم پرداخت. در فصل ۰ روش پیشنهاد شده در این مقاله را با دیگر روش‌های نهان‌نگاری بر اساس کدهای BCH مقایسه می‌کنیم. در نهایت در فصل ۷ به نتیجه‌گیری خواهیم پرداخت.

کدهای BCH

تعریف ۰-۱- تابع $\psi((e_1, e_2, \dots, e_n)) = (e_n, e_1, \dots, e_{n-2}, e_{n-1})$ را در نظر بگیرید، تابع ψ، تابع شـیفت‌برداری نامیده می‌شود.

تعریف ۰-۲- یک (n, k)- کد خطی را دوری گوییم هرگاه:

$$\mathbf{c} = (c_0, c_1, c_2, \dots, c_{n-1}) \in \mathbf{C} \Longrightarrow \psi((c_0, c_1, c_2, \dots, c_{n-1}) \in \mathbf{C}$$

کد BCH برای اولین بار توسط آر.سی.بز[۱] و دی.ری-چادهوری[۲] و ای.هوکنگم[۳]درسال‌های ۱۹۵۹-۱۹۶۰ کشف شد.

تعریف ۰-۳- یک کد BCH، t- خطا تصحیح کنندهٔ q- آرایه‌ای از طول n به صورت زیر ساخته می‌شود.

(۱) یک n امین ریشهٔ واحد $\alpha \in \mathbb{F}_{q^m}$ را در نظر بگیرید، $\mathbb{F}_{q^m}$ کوچکترین توسیع $\mathbb{F}_q$ شامل α است.

(۲) تعداد $2t = \delta - 1$ توان متوالی α، $(b \geq 1)$ $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2}$ را انتخاب کنید.

(۳) قرار دهید $g(x) = \mathrm{LCM}\{M_{\alpha^b}(x), M_{\alpha^{b+1}}(x), \dots, M_{\alpha^{b+\delta-1}}(x)\}$ که به ازای هر i، $M_{\alpha^i}(x)$ موجود در این جمله $(i = b, b+1, \dots, b+\delta-1)$ چندجمله‌ای مینیمال α^i نسبت به $\mathbb{F}_q$ است. به این ترتیب کد BCH متناظر، کدی با چند جمله‌ای مولد $g(x)$ است

تعریف ۰-۴- در حالت $b = 1$، کد BCH را تشخیص محدود[۴] می‌نامیم.

یک کد BCH، t- خطا ت صحیح کننده از طول n و بعد k را با نماد $BCH(n, k, t)$ ن شان می‌دهند. ماتریس برر سی توازن یک کد BCH، t- خطا تصحیح کننده، تشخیص محدود، دودویی به شکل زیر است.

[۱] R.C.Bose
[۲] D.K.Ray-Chaudhuduri
[۳] A.Hocquenghem
[۴] Narrow-sence

$$H=\begin{bmatrix}1 & \alpha & (\alpha)^2 & \dots & (\alpha)^{n-1}\\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \alpha^{2\,t-3} & (\alpha^{2\,t-3})^2 & \dots & (\alpha^{2\,t-3})^{n-1}\\ 1 & \alpha^{2\,t-1} & (\alpha^{2\,t-1})^2 & \dots & (\alpha^{2\,t-1})^{n-1}\end{bmatrix} .$$

بنابراین ماتریس بررسی توازنی کد دودویی $\mathrm{BCH}(n,k,2)$ به شکل زیر است.

$$H=\begin{bmatrix}1 & \alpha & (\alpha)^2 & \dots & (\alpha)^{n-1}\\ 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{n-1}\end{bmatrix} \qquad (۱۰-۱)$$

فرض کنید $\mathbf{x}=(x_0,x_1,\dots,x_{n-2},x_{n-1})$ یک بردار است $(i=0,1,\dots,n-1)$ و $\alpha^i\in GF(2^m)$، با ضرب بردار $\mathbf{x}$ در ماتریس (۱۰-۱) بردار $\mathbf{S}=[S_1,S_2]$ حاصل می‌شود که بردار، بردار مشخصه نامیده می‌شود.

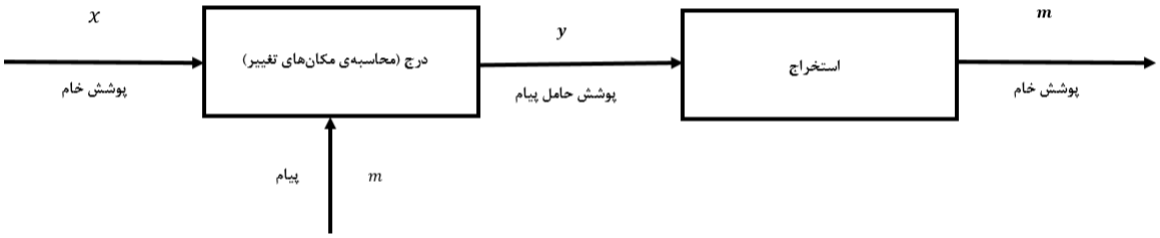
$$S_1=\sum_{i=0}^{n-1}x_i\alpha^i \qquad , \qquad S_2=\sum_{i=0}^{n-1}x_i(\alpha^i)^3$$

چون $x_i\in\{0,1\}$ $(i=0,1,2,\dots,n-1)$ و $\alpha^i\in GF(2^m)$، $S_1,S_2\in GF(2^m)$.

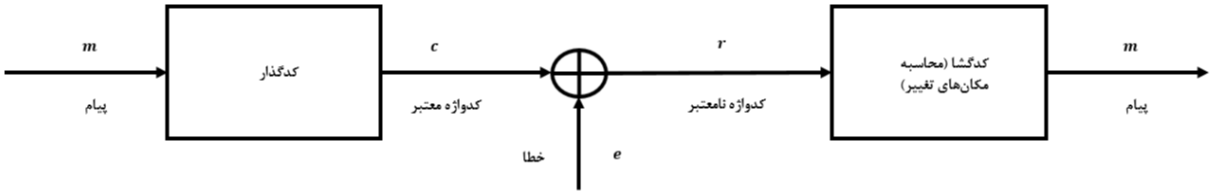
نهان‌نگاری براساس بردار مشخصه کد

رمزنگاری ازگذشته تا به امروز یک وسیله و ابزار مهم برای امن نگه‌داشتن اطلاعات خصوصی در مقابل دسترسی‌های غیرمجاز بوده است. نمونه‌های استفاده از رمزنگاری همواره در طول تاریخ وجود داشته است که می‌توان به ارتباط رمز شده در بین فرماندهان در طی جنگ‌ها اشاره‌کرد. امروزه رمزنگاری در مسائل مهم اقتصادی و تجاری نیز وارد شده است. با توجه به پیشرفت فناوری و افزایش‌کانال‌های ناامن ارتباطی مانند تلفن، اینترنت و ... نیاز به رمزنگاری و اطلاعات رمزنگاری شده هر روز افزایش می‌یابد. امروزه رمزنگاری به عنوان یک علم تخصصی در میان شاخه‌های علوم مورد بررسی قرار می‌گیرد. البته از گذشته تا به امروز تنها مخفی ماندن محتوای پیام پاسخگوی همه نیازهای بشر برای برقراری یک ارتباط نبوده است. زیرا یکی از مهمترین نیازهای بشر از یک ارتباط امن نامحسوس ماندن خود ارتباط است، بنابراین به محض تشخیص وجود ارتباط رمز شده، توسط دشمن، ممکن است خرابکاری‌هایی در جهت از بین بردن ارتباط انجام گیرد. به دلیل اهمیت نهان‌نگاری در طی سالیان اخیر تحقیقات فراوانی در این حوزه انجام گرفته است. در ادامه به بیان چند تعریف در نهان‌نگاری می‌پردازیم. به طور خلاصه عامیانه‌ترین تعریفی که می‌توان از نهان‌نگاری ارائه کرد، مخفی کردن داده در داده‌ای دیگر است. همان‌طور که از تعریف نهان‌نگاری واضح است در نهان‌نگاری یک پیام را در یک شی یا پوشش، که امروزه اغلب اسناد الکترونیکی چون عکس، فیلم، صدا، متن که بر روی شبکه اینترنت قابل حمل هستند، درج یا جایگذاری می‌شود. هدف اصلی نهان‌نگاری تبادل پیام

مخفی بین فرستنده و گیرنده در قالب یک ارتباط نامحسوس است. ایجاد ارتباط نامحسوس باعث می‌شود تا بتوانیم از خرابکاری‌هایی که دشمن در خلال ایجاد یک ارتباط رمز شده انجام می‌دهد جلوگیری کنیم. تمایز ناپذیر بودن بین پوشش خام و پوشش حامل پیام مهمترین راه رسیدن به این هدف است. همان‌طور که قبلاً اشاره شد، در طی سالیان اخیر تحقیقات زیادی در حوزه‌ی نهان‌نگاری انجام گرفته است و به دنبال آن الگوریتم‌های زیادی ارائه شده است، که هدف اصلی همهٔ الگوریتم‌ها تلاش بر افزایش میزان ظرفیت پیام در یک پوشش خاص، کاهش تمایزپذیری بین پوشش حامل پیام و پوشش بدون پیام و پایین بودن پیچیدگی محاسباتی و فضایی الگوریتم پیشنهادی است. البته این نکته قابل ذکر است که دو مسأله افزایش میزان ظرفیت و کاهش تشخیص‌پذیری همواره در تقابل با یکدیگرند، یعنی افزایش ظرفیت درج باعث افزایش تشخیص‌پذیری می‌شود که این خوب نیست. به همین دلیل همواره رقابت، برای ارائه الگوریتم‌هایی با ظرفیت درج بالا، تشخیص‌پذیری کم و پیچیدگی محاسباتی و فضایی پایین، در میان محققان در حوزهٔ نهان‌نگاری وجود دارد. در ادامه قصد داریم به بیان روش نهان‌نگاری با استفاده از کد بپردازیم در ابتدا توضیحاتی در مورد کدگذاری، کدگشایی و تفاوت آن با نهان‌نگاری می‌دهیم. در عمل کدگذاری کانال، کدگذار با اضافه کردن $n-k$ بیت افزونگی به k بیت پیام ورودی یک کدواژه معتبر n بیتی به نام $\boldsymbol{c}$ می‌سازد و کدگشای کانال در تلاش است اثر بردار خطای $\boldsymbol{e}$، که در کانال به صورت تصادفی به کدواژه معتبر $\boldsymbol{c}$ وارد می‌شود و آن را تبدیل به کدواژه نامعتبر $\boldsymbol{r}$ می‌کند، را خنثی کند. معمولاً این کار را با استفاده از بردار مشخصه ناصفر $\boldsymbol{S}$، که از ضرب ماتریس بررسی توازن در کدواژه نامعتبر به دست می‌آید، انجام می‌شود. زیرا پیام اصلی فقط از کدواژه معتبر قابل بازیابی است. از سوی دیگر در طرح‌های نهان‌نگاری درج‌کننده پیام با دستکاری پوشش خام $\boldsymbol{x}$ و تبدیل آن به پوشش حامل پیام $\boldsymbol{y}$ که با اعمال بردار $\boldsymbol{e}$ مناسب به پوشش خام انجام می‌گیرد عمل درج پیام را انجام می‌دهد. فرض ما بر این است که رسانهٔ نهان‌نگاری شده از طریق کانال‌های بدون نویز ارسال می‌شود. بنابراین، استخراج‌کنندهٔ پیام می‌تواند پیام را به راحتی از پوشش حامل پیام استخراج کند. در شکل‌های زیر می‌توانید تفاوت بین یک طرح کدگذاری و یک طرح نهان‌نگاری را ببینید.



تصویر ۳-۱: تصویری از یک سیستم نهان‌نگاری



تصویر ۳-۲: تصویری از سیستم کدگذاری و کدگشایی

تعریف ۳-۱- بیشترین وزن در میان نمایندهٔ همدسته‌های کد را شعاع پوششی[۱] کد گویند و با علامت R نمایش می‌دهند.

همان‌طور که از تعریف شعاع پوششی واضح است، حداکثر تغیراتی که می‌توان در پوشش اعمال کرد تا پیام در پوشش درج شود برابر شعاع پوشی کد است. فرض کنید می‌خواهیم پیام $\mathbf{m}$ را در پوشش $\mathbf{x}$ با استفاده از کدی با ماتریس بررسی‌توازن H پنهان کنیم. اگر $\mathbf{x}\mathrm{H}^{\mathrm{T}} = \mathbf{m}$ آن‌گاه پوشش حامل پیام است و آن را بدون هیچ تغییری ارسال می‌کنیم. و اگر $\mathbf{x}\mathrm{H}^{\mathrm{T}} \neq \mathbf{m}$ به شکل زیر عمل می‌کنیم.

قرار می‌دهیم:

$$\mathbf{m} - \mathbf{x}\mathrm{H}^{\mathrm{T}} = \mathbf{S} \qquad (۱-۰)$$

سپس معادلهٔ زیر را حل می‌کنیم

$$\mathbf{e}\mathrm{H}^{\mathrm{T}} = \mathbf{S}. \qquad (۲-۰)$$

در نهایت پوشش جدید را به صورت $\mathbf{y} = \mathbf{x} + \mathbf{e}$ محاسبه کرده و ارسال می‌کنیم. به بردار $\mathbf{S}$ بردار مشخصه می‌گویند. این روش اولین بار با نام نهان‌نگاری براساس بردار مشخصه کد[۲] توسط کراندال[۳] در مقاله [۳] معرفی شد. در این مقاله از طرح کد $\mathrm{BCH}(n, k, 2)$ برای درج پیام های دودویی استفاده می‌کنیم. چنین کدی دارای شعاع پوششی $R = 3$ است [۱۰]. با استفاده از این کد حداکثر تعداد تغییراتی که در پوشش ایجاد می‌شود تا پیام در پوشش درج شود برابر ۳ است [۱۰].

روش پیشنهادی

هدف اصلی در این مقاله حل معادلهٔ (۲-۰) است. ایدهٔ پیشنهاد شده در این مقاله برای حل معادله (۲-۰) به این ترتیب است که با تعریف یک عدد به عنوان مشخصه بردار مشخصه که نسبت به شیفت برداری پایا است همهٔ بردارهای محتمل $\mathbf{e}$

[۱] Cover Radius
[۲] Syndrom Coding for Steganography
[۳] R.Crandal

که در معادلهٔ (۰-۲) صدق می‌کنند را د سته‌بندی می‌کنیم و سپس با انتخاب یک بردار از هر د سته ایجاد شده به عنوان بردار مولد و ذخیرهٔ آن داخل یک جدول به حل معادله (۰-۲) با رویکردی بسیار ساده می‌پردازیم. در ادامه به شرح دقیق ایدهٔ پیشنهاد شده خواهیم پرداخت.

تعریف ۰-۱- وزن همینگ یک بردار مانند $\mathbf{e}$ عبارت است از تعداد مؤلفه‌های غیر صفر آن بردار که با نماد$\omega(\mathbf{e})$ نشان داده می‌شود.

تعریف ۰-۲- فرض کنید $1 \le t \le n$ کوچکترین عدد با خاصیت $\psi^{(t)}(\mathbf{e}) = \mathbf{e}$ باشد. در این صورت مجموعه‌ای به شکل $\{\mathbf{e}, \psi(\mathbf{e}), \psi^{(2)}(\mathbf{e}), \psi^{(3)}(\mathbf{e}), \dots, \psi^{(t-1)}(\mathbf{e})\} = <\mathbf{e}>$را تولید شده توسط بردار $\mathbf{e}$ نامیده و برداری مانند $\mathbf{e}$ که کل فضا را تولید می‌کند بردار مولد می‌گویند و آن را با $\tilde{\mathbf{e}}$ نمایش می‌دهند.

مجموعه‌های A_i را به صورت زیر تعریف می‌کنیم.

$$A_i = \{\mathbf{e} \in \{0,1\}^n \mid \omega(\mathbf{e}) = i\} \quad , \quad (i = 1, 2, 3)$$

قضیهٔ ۰-۳- فرض کنید $1 \le t \le n$ کوچکترین عدد با خاصیت $\psi^{(t)}(\mathbf{e}) = \mathbf{e}$ باشد در این صورت اگر $\mathbf{e} \in A_i$, $(i = 1, 2, 3)$ آن‌گاه مقدار t برابر n یا $\frac{n}{3}$ است.

اثبات. فرض کنید $\mathbf{e} \in A_1$ در این حالت واضح است که مقدار t برابر n است. فرض کنید:

$$\mathbf{e} = \left(1 \underbrace{0 \cdots 0}_{a} \; 1 \underbrace{0 \cdots 0}_{b}\right) \in A_2$$

در این حالت شرط لازم برای آنکه $t < n$ این است که $a = b$ ولی چون n همواره فرد است$(n = 2^m - 1)$ این شرط هرگز برقرار نمی شود. بنابراین در حالتی که $\mathbf{e} \in \boldsymbol{A_2}$ باز هم مقدار t برابر n است. فرض کنید که $\mathbf{e} \in A_3$ با شد بردار $\mathbf{e}$ را می‌توان به صورت زیر نوشت:

$$\mathbf{e} = \left(1 \underbrace{0 \cdots 0}_{a} \; 1 \underbrace{0 \cdots 0}_{b} \; 1 \underbrace{0 \cdots 0}_{c}\right) \quad ; \quad a + b + c = n - 3$$

اگر $n - 3$ بر 3 بخش‌پذیر باشد آن‌گاه مقادیری برای a, b, c وجود دارد که $a = b = c = \frac{n-3}{3}$. در این حالت مقدار t برابر با $\frac{n}{3}$ است. اگر $n - 3$ بر ۳ بخش‌پذیر نباشد در این صورت مقادیری برای a, b, c وجود ندارد که تساوی $a = b = c = \frac{n-3}{3}$ برقرار شود. در این حالت مقدار t برابر با n است. □

قضیهٔ ۰-۴- تعداد بردارهای مولد از وزن i برابر است با:

(آ) $i=(1,2),\ \frac{|A_i|}{n}$

(ب) $i=3,\left\lceil\frac{|A_i|}{n}\right\rceil$

اثبات. (آ): طبق قضیهٔ ۰-۳، به ازای هر $\mathbf{e}\in A_i\ ,(i=1,2)$، داریم $\psi^{(n)}(\mathbf{e})=\mathbf{e}$. یعنی هر بردار بعد از n بار شیفت برداری تکرار می‌شود که طبق تعریف بردار مولد، هریک از این n بردار را می‌توان به عنوان بردار مولد انتخاب کرد. بنابراین تعداد بردارهای مولد برابر است با: $i=(1,2),\frac{|A_i|}{n}$

اثبات. (ب): فرض کنیم $\mathbf{e}=\left(1\ \underbrace{0\cdots0}_{a}\ 1\ \underbrace{0\cdots0}_{b}\ 1\ \underbrace{0\cdots0}_{c}\right)\in A_3\ ,\ a+b+c=n-3$ باشد. دو حالت زیر را در نظر می‌گیریم.

(۱) اگر $3\nmid n-3$ آن‌گاه $|A_3|=\frac{n(n-1)(n-2)}{6}$ بر n بخش‌پذیر است. زیرا از بین دو عدد متوالی $n-1$ و $n-2$ حتما یکی بر سه بخش‌پذیر است. پس $3\mid(n-2)(n-1)$. از طرفی، همواره داریم $2\mid(n-1)(n-2)$. چون $\gcd(3,2)=1$ می‌توان نوشت: $6\mid(n-2)(n-1)$. از طرفی طبق قضیهٔ ۰-۳ اگر $3\nmid n-3$ ، هر بردار از مجموعه A_3 بعد از n بار شیفت برداری تکرار می شود پس تعداد بردارهای مولد در این حالت برابر است با: $\frac{|A_3|}{n}$.

(۲) اگر $3\mid n-3$ آن‌گاه $|A_3|$ بر n بخش‌پذیر نیست. زیرا $3\nmid(n-2)(n-1)$، پس $6\nmid(n-2)(n-1)$. از طرفی طبق قضیهٔ ۰-۳ درحالتی که $3\mid n-3$، $\frac{n}{3}$ از بردارهای مجموعه A_3 بعد از $\frac{n}{3}$ مرتبه شیفت برداری تکرار می‌شوند (بردار $\mathbf{e}$ را در نظر بگیرید، هنگامی که رابطه $a=b=c=\frac{n-3}{3}$ برقرار باشد، این بردار بعد از $\frac{n}{3}$ مرتبه شیفت برداری به خود می‌رسد. همهٔ این $\frac{n}{3}$ بردار که در این شیفت برداری وجود دارند دارای این خاصیت هستند.). برای این $\frac{n}{3}$ بردار، یک بردار را به عنوان بردار مولد در نظر می‌گیریم. با کم کردن این اعضا از مجموعهٔ A_3، $|A_3|-\frac{n}{3}=\frac{n^3-3n^2}{6}$. عدد $\frac{n^3-3n^2}{6}$ بر n بخش‌پذیر است زیرا از بین اعداد n و $n-3$ یکی حتماً زوج است، پس $2\mid n(n-3)$. از طرفی، طبق فرض $3\mid n-3$ و در نتیجه $6\mid n(n-3)$. پس عدد $\frac{n^3-3n^2}{6}$ بر n بخش‌پذیر است. یعنی، $\frac{n^3-3n^2}{6}$ تعداد از بردارها بعد از n مرتبه شیفت برداری تکرار می‌شوند. بنابراین می‌توان از بین $\frac{n^3-3n^2}{6}$ تعداد عضو باقی مانده از اعضای مجموعه A_3، با توجه به تعریف بردار مولد، $\frac{n(n-3)}{6}$ عضو را به عنوان بردار مولد انتخاب کرد. بنابراین تعداد بردارهای مولد مجموعه A_3 در حالتی که $3\mid n-3$ برابر است با $1+\frac{n(n-3)}{6}$ ($\frac{n(n-3)}{6}$ بردار مولد، $\frac{n^3-3n^2}{6}$ تعداد عضو از اعضای مجموعه A_3 را تولید کرده و یک بردار باقی مانده، $\frac{n}{3}$ عضو باقی مانده از این مجموعه را تولید می‌کند.). حال باید نشان دهیم

اگر $3 \mid n-3$ آن‌گاه تساوی $\left\lceil \frac{|A_i|}{n} \right\rceil = \frac{n(n-3)}{6} + 1$ برقرار است. چون $6 \mid n(n-3)$ پس $\frac{n(n-3)}{6}$ یک عدد صحیح است. بنابراین:

$$\left\lceil \frac{|A_i|}{n} \right\rceil = \left\lceil \frac{(n-1)(n-2)}{6} \right\rceil = \left\lceil \frac{(n(n-3)+2)}{6} \right\rceil \underset{(a)}{=} \left\lceil \frac{(n(n-3))}{6} \right\rceil + \left\lceil \frac{2}{6} \right\rceil$$

$$= \frac{n(n-3)}{6} + 1 . \square$$

(a): چون $\frac{n(n-3)}{6}$ یک عدد صحیح است.

مجموعه‌های B_i را به صورت زیر تعریف می‌کنیم:

$$B_j = \{ e \in A_j \mid \forall e, e'; < e > \neq < e' > \}$$

با فرض $\mathbf{e_i} = \left(\underbrace{0 \cdots 0}_{i-1} \ 1 \ \underbrace{0 \cdots 0}_{n-i} \right)$:

$$B_1 = \{\mathbf{e_1}\} .$$

همان‌طور که در قضیهٔ ۴-۴ بیان شد تعداد بردارهای مولد از وزن یک، برابر است با: $\frac{|A_1|}{n} = 1$.

$$B_2 = \{\mathbf{e_1} + \mathbf{e_i} \mid i = 2, 3, \dots, \frac{n+1}{2}\} .$$

همچنین بنا به قضیهٔ ۴-۴ تعداد بردارهای مولد از وزن دو، برابر است با: $\frac{|A_2|}{n} = \frac{n-1}{2}$.

با معرفی مجموعه B_2 به شکل فوق از ایجاد اشتراک بین مجموعه‌های تولید شده توسط اعضای B_2 جلوگیری می‌شود. در ادامه با فرض شرط‌هایی بردارهای مولد مجموعهٔ B_3 را نیز تعریف می‌کنیم.

$\tilde{\mathbf{e}}(\tilde{\mathbf{e}} = \left(1 \ \underbrace{0 \cdots 0}_{a} \ 1 \ \underbrace{0 \cdots 0}_{b} \ 1 \ \underbrace{0 \cdots 0}_{c} \right) \in B_3$ بردار مولدی از وزن سه) دارای ویژگی‌های زیر است

(۱) یکی از سه درایه برابر یک موجود در بردار باید در اولین مکان باشد.

(۲) از بین بردارهایی که شرط (۱) را دارند برداری که دارای کمترین مقدار برای a است انتخاب می‌شود.

(۳) اگر $a = c$ آن‌گاه $a = b = c$

(۴) $a + b + c = n - 3 \ , \ a \leq \min\{b, c\}$

براساس شرط‌های (۱)، (۲)، (۳) و (۴) جدول ۱ برای $n = 31$ به منظور نمایش مقدارهای مجاز a, b در بردارهای مولد با وزن ۳ تنظیم شده است (مکان‌های مجاز برای a, b را با * مشخص شده‌اند).

جدول ۱: مقادیر مجاز a, b در بردارهای مولد با وزن ۳

a / b	0	1	2	3	4	5	6	7	8	9
0	*									
1	*	*								
2	*	*	*							
3	*	*	*	*						
4	*	*	*	*	*					
5	*	*	*	*	*	*				
6	*	*	*	*	*	*	*			
7	*	*	*	*	*	*	*	*		
8	*	*	*	*	*	*	*	*	*	
9	*	*	*	*	*	*	*	*	*	*
10	*	*	*	*	*	*	*	*	*	
11	*	*	*	*	*	*	*	*	*	
12	*	*	*	*	*	*	*	*		
13	*	*	*	*	*	*	*	*		
14	*	*	*	*	*	*	*			
15	*	*	*	*	*	*	*			
16	*	*	*	*	*	*				
17	*	*	*	*	*	*				
28	*	*	*	*	*					
19	*	*	*	*	*					
20	*	*	*	*						
21	*	*	*	*						
22	*	*	*							
23	*	*	*							
24	*	*								
25	*	*								
26	*									
27	*									

لم ۰-۵- در حالت کلی برای زوج a, b داریم:

$$a \in \left\{0, 1, \dots, \left\lfloor \frac{(n-3)}{3} \right\rfloor\right\}, b \in \{0, 1, \dots, n-4\}$$

اثبات. اگر b بیشتر از $n-4$ باشد آن‌گاه با شرط (۳) در تناقض است. اگر a بیشتر از $\frac{n-3}{3}$ باشد آن‌گاه با شرط (۴) در تناقض است. □

کد $BCH(n,k,2)$ با ماتریس بررسی توازن $H=\begin{bmatrix}1 & \alpha & (\alpha)^2 & \dots & (\alpha)^{n-1}\\ 1 & \alpha^3 & (\alpha^3)^2 & \dots & (\alpha^3)^{n-1}\end{bmatrix}$ را در نظر بگیرید برای درج پیام $\mathbf{m}=[m_1,m_2]$ در پوشش $\mathbf{x}=(x_0,x_1,\dots.x_{n-2},x_{n-1})$، ابتدا مقدار $\mathbf{S}=\mathbf{m}-\mathbf{x}H^T$ محاسبه شود. قرار دهید: $\mathbf{S}=[S_1,S_2]$.

تعریف ۰-۶- $\frac{S_2}{S_1^3}\in GF(2^m)$ را به عنوان مشخصهٔ بردار مشخصه تعریف می‌کنیم و با علامت $N(\mathbf{S})$ نشان می‌دهیم.

گزارهٔ ۰-۷- مقدار $N(\mathbf{S})$ نسبت به شیفت برداری پایا است [۱۱].□

با توجه به گزارهٔ ۴-۷- برای همهٔ اعضای مجموعهٔ $<\tilde{\mathbf{e}}>$ مقدار $N(\mathbf{S})$ عدد ثابتی است. مجموعه‌های D_i را به صورت زیر تعریف می‌کنیم.

$$D_i=\{N_{\tilde{e}}(\mathbf{S})\,|\,\mathbf{S}=\tilde{\mathbf{e}}H^T,\tilde{\mathbf{e}}\in B_i\}\ ,\ (i=1,2,3).$$

گزارهٔ ۰-۸- اگر $\tilde{\mathbf{e}}_x\neq\tilde{\mathbf{e}}_y$ و $\tilde{\mathbf{e}}_x,\tilde{\mathbf{e}}_y\in B_2$ آنگاه $N_{\tilde{\mathbf{e}}_x}(\mathbf{S})\neq N_{\tilde{\mathbf{e}}_y}(\mathbf{S})$.

اثبات. فرض کنید $\tilde{\mathbf{e}}_x\neq\tilde{\mathbf{e}}_y$ آن‌گاه:

$$\tilde{\mathbf{e}}_x=\mathbf{e}_1+\mathbf{e}_i\quad,\quad\tilde{\mathbf{e}}_y=\mathbf{e}_1+\mathbf{e}_j\qquad i,j\in\left\{2,3,\dots,\frac{n+1}{2}\right\},i\neq j$$

$$N_{\tilde{\mathbf{e}}_x}(\mathbf{S})=\frac{1+\alpha^{3(i-1)}}{(1+\alpha^{i-1})^3}\quad,\quad N_{\tilde{\mathbf{e}}_y}(\mathbf{S})=\frac{1+\alpha^{3(j-1)}}{(1+\alpha^{j-1})^3}$$

برای اثبات گزاره ابتدا ثابت می‌کنیم اگر t جواب معادله $\frac{1+x^3}{(1+x)^3}=\beta$ باشد این معادلهٔ حداکثر یک جواب دیگر دارد و آن جواب برابر t^{-1} است.

برای اثبات این مطلب ابتدا معادله $\frac{1+x^3}{(1+x)^3}=\beta$ را به شکل زیر ساده می‌کنیم (توجه داشته باشید همهٔ محاسبات به کار رفته در این اثبات، در میدان‌های گسترش یافته $\mathbb{F}_2$ است).

$$\frac{1+x^3}{(1+x)^3}=\frac{(1+x)(1+x+x^2)}{(1+x)(1+x)^2}=\frac{1+x+x^2}{1+x^2}=\beta\Rightarrow(1+\beta)x^2+x+(1+\beta)=0\ (*)$$

معادله * بنا به قضیهٔ اساسی جبر حداکثر دو جواب دارد و با توجه شکل معادله دو جواب معادله معکوس ضربی یکدیگرند. حال اگر $i \in \{2,3,\dots,\frac{n+1}{2}(\ )\}$ یک جواب معادله $\beta = \frac{1+x^3}{(1+x)^3}$ باشد، $\alpha^{n-(i-1)}$ (معکوس ضربی α^i) جواب دیگر این معادله است. از طرفی با توجه به محدودهٔ i:

$$\frac{n+1}{2} \le n-(i-1) \le n-1$$

(در حالتی که $i = \frac{n+1}{2}$ باشد مقدار $n-(i-1)$ نیز برابر $\frac{n+1}{2}$ است.). با توجه محدودهٔ $n-(i-1)$ به ازای هر $i \ne j$ و $i,j \in \left\{2,3,\dots,\frac{n+1}{2}\right\}$، $N_{\tilde{e}_x} \ne N_{\tilde{e}_y}$. □

گزارهٔ ۰-۹- همواره:

$$D_1 \cap D_2 = \emptyset$$

اثبات.

$$x \in D_1 \Longrightarrow x = 1$$

$$\forall x \in D_2, x = \frac{1+\alpha^{3(i-1)}}{(1+\alpha^{i-1})^3}, \quad i \in \left\{2,3,\dots,\frac{n+1}{2}\right\}$$

باید نشان دهیم به ازای هر $x \in D_2$ رابطهٔ $x = \frac{1+\alpha^{3(i-1)}}{(1+\alpha^{i-1})^3} \ne 1$ برقرار است. قرار دهید $i' = i-1$ آن‌گاه به ازای هر $x \in D_2$، $x = \frac{1+\alpha^{3i}}{(1+\alpha^i)^3}$ و اگر به ازای $x \in D_2$ قرار دهیم: $i' \in \left\{1,2,\dots,\frac{n-1}{2}\right\}$ آن‌گاه رابطهٔ $x = \frac{1+\alpha^{3i'}}{(1+\alpha^{i'})^3} = 1$ را داریم که با توجه به مقادیر ممکن برای i'، $\alpha^{i'}(1+\alpha^{i'}) = 0$ تناقض است. □

گزارهٔ ۴-۱۰ همواره:

$$D_3 \cap D_1 = \emptyset$$

اثبات:

$$x \in D_1 \Longrightarrow x = 1$$

$$\forall x \in D_3, x = \frac{1+\alpha^{3(a+1)}+\alpha^{3(a+b+2)}}{(1+\alpha^{a+1}+\alpha^{a+b+2})^3}$$

همان‌طور که اشاره شد مقادیر a, b باید در شروط (۱)، (۲)، (۳) و (۴) صدق کنند. باید نشان دهیم برای هر $x \in D_3$ مقدار $x \ne 1$. به عبارت دیگر نشان می‌دهیم، به ازای مقادیری از a, b که در شروط (۱)، (۲)، (۳) و (۴) صدق می‌کنند، رابطهٔ $\frac{1+\alpha^{3(a+1)}+\alpha^{3(a+b+2)}}{(1+\alpha^{a+1}+\alpha^{a+b+2})^3} \ne 1$ برقرار است. فرض کنید (فرض خلف) $\frac{1+\alpha^{3(a+1)}+\alpha^{3(a+b+2)}}{(1+\alpha^{a+1}+\alpha^{a+b+2})^3} = 1$ در این صورت

رابطهٔ داریم: $1+\alpha^{3(a+1)}+\alpha^{3(a+b+2)}=1+\alpha^{3(a+1)}+\alpha^{3(a+b+2)}+M$ که در این رابطه مقدار M برابر است با: $M=\alpha^{a+1}(1+\alpha^{a+1})(1+\alpha^{b+1})(1+\alpha^{a+b+2})$ حال باید نشان دهیم که $M\neq 0$ برای این منظور باید سه شرط زیر را اثبات کنیم.

۱. $a+1\neq 0 \pmod n$

۲. $b+1\neq 0 \pmod n$

۳. $a+b+2\neq 0 \pmod n$

با توجه به شروط (۱)، (۲)، (۳) و (۴) سه شرط فوق نتیجه می‌شود. □

در جدول ۲ مقدار $N(\mathbf{S})$ متناظر با هریک از ۱۴۵ زوج a,b که در جدول ۱ نمایش داده شد، محاسبه شده است.

جدول ۲: $\omega(\tilde{e})=3,\ N(\mathbf{S})$

b \ a	0	1	2	3	4	5	6	7	8	9
0	α^{16}									
1	α^{29}	α								
2	α^{22}	$S_1=0$	α^{29}							
3	α^{2}	α^{27}	α^{7}	α^{2}						
4	α^{12}	α^{18}	α^{30}	α^{14}	α^{16}					
5	α^{25}	α^{13}	α^{15}	$S_1=0$	α^{17}	α^{27}				
6	α^{21}	0	α^{28}	α^{5}	α^{29}	α^{7}	α^{15}			
7	α^{19}	α^{4}	α^{10}	α^{23}	α^{16}	α^{14}	α^{15}	α^{4}		
8	α^{19}	α^{20}	α^{22}	α^{8}	α^{12}	α^{25}	α	α^{3}	α^{4}	
9	α^{2}	α^{24}	α^{24}	α^{5}	α^{1}	α^{29}	α^{27}	α^{28}	α^{3}	α
10	α^{27}	α^{6}	α^{23}	α^{25}	α^{25}	α^{11}	α^{6}	α^{16}	α^{2}	
11	α^{19}	α^{19}	α^{28}	α^{26}	α^{14}	α^{30}	α^{23}	$S_1=0$	α^{11}	
12	α^{2}	α	α^{6}	α^{15}	α^{8}	α^{29}	α^{22}	α^{24}		
13	α^{30}	α^{11}	α^{30}	0	α^{26}	α^{25}	α^{23}	α^{10}		
14	α^{8}	α^{20}	α^{20}	α^{5}	α^{17}	0	$S_1=0$			
15	α^{24}	α^{7}	α^{13}	α^{8}	α^{5}	α^{20}	α^{12}			
16	$S_1=0$	α^{21}	α^{15}	α^{14}	α^{13}	α^{22}				
17	α^{9}	α^{7}	α^{26}	α^{9}	α^{18}	α^{13}				
28	0	α^{18}	α^{19}	α^{6}	α^{27}					
19	α^{10}	α^{4}	α^{28}	α^{17}	α^{21}					

20	α^3	α^{28}	α^{21}	α^8						
21	α^{16}	α^{23}	α^{30}	α^{12}						
22	α^{10}	α^{18}	0							
23	α^{26}	α^7	α^{11}							
24	α^9	α^3								
25	α^{14}	α^4								
26	α^9									
27	α^{17}									

در جدول۳ مقدار$\mathrm{N}(\mathbf{S})$ متناظر با بردار های مجموعه B_2 را به ازای $\mathrm{i} \in \left\{2, 3, \dots, \frac{\mathrm{n}+1}{2}\right\}$ برای $\mathrm{n} = 31$ محاسبه کرده‌ایم.

جدول ۳: $\boldsymbol{\omega(\tilde{e}) = 2,\ N(S)}$

i	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{N}(\mathbf{S})$	α^6	α^{12}	α^{22}	α^{24}	α^{18}	α^{13}	α^{21}	α^{17}	α^{20}	α^5	α^{10}	α^{26}	α^9	α^{11}	α^3

برای انجام نهان‌نگاری با استفاده از کد $\mathrm{BCH}(\mathrm{n}, \mathrm{k}, 2)$، بدون حل چندجمله‌ای، از خاصیت موجود در گزارهٔ ۴-۷ استفاده می‌کنیم. به این صورت که، برای بردارهای مولد اعضای مجموعه‌های $\mathrm{B_i}$ $(\mathrm{i} = 1, 2, 3)$مقدار $\mathrm{N}(\mathbf{S})$ را مشخص می‌کنیم به این ترتیب هنگام حل معادله (۲-۰)، با استفاده از مقدار$\mathbf{S} = [\mathrm{S}_1, \mathrm{S}_2]$، بردار مولد $\mathbf{e}$ یعنی $\tilde{\mathbf{e}}$ را به دست می‌آید. در ادامه الگوریتم رسیدن از بردار مولد $\tilde{\mathbf{e}}$ و $\mathbf{S} = [\mathrm{S}_1, \mathrm{S}_2]$ به مقدار دقیق بردار خطای $\mathbf{e}$، که در معادلهٔ (۲-۰) صدق می‌کند ارائه می‌شود. الگوریتم مورد نظر برای رسیدن به بردار $\mathbf{e}$، که در معادلهٔ (۲-۰) صدق کند برگرفته از مقاله [۱۱] است. البته چون نیاز بود این روش را برای نهان‌نگاری براساس کدگذاری بردار مشخصه تعمیم دهیم، تغییراتی در آن اعمال کرده‌ایم؛ زیرا هنگامی که می‌خواهیم از مقدار $\frac{\mathrm{S}_2}{\mathrm{S}_1^3}$ برای بردار های خطای $\mathbf{e}$ با وزن ۳ استفاده کنیم با حالت تعریف نشده $\mathrm{S}_1 = 0$ مواجه می‌شویم.

معرفی الگوریتم و اجزای آن

در این قسمت قصد داریم به معرفی الگوریتم پیشنهادی بپردازیم. قبل از شروع، ابتدا اجزای مختلف الگوریتم را تعریف و بررسی می‌کنیم. مقادیر $\mathrm{a}, \mathrm{b}, \mathrm{c}$ به ترتیب مکان قرار گرفتن اولین، دومین و سومین ۱ در بردار مولد $\tilde{\mathbf{e}}$ و $\mathrm{a}', \mathrm{b}', \mathrm{c}'$ مکان قرار گرفتن اولین، دومین و سومین ۱ در بردار $\mathbf{e}$ که در معادلهٔ (۲-۰) صدق می‌کند، هستند. مقدار $\mathbf{S} = [\mathrm{S}_1, \mathrm{S}_2]$ در ورودی الگوریتم از معادلهٔ (۲-۰) به دست می‌آید. منظور از $\mathrm{T}(\mathrm{N}(\mathbf{S}))$ در الگوریتم زیر، بردار مولد (بردارهای مولد) متناظر با مقدار

$\mathrm{N}(\mathbf{S})$ است که در فاز پیش محاسبه[1] در داخل جدولی با نام T ذخیره شده است (جدول ۴ و جدول ۶ جداول فاز پیش محاسبه برای $\mathrm{n} = 31$ هستند). $\mathrm{t} = 3^{-1} \pmod{\mathrm{n}}$ است. به ازای مقادیری از n که مقدار یا جوابی برای t وجود ندارد $(\mathrm{n} = 2^{\mathrm{m}} - 1, \mathrm{m} = 2\,\mathrm{k}, \mathrm{k} \in \mathbb{Z} \Longrightarrow \gcd(\mathrm{n}, 3) \neq 1)$ اگر با مرحلهٔ (۶) الگوریتم (۱) مواجه شویم نمی‌توانیم مقدار i را محاسبه کنیم. به دنبال آن نمی‌توانیم مقادیر $\mathrm{a}', \mathrm{b}', \mathrm{c}'$ را محاسبه کنیم (چون t قابل محاسبه نیست) در این حالت برای به دست آوردن بردار $\mathbf{e}$، که در معادلهٔ (۲-۰) می‌کند، باید به ازای همهٔ مقادیر i مقادیر $\mathrm{a}', \mathrm{b}', \mathrm{c}'$ متناظر را محاسبه کنیم تا بتوانیم بردار $\mathbf{e}$ که در معادلهٔ (۲-۰) صدق می‌کند را به دست بیاوریم.

الگوریتم ۱: پیدا کردن مکان یک‌های بردار $\mathbf{e}$ در معادلهٔ (۲-۰)

۱- ورودی: $\mathbf{S} = [\mathrm{S}_1, \mathrm{S}_2]$

۲- محاسبه: $\mathrm{N}(\mathbf{S}) = \frac{\mathrm{S}_2}{\mathrm{S}_1^3}$

۳- محاسبه: $\tilde{\mathbf{e}} = \mathrm{T}(\mathrm{N}(\mathbf{S}))$

۴- محاسبه: $\tilde{\mathbf{e}}\mathrm{H}^{\mathrm{T}} = [\mathrm{S}_1', \mathrm{S}_2']$

۵- اگر $\mathrm{S}_1 = 0$ برو به خط ۶ در غیر این‌صورت بده: $\mathrm{i} = \left(\deg(\mathbf{S}_1) - \deg(\mathbf{S}_1')\right) (\mathrm{mod}\ \mathrm{n})$

۶- $\mathrm{i} = \mathrm{t}\left(\left(\deg(\mathbf{S}_2) - \deg\left(\mathbf{S}_2'\right)\right) (\mathrm{mod}\ \mathrm{n})\right) \pmod{\mathrm{n}}$

۷- محاسبه: $\mathrm{a}' = \mathrm{a} + \mathrm{i} \pmod{\mathrm{n}},\ \mathrm{b}' = \mathrm{b} + \mathrm{i} \pmod{\mathrm{n}},\ \mathrm{c}' = \mathrm{c} + \mathrm{i} \pmod{\mathrm{n}}$

در نهان‌نگاری همواره تلاش ما بر این است که در اثر درج پیام بردارهای با وزن کمتر به پوشش خام اعمال شود. بنابراین مقادیر موجود در D_1 و D_2 را از مجموعه D_3 حذف می‌کنیم و قرار می‌دهیم $\mathrm{U} = \mathrm{D}_3 - \{\mathrm{D}_1 \cup \mathrm{D}_2\}$. همچنین بردارهای مولد متناظر با اعضای حذف شده از مجموعه D_3 را از مجموعه B_3 حذف می‌کنیم. با انجام این کار همواره کمترین تغییرات ممکن را به پوشش خام در جهت درج پیام اعمال می‌کنیم. با دسته‌بندی‌های انجام شده برای مقادیر مختلف $\mathrm{N}(\mathbf{S})$ به سه مجموعهٔ $\mathrm{D}_1, \mathrm{D}_2, \mathrm{U}$، می‌توان با الگوریتم ۱ به راحتی مقدار یا مقادیر مختلف بردار $\mathbf{e}$ را، که در معادله (۲-۰) صدق می‌کنند به دست آورد.

همان‌طور که در جدول ۵ مشاهده می‌نمایید اعضای موجود در مجموعه D_2، که باید از مجموعهٔ D_3 حذف شود با رنگ قرمز مشخص شده‌اند.

[1] Pre-compute

جدول ۴: $\omega(\tilde{e}) = 2$, T

N(S)	α^3	α^5	α^6	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{17}	α^{18}	α^{20}	α^{21}	α^{22}	α^{24}	α^{26}
(a,b)	(1,16)	(1,11)	(1,2)	(1,14)	(1,12)	(1,15)	(1,3)	(1,7)	(1,9)	(1,6)	(1,10)	(1,8)	(1,4)	(1,5)	(1,13)

جدول ۵: $\omega(\tilde{e}) = 3, N(S)$

b \ a	0	1	2	3	4	5	6	7	8	9
0	α^{16}									
1	α^{29}	α								
2	α^{22}	$S_1 = 0$	α^{29}							
3	α^2	α^{27}	α^7	α^2						
4	α^{12}	α^{18}	α^{30}	α^{14}	α^{16}					
5	α^{25}	α^{13}	α^{15}	$S_1 = 0$	α^{17}	α^{27}				
6	α^{21}	0	α^{28}	α^5	α^{29}	α^7	α^{15}			
7	α^{19}	α^4	α^{10}	α^{23}	α^{16}	α^{14}	α^{15}	α^4		
8	α^{19}	α^{20}	α^{22}	α^8	α^{12}	α^{25}	α	α^3	α^4	
9	α^2	α^{24}	α^{24}	α^5	α	α^{29}	α^{27}	α^{28}	α^3	α
10	α^{27}	α^6	α^{23}	α^{25}	α^{25}	α^{11}	α^6	α^{16}	α^2	
11	α^{19}	α^{19}	α^{28}	α^{26}	α^{14}	α^{30}	α^{23}	$S_1 = 0$	α^{11}	
12	α^2	α	α^6	α^{15}	α^8	α^{29}	α^{22}	α^{24}		
13	α^{30}	α^{11}	α^{30}	.	α^{26}	α^{25}	α^{23}	α^{10}		
14	α^8	α^{20}	α^{20}	α^5	α^{17}	0	$S_1 = 0$			
15	α^{24}	α^7	α^{13}	α^8	α^5	α^{20}	α^{12}			
16	$S_1 = 0$	α^{21}	α^{15}	α^{14}	α^{13}	α^{22}				
17	α^9	α^7	α^{26}	α^9	α^{18}	α^{13}				
18	0	α^{18}	α^{19}	α^6	α^{27}					
19	α^{10}	α^4	α^{28}	α^{17}	α^{21}					
20	α^3	α^{28}	α^{21}	α^8						
21	α^{16}	α^{23}	α^{30}	α^{12}						
22	α^{10}	α^{18}	0							
23	α^{26}	α^7	α^{11}							
24	α^9	α^3								
25	α^{14}	α^4								
26	α^9									
27	α^{17}									

جدول ۶: $\boldsymbol{\omega(\tilde{e}) = 3, T}$

$N(\mathbf{S})$	α^1	α^2	α^4	α^7	α^8	α^{14}	α^{15}	α^{16}
(a, b, c)	(1,3,5)	(1,2,6)	(1,3,11)	(1,4,8)	(1,5,14)	(1,5,10)	(1,4,10)	(1,2,3)
(a, b, c)	(1,8,17)	(1,5,9)	(1,9,17)	(1,7,14)	(1,6,19)	(1,7,15)	(1,8,15)	(1,6,11)
(a, b, c)	(1,6,16)	(1,2,12)	(1,10,19)	(1,3,19)	(1,2,17)	(1,6,18)	(1,8,16)	(1,6,14)
(a, b, c)	(1,11,21)	(1,10,21)	(1,3,23)	(1,3,21)	(1,5,21)	(1,5,22)	(1,5,18)	(1,9,20)
(a, b, c)	(1,3,16)	(11,2,5)	(1,3,29)	(1,3,27)	(1,5,26)	(1,2,28)	(1,4,21)	(1,2,24)

$N(\mathbf{S})$	α^{19}	α^{23}	α^{25}	α^{27}	α^{28}	α^{29}	α^{30}	$S_1 = 0$	0
(a, b, c)	(1,2,10)	(1,5,13)	(1,2,8)	(1,3,7)	(1,4,11)	(1,2,4)	(1,4,9)	(1,3,6)	(1,3,10)
(a, b, c)	(1,2,21)	(1,4,15)	(1,7,16)	(1,7,13)	(1,9,19)	(1,4,7)	(1,7,19)	(1,5,11)	(1,5,19)
(a, b, c)	(1,2,14)	(1,8,20)	(1,5,16)	(1,8,18)	(1,4,16)	(1,6,13)	(1,2,16)	(1,9,21)	(1,7,22)
(a, b, c)	(1,3,15)	(1,8,22)	(1,6,17)	(1,2,13)	(1,4,24)	(1,7,17)	(1,4,18)	(1,8,23)	(1,2,21)
(a, b, c)	(1,4,23)	(1,3,25)	(1,7,21)	(1,6,25)	(1,3,24)	(1,7,20)	(1,4,26)	(1,2,19)	(1,4,27)

نتایج اجرایی

در این بخش به منظور تفهیم بهتر و سریع‌تر الگوریتم ۱ به بیان چند مثال می‌پردازیم. تمام محاسبات موجود در این مقاله و جداول براساس چندجمله‌ای اولیه $x^5 + x^2 + 1$ در $GF(2^5)$ انجام شده است.

مثال ۱-۵: فرض کنیم: $t = 2,\ m = 5,\ n = 31,\ \mathbf{m} = [20, 10]$.

(آ) با فرض پوشش $\mathbf{x} = [1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,0\,1\,0\,1\,1\,1]$:

$$\mathbf{x}H^T = [\alpha^6, \alpha^{20}] = [10, 12]$$

$$\mathbf{S} = \mathbf{m} - \mathbf{x}\,H^T = [S_1, S_2] = [\alpha^{24}, \alpha^{19}] = [30, 6]\ .$$

چون $\mathbf{S} \neq [0, 0]$ پس برای درج پیام نیاز به اعمال تغییراتی در پوشش $\mathbf{x}$ داریم. به منظور پیدا کردن خطای $\mathbf{e}$ به این شکل عمل می‌کنیم: با توجه به مقدار $N(\mathbf{S}) = \frac{S_2}{S_1^3} = \frac{\alpha^{19}}{(\alpha^{24})^3} = \alpha^9$ و با استفاده از جدول ۴ بردار مولد $\tilde{\mathbf{e}}$ و مکان‌های عدد ۱ را در بردار مولد $\tilde{\mathbf{e}}$ پیدا کرده و در ادامه با استفاده از الگوریتم ۱ بردار $\tilde{\mathbf{e}}$ را به دست آورده و به پوشش اعمال می‌کنیم. با توجه به جدول ۴، $(a, b) = (1, 14)$. لذا، $\tilde{\mathbf{e}}H^T = [S_1', S_2'] = [\alpha^{14}, \alpha^{20}]$ پس $\deg(S_1') = 14$ و در نتیجه مقدار i به صورت زیر محاسبه می‌شود.

$$i = \big(\deg(S_1) - \deg(S_1')\big) (\mathrm{mod}\ 31) = 10\ .$$

پس مکان ۱های بردار $\mathbf{e}$ به صورت زیر است.

$$a' = (a + i)\ (\mathrm{mod}\ 31) = 1 + 10 = 11\ (\mathrm{mod}\ 31) = 11$$

$$b' = (b + i) (\mathrm{mod}\ 31) = 14 + 10 = 24\ (\mathrm{mod}\ 31) = 24\ .$$

در نتیجه: $\mathbf{e} = \mathbf{e}_{11} + \mathbf{e}_{24}$. پس پوشش جدید ما برابر است با $\mathbf{y} = \mathbf{x} + \mathbf{e}$ که این پوشش حامل پیام است $(\mathbf{m} = \mathbf{y}\mathrm{H}^{\mathrm{T}})$.

(ب) با فرض پوشش $\mathbf{x} = [1\,1\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0\,1]$:

$$\mathbf{x}\mathrm{H}^{\mathrm{T}} = [\,\alpha^{7}, \alpha^{15}] = [\,20, 31]\ .$$

$$\mathbf{S} = \mathbf{m} - \mathbf{x}\mathrm{H}^{\mathrm{T}} = [\mathrm{S}_1, \mathrm{S}_2] = [0, \alpha^{22}] = [0,21]\ .$$

چون $\mathbf{S} \neq [0, 0]$، پس برای درج پیام نیاز به اعمال تغییراتی در پوشش $\mathbf{x}$ داریم. به منظور پیدا کردن خطای $\mathbf{e}$ به این شکل عمل می‌کنیم: با توجه به مقدار $\mathrm{S}_1 = 0$ و با استفاده از جدول ۶ بردار مولد $\tilde{\mathbf{e}}$ و مکان‌های عدد ۱ را در بردار مولد $\tilde{\mathbf{e}}$ پیدا کرده در ادامه، با استفاده از الگوریتم ۱، بردار $\mathbf{e}$ را به دست آورده و به پوشش اعمال می‌کنیم. با توجه به جدول ۶، $(\mathrm{a}, \mathrm{b}, \mathrm{c}) = (1, 3, 6)$ (هر ۵ حالت $\mathrm{S}_1 = 0$ که در جدول ۶، آمده است جوابی برای مسأله ما است.) چون $\tilde{\mathbf{e}}\mathrm{H}^{\mathrm{T}} = [\mathrm{S}_1', \mathrm{S}_2'] = [0\,, \alpha^{7}]$، $\deg(\mathrm{S}_2') = 7$. با دانستن $\deg(\mathrm{S}_2) = 22$، i به صورت زیر محاسبه می‌شود:

$$\mathrm{i} = 21\ \Big(\big(\deg(\mathrm{S}_2) - \deg(\mathrm{S}_2')\big)(\mathrm{mod}\ 31)\Big)\ (\mathrm{mod}\ 31) = 5\,.$$

پس مکان یک‌های بردار$\mathbf{e}$ به شکل زیر است:

$$\mathrm{a}' = (\mathrm{a} + \mathrm{i})\ (\mathrm{mod}\ 31) = 1 + 5 = 6\ (\mathrm{mod}\ 31) = 6\,.$$

$$\mathrm{b}' = (\mathrm{b} + \mathrm{i})(\mathrm{mod}\ 31) = 3 + 5 = 8\ (\mathrm{mod}\ 31) = 8\,.$$

$$\mathrm{c}' = (\mathrm{c} + \mathrm{i})(\mathrm{mod}\ 31) = 6 + 5 = 11\ (\mathrm{mod}\ 31) = 11\,.$$

در نتیجه $\mathbf{e} = \mathbf{e}_6 + \mathbf{e}_8 + \mathbf{e}_{11}$. پس پوشش جدید برابر است با $\mathbf{y} = \mathbf{x} + \mathbf{e}$ $(\mathbf{m} = \mathbf{y}\mathrm{H}^{\mathrm{T}})$.

جدول ۷: همهٔ جواب‌های ممکن مثال

$(\mathrm{a}, \mathrm{b}, \mathrm{c})$	$(\mathrm{a}', \mathrm{b}', \mathrm{c}')$	$\mathbf{e}$
(1,5, 11)	(14, 18, 24)	$\mathbf{e}_{14} + \mathbf{e}_{18} + \mathbf{e}_{24}$
(1, 9, 21)	(7, 19. ,30)	$\mathbf{e}_{7} + \mathbf{e}_{19} + \mathbf{e}_{30}$
(1, 8, 23)	(9, 16,31)	$\mathbf{e}_{9} + \mathbf{e}_{16} + \mathbf{e}_{31}$
(1, 2,19)	(2, 3,20)	$\mathbf{e}_{2} + \mathbf{e}_{3} + \mathbf{e}_{20}$

(پ) با فرض پوشش : $\mathbf{x} = [1\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1]$

$$\mathbf{x}\mathrm{H}^{\mathrm{T}} = [\,\alpha^{5}\,, \alpha^{21}] = [\,5, 24]\,.$$

$$\mathbf{S} = \mathbf{m} - \mathbf{x}\mathrm{H}^{\mathrm{T}} = [\mathrm{S}_1, \mathrm{S}_2] = [\alpha^{10}, \alpha^{30}] = [17, 18]\,.$$

چون $\mathbf{S} \neq [0,0]$ پس پوشش $\mathbf{x}$ احتیاج به تغییر برای درج شدن پیام در آن را دارد. به منظور پیدار کردن بردار تغییر یا خطا $\mathbf{e}$ در جهت اعمال به پوشش $\mathbf{x}$ و درج پیام در پوشش به شکل زیر عمل می‌کنیم:

چون مقدار $\mathrm{N}(\mathbf{S}) = \frac{S_2}{S_1^3} = \frac{\alpha^{30}}{(\alpha^{10})^3} = 1$ در جدول ۴ و جدول ۶ موجود نیست، پس $\mathbf{e}$ با یکی از $\mathbf{e}_i, i \in \{1,2,\dots,31\}$ برابر است. از طرفی $\tilde{\mathbf{e}} = \mathbf{e}_1$ است پس با توجه به مقدار $[S_1', S_2'] = [1,1]$، $\deg(S_1') = 0$ با پیاده‌سازی الگوریتم ۱ داریم.

$$i = \deg(S_1) = 10 \ (\mathrm{mod}\ 31) = 10 \Longrightarrow a' = a + i \ (\mathrm{mod}\ 31)$$

$$a' = 1 + 10 = 11 \ (\mathrm{mod}\ 31) \Longrightarrow \mathbf{e} = \mathbf{e}_{11}$$

بنابراین پوشش جدید حامل پیام برابر است با $\mathbf{y} = \mathbf{x} + \mathbf{e}$ $(\mathbf{m} = \mathbf{y}H^T)$.

مقایسه

روش پیشنهاد شده در این مقاله، برخلاف روش‌های موجود نهان‌نگاری براساس کدBCH، عمل نهان‌نگاری را بدون نیاز به پیدا کردن ریشه‌های چندجمله‌ای در میدان‌های گالوا انجام می‌دهد. در این مقاله با ذخیره کردن دو جدول در حافظه (مانند جدول ۴ و جدول ۶) و انجام چند عمل ساده ریاضی، همان‌طور که در الگوریتم ۱ بیان شده است، عمل نهان‌نگاری را با پیچیدگی محاسباتی خطی و فضایی چندجمله‌ای انجام می‌دهیم. به منظور مقایسهٔ الگوریتم پیشنهادی با روش‌های موجود نهان‌نگاری با استفاده از کدهای BCH، نتایج به دست آمده از اجرای الگوریتم ۱ را با نتایج عددی الگوریتم‌های بیان شده در مقاله های [۴]، [۵] و [۹] در جدول ۸، که برگرفته از مقالهٔ [۹] است، مقایسه کرده‌ایم.

جدول ۸: مقایسه پیچیدگی زمانی روش‌های نهان‌نگاری مبتنی بر کدهای (BCH)

روش ما	روش موجود در مقاله [9]	روش موجود در مقاله [5]	روش موجود در مقاله [4]	طرح BCH
سه مقایسه، دو حافظه با مرتبه چندجمله‌ای، تعدادی عملیات ساده (مرتبهٔ یک)	سه مقایسه، دو حافظه با مرتبهٔ چندجمله‌ای، تعدادی محاسبه در میدان گالوا (مرتبه یک)	1920	2066	(15,7,2)
		65011712	539333	(31,21,2)
		$\approx 10^{15}$	895776	(63,51,2)
		$\approx 10^{34}$	11009491	(127,113,2)

نتیجه‌گیری

در این مقاله ما با تعریف یک عدد به عنوان مشخصه بردار مشخصه ، که نسبت به شیفت برداری پایا است، توانستیم عمل نهان‌نگاری براساس کدهای BCH را، برخلاف روش‌های موجود، بدون نیاز به حل چندجمله‌ای در میدان‌های گالوا انجام دهیم. این رویکرد سبب کاهش قابل ملاحظهٔ پیچیدگی محاسباتی شده است.

References

1. Y. Wang and P. Moulin, “Perfectly secure steganography: Capacity,error exponents, and code constructions,” IEEE Trans. Inf. Theory, vol.54, no. 6, pp. 2706–2722, Jun. 2008.

2. A. Ker, “The square root law in stegosystems with imperfect information,” in Information Hiding, ser. Lecture Notes Comput. Sci. Berlin, Germany: Springer, 2010, vol. 6387, pp. 145–160.

3. R. Crandall, Some notes on steganography 1998 [Online]. Available:http://os.inf.tu-dresden.de/westfeld/crandall.pdf.

4. D. Schönfeld and A. Winkler, “Embedding with syndrome coding based on BCH codes,” in Proc. 8th ACM Workshop Multimedia Security, 2006, pp. 214–223.

5. D. Schönfeld and A. Winkler, “Reducing the complexity of syndromecoding for embedding,” in Information Hiding, ser. Lecture Notes Comput. Sci. Berlin, Germany: Springer, 2007, vol.4567, pp.145–158.

6. C. Fontaine and F. Galand, “How Reed–Solomon codes can improve steganographic schemes,” EURASIP J. Inf. Security, vol. 2009, pp.274845-1–274845-10, 2009.

7. A. Westfeld, “F5: A steganographic algorithm, “High capacity despite better steganalysis”, in Information Hiding, ser. Lecture Notes Comput. Sci. Berlin, Germany: Springer, 2001, vol. 2137, pp.289–302.

8. Y. Kim, Z. Duric, and D. Richards, “Modified matrix encoding technique for minimal distortion steganography,” in Information Hiding,ser. Lecture Notes Comput. Sci. Berlin, Germany: Springer, 2007, vol. 4437, pp. 314–327.

9. R. Zhang, V. Sachnev and H.J. Kim, "Fast BCH Syndrome Coding for Steganography," in Information Hiding. vol. 5806, S. Katzenbeisser and A.-R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 48-58.

10. D. Gorenstein, W. W. Peterson, and N. Zierler, “Two error correcting Bose–Chaudhuri–Hocquenghem codes are quasi-perfect,” Inf. Control,vol. 3, pp. 291-294,1960.

11. Van, Nguyen Thi Phuoc, and Pham Khac Hoan. "A novel method of decoding the BCH code based on norm syndrome to improve the error correction efficiency." In 2017 2nd Workshop on Recent Trends in Telecommunications Research (RTTR), pp. 1-4. IEEE, 2017.