ارائه روشی جدید برای شناسایی کور کدهای توربو ضربی سه‌بعدی با استفاده از ترکیب روش های بزرگ‌ترین مقسوم‌علیه مشترک و مرتبه ماتریس

تاریخ دریافت:
٤ تیر ماه ١٤٠٣

تاریخ پذیرش:
٢١ آذر ماه ١٤٠٣

هومن اکبرزاده خشکه رود*[۱]، حمیدرضا خدادادی[۲]، سید علی حسینی[۳]، رضا اصفهانی[۴]

۱. استادیار دانشکده جنگال، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران.
۲. دانشیار دانشکده مهندسی برق، جنگ الکترونیک و سایبری دانشگاه جامع امام حسین(ع)، تهران، ایران.
۳. دانشجوی دکتری دانشکده مهندسی برق، جنگ الکترونیک و سایبری دانشگاه جامع امام حسین(ع)، تهران، ایران.
۴. استادیار دانشکده مهندسی برق و کامپیوتر دانشگاه جامع امام حسین(ع)، تهران، ایران.

چکیده

در این مقاله کدهای توربو ضربی سه‌بعدی و تشریح چگونگی عملکرد آن‌ها و سپس روش های شناسایی کور این کدها بررسی گردیده است. تاکنون روش های مختلفی برای شناسایی کور کدهای بلوکی ارائه گردیده اما برای شناسایی کور کدهای توربو ضربی سه‌بعدی روشی ارائه نشده است. با توجه به اینکه کدهای توربو ضربی از ترکیب کدهای بلوکی ساخته‌شده‌اند، روشی نو بر مبنای روش‌های شناسایی کور کدهای بلوکی، جهت شناسایی کور کدهای توربو ضربی ارائه گردیده است. با توجه به اینکه کدهای توربو ضربی سه‌بعدی از ترکیب سه کد بلوکی و دو جایگردان ماتریسی تشکیل‌شده‌اند، به بررسی روش‌های جاری شناسایی کور کدهای بلوکی، جایگردان ماتریسی و استفاده از آن‌ها در تشخیص کدهای توربو ضربی پرداخته‌شده و به همین منظور از دو روش شناسایی کور GCD و مرتبه ماتریس برای شناسایی کور کدگذاری کانال استفاده‌شده است. اکثر روش‌های شناسایی کور پارامترهای توربو کدهای ضربی بر اساس روش GCD در کانال بدون تأخیر هستند. در این مقاله روش شناسایی کور توربو کدهای ضربی به‌وسیله شناسایی جایگردان ارائه‌شده و در ادامه با فرض تأخیر کانال به‌وسیله روش RREF، مقدار تأخیر تخمین زده و پس حذف آن، از روش GCD استفاده‌شده است. نتایج تحلیل و شبیه‌سازی بر اساس GCD و RREF ارائه‌شده و نتایج ارزیابی نشان می‌دهد الگوریتم GCD می‌تواند به‌صورت صحیح به شناسایی کد توربو ضربی با احتمال خطای $۱۰^{-۷}$ و کمتر از آن اقدام نماید و درنتیجه عملکرد این الگوریتم بر اساس BER نشان داده شده بسیار مطلوب است و به‌کارگیری این الگوریتم در سامانه‌های عملی و بلادرنگ مناسب است.

واژه‌های کلیدی: کد بلوکی، کد توربو ضربی سه‌بعدی، جایگردان، شناسایی کور.

Presenting a New Method in Blind Recognition of Three Dimension TPC (Turbo Product Codes) with GCD (Great Common Divisor) Method

Houman Akbarzade*[1], Hamidreza Khodadadi[2], Seyed Ali Hosseini[3], Reza Esfahani[4]

1. Assistant Professor, Faculty of Electronic Warfare, Shahid Sattari University of aeronautical Sciences and Technology, Tehran, Iran.
2. Associate Professor, Faculty of Electrical Engineering, Imam Hossein University, Tehran, Iran.
3. PhD Candidate, Electrical Engineering Faculty, Imam Hossein University, Tehran, Iran.
4. Assistant Professor, Faculty of Computer Engineering, Imam Hossein University, Tehran, Iran.

Abstract

This article investigates three-dimensional multiplicative turbo codes, their functionality, and blind identification methods. Although various methods have been proposed for the blind identification of block codes, no method has been proposed for the blind identification of 3D multiplicative turbo codes. To address this issue, a new method based on the blind recognition methods of block codes has been presented. Since 3D multiplicative turbo codes are composed of three block codes and two matrix displacements, this study investigates current methods of blind recognition of block codes, matrix displacements, and their use in diagnosing turbo-multiplicative codes. For this purpose, two GCD blind identification methods have been examined, and the matrix order has been used for blind identification of channel coding. Most blind identification methods of multiplicative turbo code parameters are based on the GCD method in the channel without delay. In this article, the method of blind recognition of multiplicative turbo codes is presented. Then, assuming channel delay by the RREF method, the amount of delay is estimated and, after its removal, the GCD method is used. The analysis and simulation results based on GCD and RREF are presented, and the evaluation results show that the GCD algorithm can correctly identify the multiplicative turbo code with an error probability of 10^{-7} or less. Therefore, the performance of this algorithm based on BER is very favorable, and its use in practical and real-time systems is appropriate

Key words: Block code 3 ؛D multiplicative turbo code؛ displacement؛ blind recognition.

ایمیل نویسنده مسئول: houman.akbarzadeh@gmail.com

۱-مقدمه

با شناسایی کور کدهای کانال، از روی بیت‌های شنود شده بر روی کانال، می‌تواند به محتوای اطلاعات موجود در آن‌ها دست‌یافت[۱]. بر روی بیت‌های اطلاعات قبل از ارسال در کانال، پردازش‌های متعددی اعمال می‌شود که یکی از آن‌ها اضافه کردن بیت‌های بررسی برای مقابله با نویز کانال است[۲]. ازاین‌رو محققین به ارائه راه‌کارهای مختلفی جهت شناسایی کدینگ‌های مورداستفاده در ارتباطات نموده‌اند که این شناسایی‌ها بر اساس شناسایی کور است[۳]. این بدین معناست که هیچ‌گونه اطلاعاتی از ساختار و نوع کدها در دسترس نیست[۴]. روش‌های شناسایی برای کدهای بلوکی را عموماً می‌توان به دودسته کلی تقسیم کرد که در دسته اول فقط مشخصات کلی (مانند طول کلمه کد و طول پیام) کدها را به‌دست آورد[۱] [۵]. و در دسته دوم علاوه بر مشخصات کلی کد، ساختار کد (چندجمله‌ای مولد) را نیز مشخص می‌کند[۲][۶]. البته به‌غیراز این دو روش کلی برخی از روش‌های شناسایی وجود دارند که فقط به بررسی استفاده از کدهای تصحیح خطا در سامانه‌های مخابراتی می‌پردازند[۸-۷]. با توجه به اهمیت و کاربردهای فراوان توربو کدهای ضربی در ارتباطات نظامی و شناسایی کور این نوع کدها در یک سامانه شنود، تاکنون اغلب روش‌ها به دلیل شناسایی هم‌زمان بر روی دو بعد، زمان و پیچیدگی بیشتری صرف شناسایی می‌شود و فرض بدون تأخیر بودن کانال شناسایی را انجام می‌دهند[۹]. اغلب شناسایی را بر روی یک توربو کد ضربی مربعی انجام داده و تک بعد آن را شناسایی می‌نمایند[۱۰]. در مورد شناسایی کور توربو کدهای سه‌بعدی روشی مطرح نشده است. با توجه به اینکه توربو کدهای ضربی سه‌بعدی از ترکیب سه کد بلوکی و دو جایگردان ساخته می‌شوند، از روش‌هایی که برای شناسایی کدهای بلوکی و جایگردان استفاده می‌شود، برای شناسایی پارامترهای توربو کدهای ضربی سه‌بعدی نیز می‌توان استفاده نمود.

ساختار این مقاله به نحوی است که در ابتدا به معرفی کدهای بلوکی و کد توربو ضربی دوبعدی و کد توربو ضربی سه‌بعدی(بدون محدودیت در ابعاد) پرداخته‌شده و سپس روش‌های شناسایی کور بیان می‌شود. روش‌های GCD[3] و RREF[4] توضیح و باهم مقایسه می‌شوند. همچنین دو روش برای شناسایی جایگردان ماتریسی بیان و مقایسه شده است. روش‌های ارائه‌شده قادر به تشخیص چندجمله‌ای مولد و پارامترهای کد (طول کد و طول پیام) و عمق جایگردان هستند.

سایر بخش‌های این مقاله از ساختار زیر تبعیت می‌کند. در این مقاله در بخش ۲ به معرفی روش‌های شناسایی کور کدهای بلوکی می‌پردازیم. در بخش ۳ به معرفی جایگردان و شناسایی کور آن پرداخته‌شده است. در بخش ۴ روش‌های GCD و RREF باهم مقایسه شده و عملکرد موردبررسی و تحلیل قرار خواهند گرفت. نهایتاً، در بخش ۵، روش پیشنهادی برای شناسایی توربو کدهای ضربی سه‌بعدی ارائه‌شده و در بخش ۶ به مقایسه روش پیشنهادی با سایر روش‌ها پرداخته خواهد شد.

۲- روش‌های شناسایی کور کدهای بلوکی

برخی از روش‌های شناسایی وجود دارند که فقط به بررسی استفاده از کدهای تصحیح خطا در سامانه‌های مخابراتی می‌پردازند[۱۱]. این روش‌ها به این سؤال که آیا از کدهای تصحیح خطا در رشته بیت دریافتی استفاده‌شده است یا نه پاسخ می‌دهند. این روش‌ها عموماً با مقایسه مشاهدات جمع‌آوری‌شده با یک سطح آستانه به تعیین استفاده از کدهای تصحیح خطا می‌پردازند. در این روش‌ها از تخمین حداکثر احتمال استفاده می‌شود؛ یعنی با تعیین حداکثر احتمال و مقایسه آن با سطح آستانه نتیجه‌گیری می‌کنند که از کدهای تشخیص خطا استفاده‌شده است یا خیر؛ تا سطح آستانه را از روی مشاهدات جمع‌آوری‌شده تعیین می‌کنند[۱۲].

از روش‌های مذکور، برخی برای شناسایی هر دو نوع کد بلوکی و کانولوشنال[5] و جایگردان استفاده‌شده و برخی دیگر فقط برای شناسایی کدهای بلوکی به‌کارگیری می‌شوند. با توجه به این‌که کدهای توربو ضربی از خانواده کدهای بلوکی هستند و نیز دارای خواص جبری کد-های مذکور می‌باشند، لذا می‌توان کارایی روش‌های شناسایی را که برای کدهای بلوکی خطی کاربرد دارند، بر روی کدهای توربو ضربی نیز بررسی نمود[۱۳]. روش‌هایی که برای شناسایی کدهای توربو ضربی به کار می‌روند باید بتوانند ساختار و مشخصات کلی را به‌دست آورند به همین دلیل روش‌هایی به کار گرفته‌شده است که بتوانند ساختار و یا مشخصات کدها را استخراج کنند که در ادامه به بررسی این روش‌ها به‌اجمال پرداخته خواهد شد.

۲-۱- همبستگی

همبستگی متقابل[6] میزان شباهت بین دو سیگنال را محاسبه می‌کند و خودهمبستگی، همبستگی متقابل یک سیگنال با خودش است. به‌طور غیررسمی خودهمبستگی، همسانی بین مشاهدات به‌عنوان تابعی از زمان جدایی بین آن‌ها است. این مفهوم، یک ابزار ریاضی برای یافتن الگوهای تکراری مانند حضور یک سیگنال تناوبی است که تحت نویز پوشانده شده است[۱۴].

برای دو فرایند تصادفی و ایستان ، y_n و x_n همبستگی متقابل به‌صورت رابطه۱ تعریف می‌شود:

$$R_{xy}(m) = E\{x_{n+m}\, y_n^*\} = E\{x_n\, y_{n-m}^*\} \qquad (۱)$$

که در این رابطه $R_{xy}(m)$ تابع همبستگی متقابل سیگنال‌های x_n و y_n^* است. این محاسبه کمک به شناسایی هم‌زمان‌سازها می‌کند.

---

[1] [۵] همانند روش رنک

[2] ، روش ریشهGCD همانند روش

[3] The greatest common divisor

[4] 4 Reduced Row-Echelon Form

[5] Convolutional

[6] Cross – Correlation

۲-۲- مرتبه ماتریس RREF

مرتبه یک ماتریس نشان‌دهنده تعداد سطرها یا ستون‌های مستقل خطی آن ماتریس است. روش‌های مختلفی برای محاسبه مرتبه یک ماتریس وجود دارد. همچنین مرتبه ماتریس در فضای میدان متناهی $GF(2)$ محاسبه می‌گردد[۵]. درصورتی‌که هیچ‌کدام از سطرها یا ستون‌های یک ماتریس ترکیبی خطی از سطرها یا ستون‌های دیگر آن ماتریس نباشد، گفته می‌شود آن ماتریس دارای «مرتبه کامل»[1] است. چنانچه نموداری از مقادیر این ضریب (رتبه ماتریس / طول بلوک) برحسب طول بلوک رسم شود در مقادیر n نمودار دارای مقادیر ثابت کمتر از یک بوده و در سایر نقاط برابر یک است. با ضرب n به‌دست‌آمده از این نمودار در مقدار نمودار ازای n می‌توان k (طول کلمه پیام) را به‌دست آورد. در استفاده از روش رتبه ماتریس، فرض می‌شود بیت‌ها در عبور از کانال دچار خطا نشده باشند، در غیر این صورت خروجی این روش چندان معتبر نخواهند بود. مرتبه ماتریس را نسبت به ماتریس با مرتبه کامل بیان نمود[۶].

$$Proportional\ Rank(m) = \frac{Observed\ Rank(m)}{Full\ Rank(m)} \qquad (۲)$$

در این رابطه رتبه ماتریس[2] (m) مرتبه محاسبه‌شده برای ماتریس m و مرتبه کامل m مقدار مرتبه ماتریس درصورتی‌که مرتبه آن کامل باشد را نشان می‌دهد. در این حالت مرتبه نسبی ماتریس[3] m همواره عددی بین صفرتا یک خواهد بود. تحت فرضیه واقع‌بینانه که $\mathrm{C}(n_e, d_e)$ شبیه به یک ماتریس باینری تصادفی رفتار کند هنگامی‌که $n_e \neq \alpha n, \alpha \in N^*$، خواهیم داشت[۵، ۱۳و۱۴]:

$$\frac{k}{n} = \frac{rk(C(n,d))}{n} \leq \frac{rk(C(n,d_e))}{n} \leq \frac{rk(C(n_e,d_e))}{n_e} = 1 \qquad (۳)$$

برای $\forall d_e, n_e \neq n$ احتمال نزدیک به یک است. تخمین $p(n_e, d_e)$ و H با استفاده از $\tilde{C}(n_e, d_e)$ می‌تواند به‌وسیله‌ی جستجوی کلمه کد وزنی همینگ کوچک در کد تولیدشده توسط ستون‌های ماتریس مرتبه به‌دست آید[۱۴–۱۸]. هنگامی‌که کانال کامل هست، یک فرآیند حذف گاوس ساده، مسئله را حل می‌کند اگر یک عدد صحیح غیر صفر را با α مشخص کنیم. [۱۹]. در این حالت داریم:

$$p(n_e, d_e) = \begin{cases} 1 & if\ n_e \neq \alpha n \\ k/n \leq 0 \leq 1 & if\ \ n_e = \alpha n\ \ and\ d_e \neq d, \\ k/n & if\ \ n_e = \alpha n\ \ and\ d_e \neq d. \end{cases} \qquad (۴)$$

به‌منظور نتیجه‌گیری از معرفی مقیاس مرتبه برای کدهای بلوکی خطی، متذکر می‌شویم که معادله (۵) نرخ کد است[۱۴].

$$\lim_{\alpha \to \infty} \quad \rho(\alpha\, n, d) = k/n \qquad (۵)$$

۲-۳- روش GCD

ریشه‌های یک چندجمله‌ای مقادیری هستند که چندجمله‌ای موردنظر به ازای آن‌ها برابر صفر خواهد شد. این ریشه‌ها متناسب با میدانی که در آن به‌دست می‌آیند، ممکن است تغییر کنند[۲۰]. در هنگام استفاده از ریشه باید فرضیات زیر را در نظر بگیریم:

۱) ساختار تعیین شود.

۲) طول کد باید قبلاً مشخص‌شده باشد.

۳) وجود هم‌زمانی لازم است.

. شناسایی کور یک کد باینری $\mathrm{BCH}(n, k)$ در تعیین این سه پارامتر خلاصه می‌شود: طول بلوکn، طول کلمه پیام k و چندجمله‌ای مولد $g(x)$؛ اما چون درجه $\mathrm{g(x)}$ برابر $n-k$ است، بنابراین با به‌دست آمدن n و $g(x)$، k نیز خودبه‌خود به‌دست می‌آید که در ادامه ابتدا به شناسایی طول بلوک و چندجمله‌ای مولد$g(x)$ پرداخته خواهد شد. برای شناسایی فرض شده که طول فریم f_l مشخص و در حالت همزمانی[4] است. ازآنجاکه طول فریم f_l مشخص است و همچنین حداقل دو کلمه کد در یک فریم موجود است[۱۵]، نتیجه‌های زیر به دست خواهد آمد

۱) f_l بر n بخش‌پذیر است$(n|f_l)$.

۲) $n \in \left[3, \left|\frac{f_l}{2}\right|\right]$ است.

از خاصیت ۱ نتیجه می‌شود که طول بلوک یکی از عامل‌های f_l است، البته یکتا نیست. فرض شود که i عاملی از f_l باشد، بنابراین دو حالت پیش می‌آید:

در حالتی‌که $i = n$:، اگر i طول بلوک در نظر گرفته شود، $N_i = \frac{f_l}{i}$ کلمه کد به‌دست می‌آید. فرض شود $\mathrm{c_p(x)}$ چندجمله‌ای کد متناظر با pامین کلمه کد باشد. متناظر با $c_p(x)$، تعداد j چندجمله‌ای کد $c_{p1}(x), c_{p2}(x), \dots, c_{pj}(x)$ به‌دست می‌آید که $c_{pj}(x)$ چرخش یافته گردشی $c_p(x)$ به‌اندازه j برابر $(1 \leq \mathrm{j} \leq \mathrm{i\text{-}1})$ است.

با توجه به خاصیت گردشی این کد، اگر در c_p خطایی نباشد، کلمه کدهای متناظر با $c_{p1}(x), c_{p2}(x), \dots, c_{pj}(x)$ و همچنین $c_p(x)$ نیز متعلق به مجموعه کلمه کد با چندجمله‌ای مولد یکسان هستند. با توجه به خاصیت ۲، یک عامل مشترک بین $c_{p1}(x), c_{p2}(x), \dots, c_{pj}(x)$ وجود خواهد داشت[۱۲]. اگر $c_{p0}(x) = c_p(x)$:

1 Full Rank

2 Observed Rank

3 Proportional Rank(m)

4 Synchron

$$gcd\left[c_{p0}(x), c_p(x), c_{p1}(x), c_{p2}(x), \dots, c_{pj}(x)\right] \neq 1 \quad (۶)$$

کلمه کدی که در رابطه ۶ صدق کند یک کلمه کد معتبر گفته می‌شود. فرض شود که در کل فریم تعداد N_{ic} کلمه کد معتبر وجود دارد. واضح است که اگر کانال خطا نداشته باشد، $N_{ic} = N_i$ است. نسبت تعداد کلمه کدهای معتبر به‌کل کلمه کدها را f_{ic} می‌نامند[۱۷]. (در حالت بدون خطا $f_{ic} = 1$ است).

$$f_{ic} = \frac{N_{ic}}{N_i} \quad (۷)$$

در حالتی‌که $i \neq n$ باشد، اگر i به‌عنوان طول بلوک در نظر گرفته شود، بلوک‌بندی کلمات کد صحیح نبوده و اگر کل کلمات کد به‌دست‌آمده برابر N_i باشد، کلمات کد معتبر که در رابطه ۷ صدق می‌کند کمتر از این تعداد خواهد بود ($N_{ic} < N_i$) که مطابق [۱۶] خواهیم داشت:

$$f_{ic} = \frac{N_{ic}}{N_i} < 1 \quad (۸)$$

حالت کلی این است که اگر فرض شود خطای کانال وجود ندارد، اگر $i = n$ باشد $f_{ic} = 1$ و اگر $i \neq n$ باشد، $f_{ic} < 1$ است[۱۶]. در حالت وجود خطای کانال، f_{ic} کمتر از ۱ می‌شود اما می‌توان پیش‌بینی نمود که f_{ic} حداکثر مقدار خود را در حالت $\mathrm{i = n}$ می‌گیرد[۱۸].

$$n = \underset{\substack{i \\ i\in\left[3,\left\lfloor\frac{f_l}{2}\right\rfloor\right] \\ rem(i,2)=1 \\ rem(f_l,i)=0}}{\operatorname{argmax}} (f_{ic}) \quad (۹)$$

که $\mathrm{rem(f_l, i)}$ باقیمانده تقسیم f_l بر i است. هر چه مقدار j (تعداد نوبت‌های گردشی) و N_i بیشتر باشد، دقت تخمین طول بلوک بیشتر می‌شود.

۳-معرفی روش شناسایی جایگردان

نویزهایی که اغلب با آن‌ها برخورد می‌کنیم دودسته می‌باشند:

۱) نویز با توزیع گوسی

۲) نویز رشته‌ای یا قطاری[1]

کدهای کانال طوری طراحی‌شده‌اند که به قدرت تشخیص و اصلاح نویز با توزیع گوسی را می‌دهند. درواقع سیستم تشخیص و تصحیح خطا، زمانی درست عمل می‌کند که خطای رخداده از نوع تصادفی و با توزیع گوسی یا نقطه‌ای باشد، در غیر این صورت چنانچه خطای رخداده به‌صورت قطاری (خطای پیوسته) باشد این سیستم قادر به شناسایی و اصلاح آن نخواهد بود[۱۴]. بنابراین برای مقابله با این‌گونه خطاها، از روشی استفاده می‌کنیم که در صورت بروز خطای قطاری بتوان آن را تقسیم کرده و درون چندین کلمه کد قرارداد. با این روش می‌توانیم خطای قطاری ایجادشده را تشخیص و سپس اصلاح نماییم. همان‌طور که گفته شد کدهای بلوکی و کانولوشنال نمی‌توانند خطای قطاری را اصلاح کنند حتی اگر تعداد بیت‌ها یا سمبل‌های دارای خطا در حالتی که خطا قطاری باشد با تعداد بیت‌ها و سمبل‌های دارای خطا در حالتی که خطا به‌صورت پراکنده باشد، برابر باشد. به همین خاطر از جایگردان استفاده می‌شود. پس کاربرد جایگردان افزایش قدرت اصلاح خطای رشته‌ای است و نحو عملکرد به این صورت است که خطای قطاری را در طول سیگنال توزیع می‌کند لذا با کدینگ کانال می‌توان آن را اصلاح کرد و هیچ افزونگی اضافی به‌کاربرده نمی‌شود. باید به این نکته توجه کرد که جایگردان بدون کدینگ معنی ندارد و اگر جایگردان باشد حتماً کدینگ هم هست. پس در فرستنده ابتدا کدگذاری و سپس جایگردان روی دیتا اعمال می‌شود.

۳-۱-تشخیص جایگردان بلوکی

برای تشخیص جایگردان بلوکی، ابتدا با استفاده از روش مرتبه بهبودیافته ماتریس مولد دوگان مربوطه‌ی کل جایگردان را پیدا می‌کنیم. سپس با توجه به طول جایگردان عکس جای‌گردان‌های مذکور را تک‌تک اعمال کرده و ماتریس مولد دوگان را ساده می‌کنیم. با توجه به اینکه در کدها بیت‌های وابسته خطی به هم در کنار هم هستند تصمیم‌گیری می‌کنیم. باید توجه داشت که حتی اگر فرض کنیم که کد بلوکی است، ازآنجایی‌که ممکن است ورودی کد بلوکی خود کدی دیگر باشد، نمی‌توان با استفاده از این فرض بلوک‌ها را به‌صورت جدا از هم تشخیص داد و متعاقباً نمی‌توان میزان محاسبات مربوطه به هر آزمون جای‌گردان‌های بهینه را کمتر کرد. یعنی باید در تمامی موارد از خود ماتریس مولد دوگان به‌دست‌آمده برای ساده‌سازی استفاده کنیم و نمی‌توانیم با تشخیص بلوک‌ها و مکان آن‌ها نوع جایگردان را حدس بزنیم.

۳-۲-جایگردان ماتریسی

در این جایگردان جابجایی بیت‌ها یا دسته بیت‌ها (در صورت m تایی (M-arry)) در ماتریسی به‌صورت سطری نوشته‌شده و در انتها به‌صورت ستونی بازیابی می‌شود. چنین روشی باعث جابجا شدن بیت‌ها در ترتیب ارسال می‌گردد. واضح است که تنها پارامترهای جایگردان تعداد ستون‌ها و سطرهای ماتریس است.

۳-۳- جایگردان قطری و مارپیچی

در این جایگردان ابتدا به فرم ماتریسی داده‌ها در ماتریسی ذخیره می‌شوند سپس به‌صورت قطری یا مارپیچی بازیابی می‌شوند که اگر

[1] Bust error

تعداد حرکت‌ها در ستون در هر گام بیشتر شود جایگردان مارپیچی با گام مربوطه به‌دست می‌آید.

٤-کدهای توربو ضربی

به خاطر محدودیت‌های موجود در ارتباطات نظیر حد شانون[1]، لازم است که کدهای طولانی داشته تا کدهای بلوکی با حداقل فاصله همینگ (MHD)[2] و قابلیت تصحیح خطا بالا را به‌دست آورد، اما بدون یک ساختار خاص، کدگشایی این کدها تقریباً غیرممکن است[۱۲]. اختراع کدهای ضربی (محصول)، توسط الیاس[3]، صورت گرفت که هدف این کدها پیدا کردن یک‌راه ساده برای به‌دست آوردن کدهای تصحیح خطای با قابلیت بالا که بتوان به‌راحتی با کدهای ساده و ابتدایی کدگشایی شوند، بود. با ساختار هم‌گشت[4]، ازلحاظ تئوری ساخت کدهای با MHD بالا ممکن است. بااین‌حال، پیچیدگی مانع کدگشایی حتی برای کدهای با ساختار جبری، مانند کدهای ریدسالمون[5] یا کدهای BCH[6] می‌شود. ساختار کدهای ضربی اجازه می‌دهد تا این مشکل را با استفاده از کدهای ساده باقابلیت اصلاح کم، ولی کدگشایی با هزینه کمتر حل کرد[۶]. این کدهای در حالت‌های دوبعدی و سه‌بعدی ارائه‌شده‌اند.

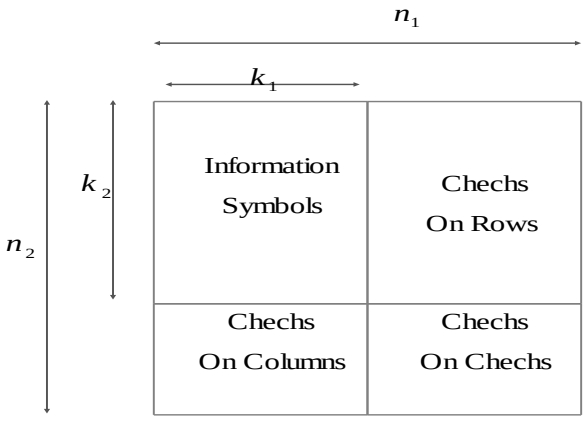
٤-١-ساختار کدگذاری کدهای توربو ضربی دوبعدی و سه‌بعدی

فرض کنید C_1 (C_2) یک کد خطی به طول n_1 (n_2) و با ابعاد k_1 (k_2) باشد کد ضربی $C = C_1 \otimes C_2$ مجموعه‌ای از ماتریس M با اندازه $n_1 \times n_2$ به‌طوری‌که:

۱) هر ردیف یک کلمه کد از C_1 است.

۲) هر ستون یک کلمه کد از C_2 است.

مطابق شکل ۱ این کد یک کد خطی طول $n_1 \times n_2$ و با ابعاد $k_1 \times k_2$ است.



شکل ۱- ساختار کدگذاری توربو ضربی دوبعدی[١٦].

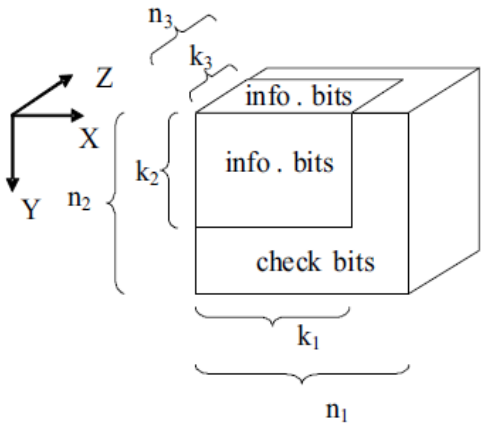
حال با فرض اینکه C_1 (C_2) (C_3) یک کد خطی به طول n_1 (n_2) (n_3) و با ابعاد k_1 (k_2) (k_3) باشد کد ضربی $C = C_1 \otimes C_2 \otimes C_3$ مجموعه‌ای از ماتریس M با اندازه $n_1 \times n_2 \times n_3$ به‌طوری‌که:

۱) هر ردیف یک کلمه کد از C_1 است.

۲) هر ستون یک کلمه کد از C_2 است.

۳) هر قطر یک کلمه کد از C_3 است.

همانطور که در شکل ۲ دیده می‌شود این کد یک کد خطی طول $n_1 \times n_2 \times n_3$ و با ابعاد $k_1 \times k_2 \times k_3$ است.

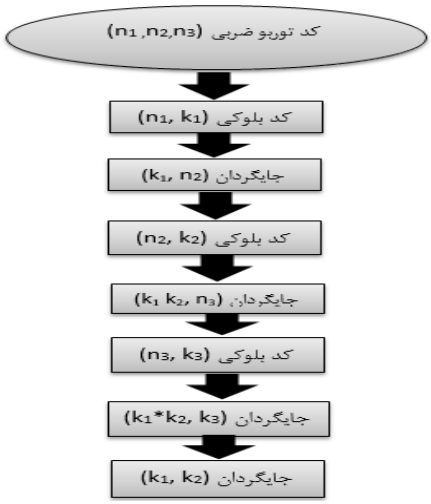


شکل ۲- ساختار کدگذاری توربو ضربی سه‌بعدی[١٨].

٥-روش پیشنهادی برای توربو کد ضربی ۳ بعدی

درروش شناسایی کور کدهای توربو ضربی سه‌بعدی سه‌بعدی همانطور که در شکل ۳ دیده می‌شود، ابتدا قاب کد(فریمینگ)را از روش خودهمبستگی یا رنک تشخیص می‌دهیم و بعد از حذف هدر طول کد ارسالی به‌دست می‌آید. طول کد ارسالی برابر $(n_1 \times n_2 \times n_3)$ یا ضرایب آن است. با استفاده از روش GCD و RREF کد بلوکی (n_1, k_1) شناسایی می‌شود. عمق جایگردان اول k_1 است. با تقسیم طول کد ارسالی بر n_1 و به‌دست آوردن فاکتورهای اول آن می‌توان ستون جایگردان اول را شناسایی کرد، که برابر n_2 یا ضریبی از آن است. حال کد بلوکی دوم (n_2, k_2) شناسایی می‌شود. عمق جایگردان دوم برابر $k_1 \times k_2$ حال با تقسیم طول کد ارسالی بر $n_1 \times n_2$ می‌توان ستون جایگردان دوم n_3 را به‌دست آورد و کد بلوکی (n_3, k_3) شناسایی می‌شود. با دو جایگردان به ترتیب $(k_1 \times k_2, k_3)$ و (k_1, k_2) داده به حالت قبل از جایگردان $(k_1 \times n_2)$ برمی‌گردد. در این روش شناسایی مربعی بودن کدها مدنظر نیست به‌عنوان نمونه می‌توان کد بلوکی سوم را کد پریتی تعریف کنیم که بعد از شناسایی دو کد بلوکی از روش RREF می‌توان کد پریتی را شناسایی کرد.

[1] Claude Elwood Shannon
[2] Minimum Hamming Distance
[3] Elias
[4] Convolution
[5] Reed–Solomon
[6] Bose–Chaudhuri–Hocquenghem codes

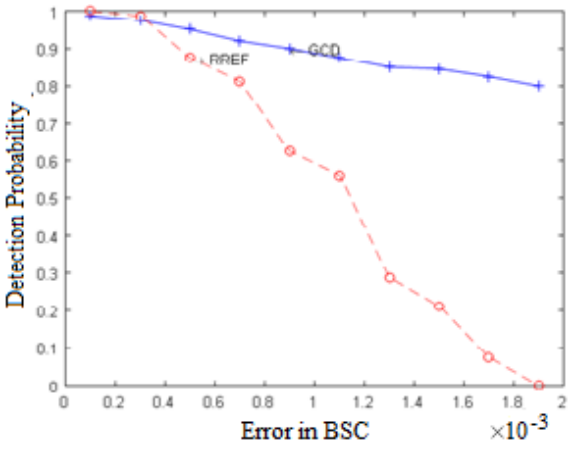


شکل ۳- روش کدگشای کدهای توربو ضربی سه‌بعدی[۱۸].

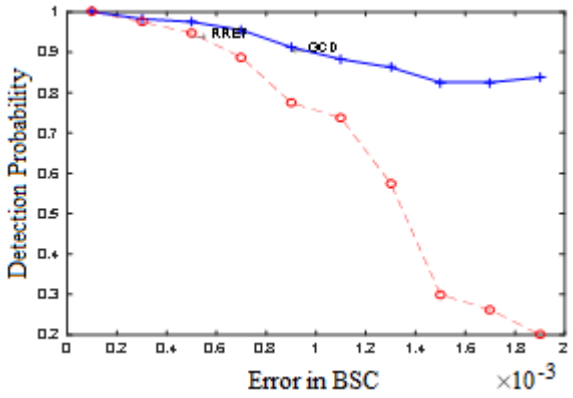
برای مثال با فرض اینکه طول کد برابر ۴۰۹۶(ارسالی ماهواره باند X) که برابر $(n_1 \times n_2 \times n_3)$ابتدا با روش RREF مقدار تأخیر را در صورت وجود به‌دست می‌آید، به‌وسیله روش GCD کد BCH(31,26) با یک بیت افزودگی را شناسایی می‌کنیم (یعنی یک بیت پریتی زوج به انتهای تمام کلمات کد اضافه می‌نماید.) حال با توجه به $26k_1 =$ عمق جایگردان به‌دست آورده‌ایم با تقسیم ۴۰۹۶ بر طول n_1 ضریبی از تعداد ستون‌ها را به‌دست می‌آید.حال فاکتورهای اول ضریب به‌دست‌آمده از تقسیم مرحله ۳ به‌دست می‌آید، با این اعداد به دنبال شناسایی کد چرخشی دوم به‌صورت جستجو و آزمون می‌گردیم به‌وسیله روش GCD کد BCH (31,26) با یک بیت افزودگی را شناسایی می‌کنیم. حال با توجه به $676k_1 \times k_2$= عمق جایگردان دوم را به‌دست آورده‌ایم با تقسیم ۴۰۹۶ بر طول $n_1 \times n_2$ تعداد ستون‌های جایگردان دوم که برابر n_3 را به‌دست می‌آید، حالا کد سوم را شناسایی می‌کنیم Parity(4,3) حال با دو جایگردان عمق $k_1 \times k_2$ و تعداد ستون k_3 و جایگردان به عمق k_1 و تعداد ستون k_2 داده را به حالات صحیح مرتب می‌شود.

۶-مقایسه روش‌های شناسایی GCD و RREF برای توربو کد ضربی

در این شبیه‌سازی نمودار شناسایی دو الگوریتم GCD وRREF مختلف برای کد BCH(63,57) در دامنه جستجوی $N_{min} =$ 35 , $N_{max} = 80$ که برای هر مقدار، نویز کانال باینری متقارن، هزار مرتبه تکرار شده و مقدار موفقیت در شناسایی، اندازه‌گیری و ترسیم‌شده است. در این شبیه‌سازی داده بدون تأخیر است. شبیه‌سازی تمامی شرایط همانند فوق بوده با این تفاوت که از یک کد BCH(63,57) با ۷ بیت کوتاه شدگی استفاده‌شده تا شرایط کدهای کوتاه شده تک‌بعدی و یا کدهای توربو ضربی غیر مربعی نیز موردبررسی قرار گیرد.



شکل ٤- مقایسه روش GCD و روش رنک سریع RREF برای کد BCH(63-57)



شکل ٥- مقایسه روش GCD و روش رنک سریع RREF برای کد BCH(63-57-7)

همان‌طور که در شکل (۵) مشاهده می‌شود، شبیه‌سازی‌ها برای یک کد BCH با ۷ بیت کوتاه شدگی انجام‌گرفته است. روش GCD نسبت به روش RREF عملکرد بهتری دارد. روش RREF در شناسایی کدهای دارای کوتاه شدگی عملکرد بهتری نسبت به کدهای بدون کوتاه شدگی دارد. در میزان خطای $p_e = 0.001$ روش RREF ٪۷۵ و روش GCD ٪۹۰ کدها را شناسایی کرده‌اند. برای مقایسه سرعت تشخیص دو روش زمان متوسط شناسایی الگوریتم‌ها به ازای 1000 مرتبه تکرار برای مقدار خطا 0.0019 در جدول (۱) آورده شده است. همان‌طور که ملاحظه می‌شود مقدار زمان محاسبه روشRREF کمتر است.

جدول۱- مقایسه زمانی دو روش شناسایی برای کد BCH(63-57-7)

الگوریتم	متوسط زمان
GCD	۰.۸۲۶۱ sec
RREF	۰.۶۴۴۲ sec

در جدول(۲) دو روش GCD و RREF با مقدار تأخیر مختلف برای کد BCH(63-57) و مقدار ۷ بیت کوتاه شدگی باهم مقایسه شده است.همان‌طور که ملاحظه می‌شود، روش GCD به میزان تأخیر بسیار

حساس بوده و نمی‌تواند هیچ‌گونه شناسایی در داده بدون همزمان‌سازی انجام دهد.

جدول ۲- مقایسه روش GCD و RREF در تشخیص تأخیر در کد BCH(63,57,7)

روش RREF	روشGCD	BCH(63,57,7)
✓	-	BCH(63,57,7),D=1
✓	-	BCH(63,57,7) ,D=3
✓	-	BCH(63,57,7) ,D=5
✓	-	BCH(63,57,7) ,D=7
✓	-	BCH(63,57,7) ,D=6
✓	-	BCH(63,57,7) ,D=14

در جدول(۳) دو روش شناسایی کور کد کانال ارائه‌شده که هرکدام مزایا و معایبی برخوردار می‌باشند. مهم‌ترین پارامترها در شناسایی کور دقت بالا و حجم محاسبات پایین است. همان‌طور که در جدول مشاهده می‌شود این دو روش در ۶ شش پارامتر باهم مقایسه شده‌اند. بسته به کاربرد می‌توان بهترین روش را شناسایی نمود.

جدول ٤- مقایسه روش GCD و RREF ازنظر ویژگی‌ها

روش‌های شناسایی کور	GCD	RREF
نیاز به طول کد	دارد	ندارد
نیاز به هم‌زمانی	دارد	ندارد
حجم داده	کم	n^2
حساسیت به نویز	ندارد	بالا
حجم محاسبات	بسیار زیاد	زیاد
تعیین ساختار	بله	نه

۷-نتیجه‌گیری

نتایج شبیه‌سازی نشان می‌دهد، از روش رتبه ماتریس فقط طول کد و طول پیام به‌دست می‌آید اما در روش GCD علاوه بر استخراج مشخصات کلی کد، می‌توان چندجمله‌ای مولد کد توربو ضربی را نیز به‌دست آورد. در این مقاله دو روش شناسایی کور کدهای توربو ضربی ارائه‌شده است، در روش الگوریتم GCD چندجمله‌ای‌های مولد کد توربو ضربی شناسایی‌شده و بر اساس آن پارامترهای مربوط به کد توربو ضربی استخراج‌شده‌اند. درروش رتبه ماتریس (RREF) ارائه‌شده است که در آن به شناسایی کور کدهای توربو ضربی سه‌بعدی پرداخته و سپس پارامترهای آن (طول کد، نرخ کد و طول پیام) استخراج می‌شوند.

نتایج ارزیابی نشان می‌دهد الگوریتم GCD می‌تواند به‌صورت صحیح به شناسایی کد توربو ضربی با احتمال خطای 10^{-7} و کمتر از آن اقدام نماید و درنتیجه عملکرد این الگوریتم بر اساس BER نشان داده‌شده بسیار مطلوب است و به‌کارگیری این الگوریتم در سامانه‌های عملی و بلادرنگ مناسب است.

از شبیه‌سازی‌های صورت گرفته می‌توان نتیجه گرفت:

۱) پاسخ GCD هرزمان که از کانالی با تأخیر استفاده شود، اشتباه خواهد بود.

۲) با روش RREF می‌توان پس از به‌دست آوردن تخمینی از طول کد، تخمینی از مقدار تأخیر نیز به‌دست آورد.

۳) برای آشکارسازی کور ابتدا روش RREF را اعمال نموده و پس از به‌دست آوردن تأخیر و حذف آن، از روش GCD استفاده شود.

۴) در الگوریتم RREF یک مقدار آستانه برای تفکیک ستون‌های مستقل از وابسته وجود دارد که با کوچک در نظر گرفتن آن توانایی الگوریتم در تشخیص کدهایی با نرخ کم افزایش خواهد یافت.

۵) با کاهش مقدار آستانه، قدرت الگوریتم در برابر احتمال خطاهای بالا کاهش خواهد یافت.

۶) با توجه به مشاهدات به ازای نرخ کدهای پایین، مقدار آستانه باید پایین باشد اما به ازای نرخ کدهای بالا مقدار آستانه باید زیاد در نظر گرفته شود.

۸-مراجع

[1] E. Yoon, S. Kwon and S. Y. Kim, "An Efficient Application of Turbo Coding for OFDM In-Phase/Quadrature Index Modulation," in IEEE Access, vol. 11, pp. 37031-37040, 2023, doi: 10.1109/ACCESS.2023.3266288.

[2] C. Berrou, "The Invention of Turbo Codes: The Ten-Year-Old Turbo Codes are Entering into Service," in IEEE Communications Magazine, vol. 61, no. 2, pp. 6-13, February 2023, doi: 10.1109/MCOM.2023.10048673.

[3] Y. Hama and H. Ochiai, "Binary-Input Ternary-Output Turbo Codes for Ternary PSK Transmission," in IEEE Communications Letters, vol. 26, no. 9, pp. 1974-1978, Sept. 2022, doi: 10.1109/LCOMM.2022.3185652.

[4] M. Lafci and Ö. Ertuğ, "Performance Optimization of 6LoWPAN Systems for RF AMR System Using Turbo and LDPC Codes," 2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP), Sofia, Bulgaria, 2022, pp. 1-4, doi: 10.1109/IWSSIP55020.2022.9854500.

[5] M. A. Khalighi and M. Uysal, "Survey on Free Space Optical Communication: A Communication Theory Perspective," IEEE Commun. Surveys & Tutorials, vol. 16, no. 4, pp. 2231–2258, fourth quarter 2014.

[6] S. Hranilovic, "Wireless Optical Communication Systems". Springer, 2006.

[7] L. Can, Z. Tian-qi, and L. Yu, "Blind Recognition of RS Codes Based on Galois Field Columns Gaussian Elimination," Telecommunication Engineering, vol. 54, 2014.

[8] M. Cluzeau, "Block Code Reconstruction Using Iterative Decoding Techniques," In IEEE Conference Seattle, USA, ISIT'06, pp. 2269-2273, 2006.

[9] C. -Y. Wei and C. -C. Chen, "Cube-Based Multitarget 3D Localization Using Bayesian Learning-Based Turbo Decoding in Wireless Sensor Networks," in IEEE Sensors Journal, vol. 22, no. 17, pp. 17291-17306, 1 Sept.1, 2022, doi: 10.1109/JSEN.2022.3193021.

[10] Z. Liu, R. Liu, H. Zhang, N. Wang, L. Sun and J. Wang, "Parallel implementation of the CCSDS turbo decoder on

GPU," in China Communications, doi: 10.23919/JCC.2023.00.101.
[11] W. Lei, H. Yihua, H. Shiqi, and Q. Lin, "The Method of Estimating The Length of Linear Cyclic Code Based on The Distribution of Code Weight," In Information Science and Engineering (ICISE), 2nd International Conference on Hefei, China, pp. 2459-2462, 2010.
[12] C. Berrou, “Codes and Turbo” (J. Ormrod, Trans). Springer-Verlag France, Paris: Telecom Bretagne. 2010.
[13] R.M. Larrson, “Fast Scheme for Blind Identification of Channel Codes” IEEE. 2011.
[14] R. Moosavi and E. G. Larsson, "A Fast Scheme for Blind Identification of Channel Codes," in 54th Annual IEEE Global Telecommunications Conference,(GLOBECOM); Houston, TX; United States, pp. 1-5, 2011.
[15] J. Barbier and J. Letessier, "Forward Error Correcting Codes Characterization Based on Rank Properties," In Wireless Communications & Signal Processing. International Conference on Bruz Cedex, France, pp. 1-5, 2009.
[16] T. Li, C. L. Miao, and J. Lv, "An Improved Algorithm of RS Codes Blind Recognition," In Applied Mechanics and Materials ,pp. 2308-2312 ,2014.
[17] J. Wang, Y. Yue, and J. Yao, "A Method of Blind Recognition of Cyclic Code Generator Polynomial," In Wireless Communications Networking and Mobile Computing (WiCOM), 6th International Conference on Sichuan Mianyang, China ,pp. 1-4, 2010.
[18] W. Lei, H. Yihua, H. Shiqi, and Q. Lin, "The Method of Estimating The Length of Linear Cyclic Code Based on The Distribution of Code Weight," In Information Science and Engineering (ICISE), 2nd International Conference on Hefei, China, pp. 2459-2462, 2010.
[19] A.U. Mustafa and G. Murtaza, “Synthesis by Analysis of BCH Codes” arXiv preprint arXiv: 1210.7906, 2012.
[20] N. Wen, X. Yang, “Recognition methods of BCH codes” Electron. Warf. 6, 30–34, 2010.
[21] Hashemi SM, Barati S, Talati S, Noori H. “A genetic algorithm approach to optimal placement of switching and protective equipment on a distribution network.” J Eng Appl Sci 2016; 11: 1395-1400.
[22] Sicot, Guillaume, Sebastien Houcke, and Johann Barbier. "Blind detection of interleaver parameters." 2009.