عنوان ارائه

مصطفی الماسی

استاد راهنما: دکتر

دانشگاه رازی کرمانشاه - گروه ریاضی - خرداد ۹۳

روش رمزنگاری تصویر مبتنی بر تابع آشوب چبیشف

تابع چبیشف

$$T_k(x) = cos(k\arccos(x)); \forall k = ۱, ۲, ۳, ...; x \in [-۱, ۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$...$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

$$T_k(x) = cos(k \arccos(x)); \forall k = ۱,۲,۳,...; x \in [-۱,۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$...$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

$$T_k(x) = cos(k \arccos(x)); \forall k = ۱, ۲, ۳, \ldots; x \in [-۱, ۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$\ldots$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

$$T_k(x) = cos(k \arccos(x)); \forall k = ۱, ۲, ۳, \ldots; x \in [-۱, ۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$\ldots$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

$$T_k(x) = cos(k \arccos(x)); \forall k = ۱,۲,۳,...; x \in [-۱,۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$...$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

$$T_k(x) = cos(k \arccos(x)); \forall k = ۱,۲,۳,...; x \in [-۱,۱]$$

$$T_۰(x) = ۱$$

$$T_۱(x) = x$$

$$...$$

$$T_{k+۱}(x) = ۲xT_k(x) - T_{k-۱}(x)$$

تابع چبیشف

چند جمله ای چبیشف در حالت دو بعدی:

$$\begin{cases} x_i = ۱ - \alpha y_{i-۱}^{۲} \\ y_i = cos(\beta \arccos(x_{i-۱})) \end{cases}$$

(اگر $x_۰$ نقطه ای در لحظه t در روی یک مسیر و $x_۰ + d_۰$ نقطه ای نزدیک به آن در مسیر دیگری باشد.اگر میزان جدایی این دو نقطه بعد از n تکرار توسط d_n نمایش داده و رابطه $|d_n| = e^{n\lambda}|d_۰|$ مابین دو نقطه برقرار کنیم آنگاه λ را نمای لیاپانوف گویند.)

تابع چبیشف

چند جمله ای چبیشف در حالت دو بعدی:

$$\begin{cases} x_i = ۱ - \alpha y_{i-۱}^{۲} \\ y_i = cos(\beta \arccos(x_{i-۱})) \end{cases}$$

(اگر $x_۰$ نقطه ای در لحظه t در روی یک مسیر و $x_۰ + d_۰$ نقطه ای نزدیک به آن در مسیر دیگری باشد.اگر میزان جدایی این دو نقطه بعد از n تکرار توسط d_n نمایش داده و رابطه $|d_n| = e^{n\lambda}|d_۰|$ مابین دو نقطه برقرار کنیم آنگاه λ را نمای لیاپانوف گویند.)

تابع چبیشف

چند جمله ای چبیشف در حالت دو بعدی:

$$\begin{cases} x_i = ۱ - \alpha y_{i-۱}^{۲} \\ y_i = cos(\beta \arccos(x_{i-۱})) \end{cases}$$

(اگر $x.$ نقطه ای در لحظه t در روی یک مسیر و $x. + d.$ نقطه ای نزدیک به آن در مسیر دیگری باشد.اگر میزان جدایی این دو نقطه بعد از n تکرار توسط d_n نمایش داده و رابطه $|d_n| = e^{n\lambda}|d.|$ مابین دو نقطه برقرار کنیم آنگاه λ را نمای لیاپانوف گویند.)

فرآیند انتشار

$$\begin{cases} x'_0, x''_0 \\ x_i = T_4(x_{i-1}) = 8x_{i-1}^4 - 8x_{i-1}^2 + 1 \end{cases}$$

$$\Downarrow$$

$$\{x'_i\}_i$$

$$\{x''_i\}_i$$

$$\Downarrow$$

$$\{\bar{x}_i\}_{i=1}^{m+n} = \{x'_i\}_{i=p+1}^{p+m+n}$$

$$\{\hat{x}_i\}_{i=1}^{m+n} = \{x''_i\}_{i=q+1}^{q+m+n}$$

فرآیند انتشار

$$\begin{cases} x'_{۰}, x''_{۰} \\ x_i = T_۴(x_{i-۱}) = ۸x_{i-۱}^۴ - ۸x_{i-۱}^۲ + ۱ \end{cases}$$

$$\Downarrow$$

$$\{x'_i\}_i$$

$$\{x''_i\}_i$$

$$\Downarrow$$

$$\{\bar{x}_i\}_{i=۱}^{m+n} = \{x'_i\}_{i=p+۱}^{p+m+n}$$

$$\{\hat{x}_i\}_{i=۱}^{m+n} = \{x''_i\}_{i=q+۱}^{q+m+n}$$

فرآیند انتشار

$$\begin{cases} x'_0 , x''_0 \\ x_i = T_4(x_{i-1}) = 8x^4_{i-1} - 8x^2_{i-1} + 1 \end{cases}$$

$$\Downarrow$$

$$\{x'_i\}_i$$

$$\{x''_i\}_i$$

$$\Downarrow$$

$$\{\bar{x}_i\}_{i=1}^{m+n} = \{x'_i\}_{i=p+1}^{p+m+n}$$

$$\{\hat{x}_i\}_{i=1}^{m+n} = \{x''_i\}_{i=q+1}^{q+m+n}$$

فرآیند انتشار

$$\begin{cases} x'_۰, x''_۰ \\ x_i = T_۴(x_{i-۱}) = ۸x^۴_{i-۱} - ۸x^۲_{i-۱} + ۱ \end{cases}$$

$$\Downarrow$$

$$\{x'_i\}_i$$

$$\{x''_i\}_i$$

$$\Downarrow$$

$$\{\bar{x}_i\}_{i=۱}^{m+n} = \{x'_i\}_{i=p+۱}^{p+m+n}$$

$$\{\hat{x}_i\}_{i=۱}^{m+n} = \{x''_i\}_{i=q+۱}^{q+m+n}$$

فرآیند انتشار

$$\{\bar{x}_i\}_{i=1}^{m+n} : \begin{array}{l} P_1 = \{\bar{x}_i\}_{i=1}^{m} \\ \\ P_2 = \{\bar{x}_i\}_{i=m+1}^{n} \end{array}$$

$$\{\hat{x}_i\}_{i=1}^{m+n} : \begin{array}{l} Q_1 = \{\hat{x}_i\}_{i=1}^{n} \\ \\ Q_2 = \{\hat{x}_i\}_{i=n+1}^{m} \end{array}$$

فرآیند انتشار

$$\{\bar{x}_i\}_{i=1}^{m+n} : \begin{cases} P_1 = \{\bar{x}_i\}_{i=1}^{m} \\ P_2 = \{\bar{x}_i\}_{i=m+1}^{n} \end{cases}$$

$$\{\hat{x}_i\}_{i=1}^{m+n} : \begin{cases} Q_1 = \{\hat{x}_i\}_{i=1}^{n} \\ Q_2 = \{\hat{x}_i\}_{i=n+1}^{m} \end{cases}$$

فرآیند انتشار

$$\{\bar{x}_i\}_{i=1}^{m+n} : \begin{array}{l} \nearrow P_1 = \{\bar{x}_i\}_{i=1}^{m} \\ \searrow P_2 = \{\bar{x}_i\}_{i=m+1}^{n} \end{array}$$

$$\{\hat{x}_i\}_{i=1}^{m+n} : \begin{array}{l} \nearrow Q_1 = \{\hat{x}_i\}_{i=1}^{n} \\ \searrow Q_2 = \{\hat{x}_i\}_{i=n+1}^{m} \end{array}$$

فرآیند انتشار

مرتب سازی $P_2, Q_2 \Longrightarrow P_2', Q_2'$

جایگشت بین $Q_2, Q_2' : P_2, P_2'$ به ترتیب : $\Longrightarrow S_1, S_2$

اثر S_1, S_2 روی P_1, Q_1 به ترتیب: $\Longrightarrow \bar{P}_1, \bar{Q}_1$

مرتب سازی $\bar{P}_1, \bar{Q}_1 \Longrightarrow \bar{\bar{P}}_1, \bar{\bar{Q}}_1$

جایگشت بین $\bar{P}_1, \bar{\bar{P}}_1 : \bar{Q}_1, \bar{\bar{Q}}_1$ به ترتیب : $\Longrightarrow H, L$

فرآیند انتشار

مرتب سازی $P_۲ , Q_۲ \Longrightarrow P'_۲ , Q'_۲$

جایگشت بین $Q_۲ , Q'_۲$: $P_۲ , P'_۲$ به ترتیب : $\Longrightarrow S_۱ , S_۲$

اثر $S_۱ , S_۲$ روی $P_۱ , Q_۱$ به ترتیب: $\Longrightarrow \bar{P}_۱ , \bar{Q}_۱$

مرتب سازی $\bar{P}_۱ , \bar{Q}_۱ \Longrightarrow \bar{\bar{P}}_۱ , \bar{\bar{Q}}_۱$

جایگشت بین $\bar{P}_۱ , \bar{\bar{P}}_۱$: $\bar{Q}_۱ , \bar{\bar{Q}}_۱$ به ترتیب : $\Longrightarrow H , L$

فرآیند انتشار

مرتب سازی $P_۲ \,, Q_۲ \Longrightarrow P'_۲ \,, Q'_۲$

جایگشت بین $Q_۲ \,, Q'_۲ \;:\; P_۲ \,, P'_۲$ به ترتیب : $\Longrightarrow S_۱ \,, S_۲$

اثر $S_۱ \,, S_۲$ روی $P_۱ \,, Q_۱$ به ترتیب: $\Longrightarrow \bar{P}_۱ \,, \bar{Q}_۱$

مرتب سازی $\bar{P}_۱ \,, \bar{Q}_۱ \Longrightarrow \bar{\bar{P}}_۱ \,, \bar{\bar{Q}}_۱$

جایگشت بین $\bar{P}_۱ \,, \bar{\bar{P}}_۱ \;:\; \bar{Q}_۱ \,, \bar{\bar{Q}}_۱$ به ترتیب : $\Longrightarrow H, L$

فرآیند انتشار

مرتب سازی $P_۲ , Q_۲ \Longrightarrow P'_۲ , Q'_۲$

جایگشت بین $Q'_۲ , Q_۲ \ : P'_۲ , P_۲$ به ترتیب : $\Longrightarrow S_۲ , S_۱$

اثر $S_۲ , S_۱$ روی $Q_۱ , P_۱$ به ترتیب: $\Longrightarrow \bar{Q}_۱ , \bar{P}_۱$

مرتب سازی $\bar{Q}_۱ , \bar{P}_۱ \Longrightarrow \bar{\bar{Q}}_۱ , \bar{\bar{P}}_۱$

جایگشت بین $\bar{P}_۱ , \bar{P}_۱ : \bar{\bar{Q}}_۱ , \bar{Q}_۱$ به ترتیب : $\Longrightarrow L , H$

فرآیند انتشار

مرتب سازی $P_۲ , Q_۲ \Longrightarrow P'_۲ , Q'_۲$

جایگشت بین $Q_۲ , Q'_۲ : P_۲ , P'_۲$ به ترتیب : $\Longrightarrow S_۱ , S_۲$

اثر $S_۱ , S_۲$ روی $P_۱ , Q_۱$ به ترتیب: $\Longrightarrow \bar{P}_۱ , \bar{Q}_۱$

مرتب سازی $\bar{P}_۱ , \bar{Q}_۱ \Longrightarrow \bar{\bar{P}}_۱ , \bar{\bar{Q}}_۱$

جایگشت بین $\bar{P}_۱ , \bar{\bar{P}}_۱ : \bar{Q}_۱ , \bar{\bar{Q}}_۱$ به ترتیب : $\Longrightarrow H , L$