
بسم الله الرحمن الرحیم

پیاده‌سازی الگوریتم رمزنگاری تصویر مبتنی بر محاسبات دی‌ان‌ای و توابع درهم‌ساز بر روی پردازنده‌گرافیکی با استفاده از پایتورچ

استاد راهنما : دکتر ابراهیم زارعی

پژوهشگر : امیررضا حسینی دهلقی

دانشگاه اصفهان
دانشکده ریاضی و کامپیوتر خوانسار

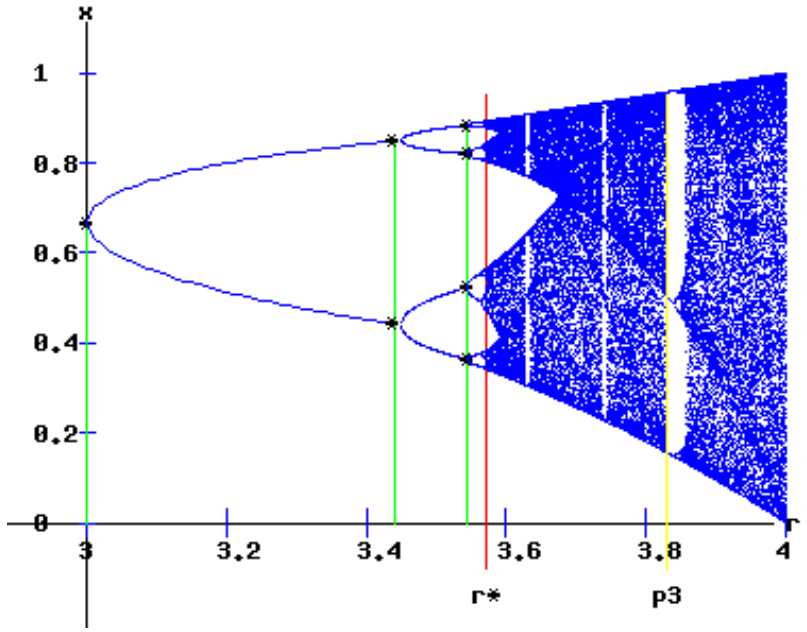
۲۰ تیر ۱۴۰۳

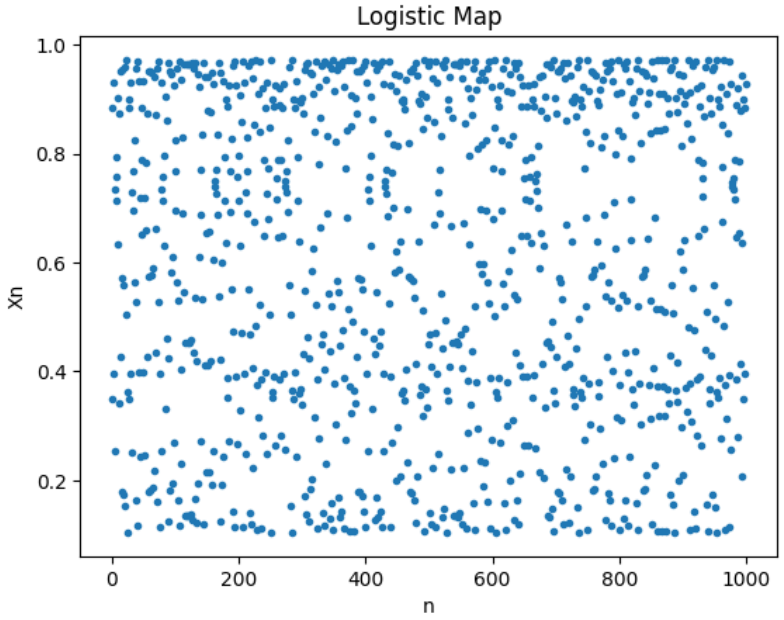
فهرست

مقدمه

- امنیت اطلاعات
- رمزنگاری تصویر
- چالش‌ها
  - پیچیدگی حافظه‌ای
  - پیچیدگی زمانی

مفاهیم پایه





1) نگاشت آشوب لجستیک یک بعدی

پیاده‌سازی با پایتون

```
def logistic_map(x, r):
    return r * x * (1 - x)
```

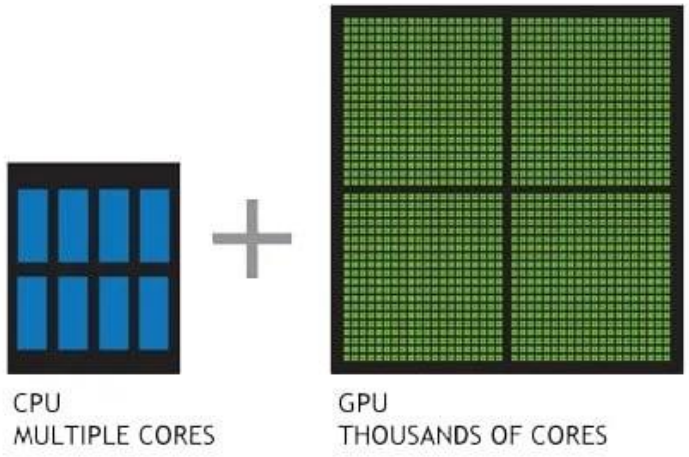
نمونه اجرای تابع برای تولید هزار عدد با مقادیر اولیه روبه رو :

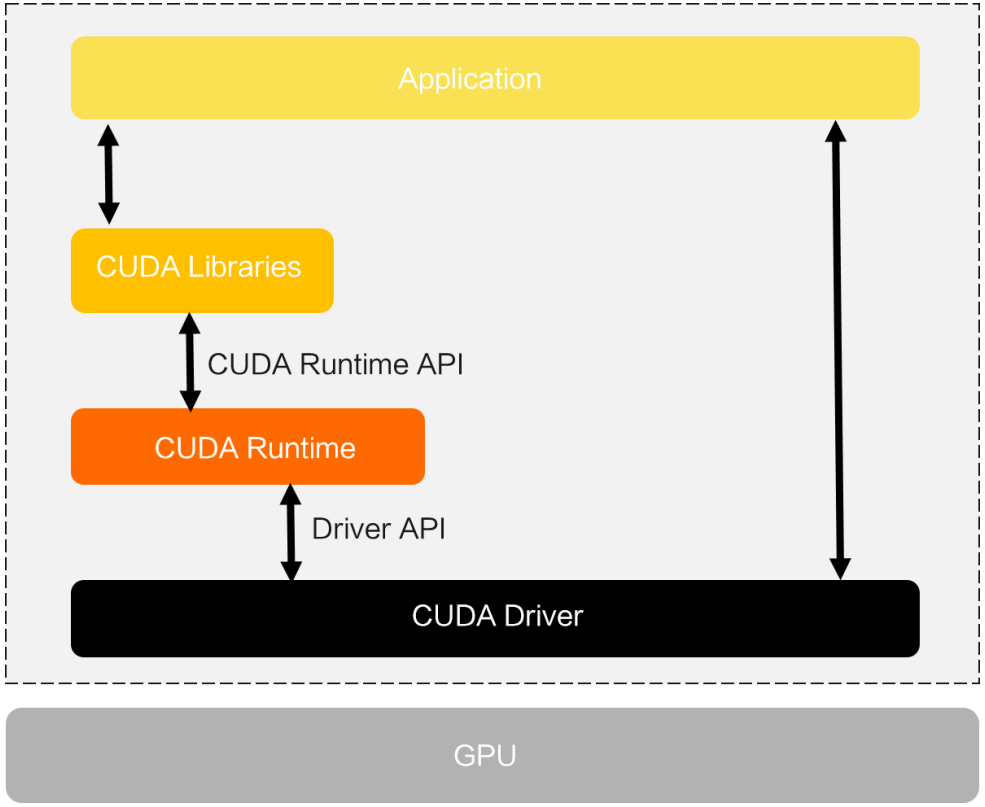
```
r = 3.89
x = 0.1  # Initial condition for x


for n in range(1000):
    x = logistic_map(x,r)
    ys.append(x)  # Store x
```

مفاهیم پایه

2) پردازنده گرافیکی

- هسته های کودا و استفاده از آنها






```
!nvidia-smi
```

```
Sun Jul  7 08:35:09 2024
+---------------------------------------------------------------------------------------+
| NVIDIA-SMI 535.104.05             Driver Version: 535.104.05   CUDA Version: 12.2     |
|-----------------------------------------+----------------------+----------------------+
| GPU  Name                 Persistence-M | Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp   Perf          Pwr:Usage/Cap |         Memory-Usage | GPU-Util  Compute M. |
|                                         |                      |               MIG M. |
|=========================================+======================+======================|
|   0  Tesla T4                       Off | 00000000:00:04.0 Off |                    0 |
| N/A   39C    P8              9W /  70W |      0MiB / 15360MiB |      0%      Default |
|                                         |                      |                  N/A |
+-----------------------------------------+----------------------+----------------------+

+---------------------------------------------------------------------------------------+
| Processes:                                                                            |
|  GPU   GI   CI        PID   Type   Process name                            GPU Memory |
|        ID   ID                                                             Usage      |
|=======================================================================================|
|  No running processes found                                                           |
+---------------------------------------------------------------------------------------+
```

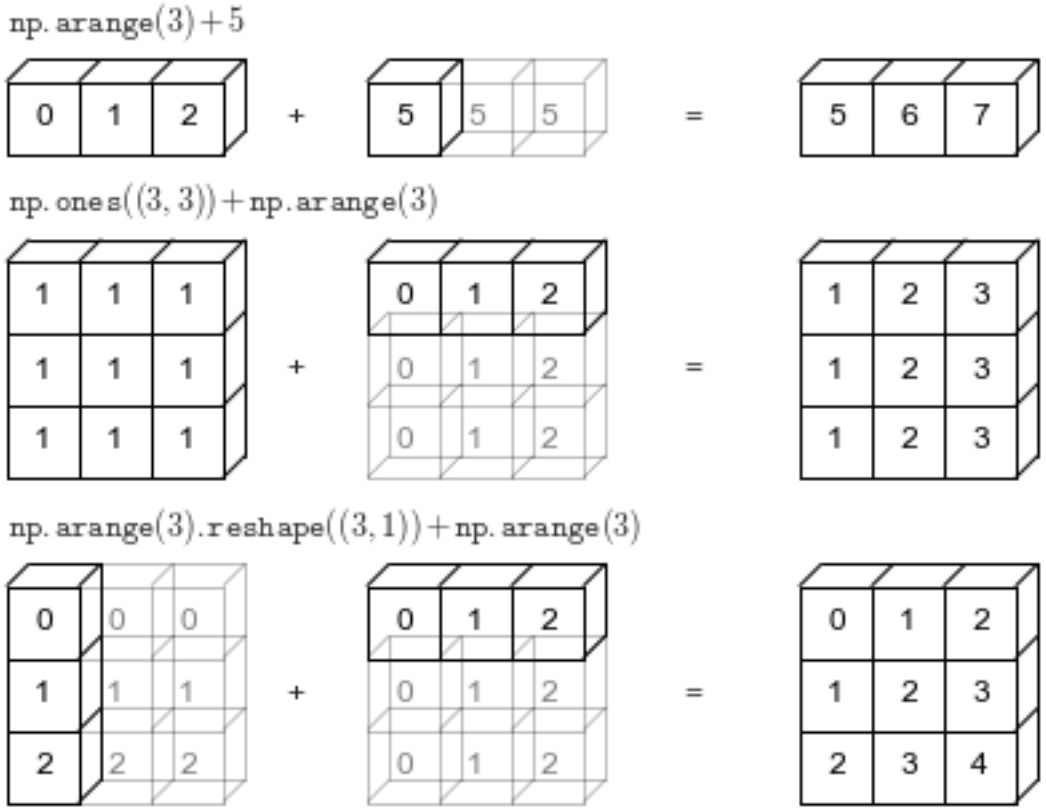
مفاهیم پایه

"بسیاری از عملیات های PyTorch از مفاهیم پخش NumPy پشتیبانی می کنند."

2) Broadcasting

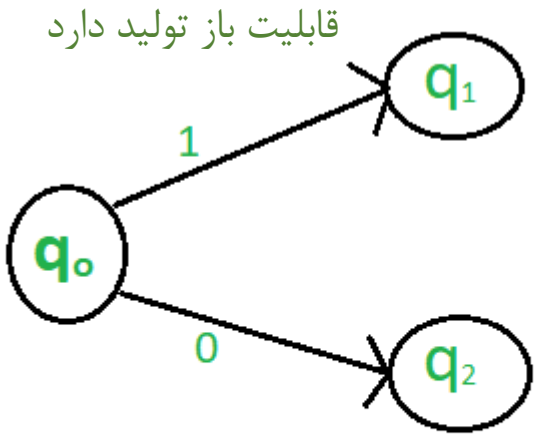
اگر قوانین زیر رعایت شود، دو تنسور قابل پخش هستند:

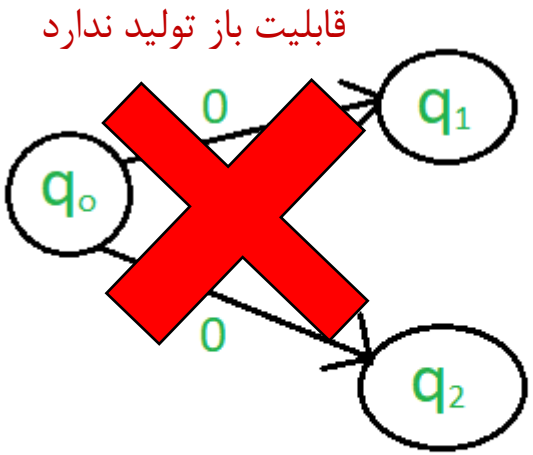
- هر تنسور حداقل یک بعد داشته باشد.
- در هنگام پیمایش اندازه‌های بعد، از بعد آخر شروع کرده و اندازه‌های بعد باید یکی از موارد زیر باشد:
  - i. برابر باشند.
  - ii. یکی از آن‌ها برابر یک باشد.
  - iii. یکی از آن‌ها وجود نداشته باشد.



مفاهیم پایه

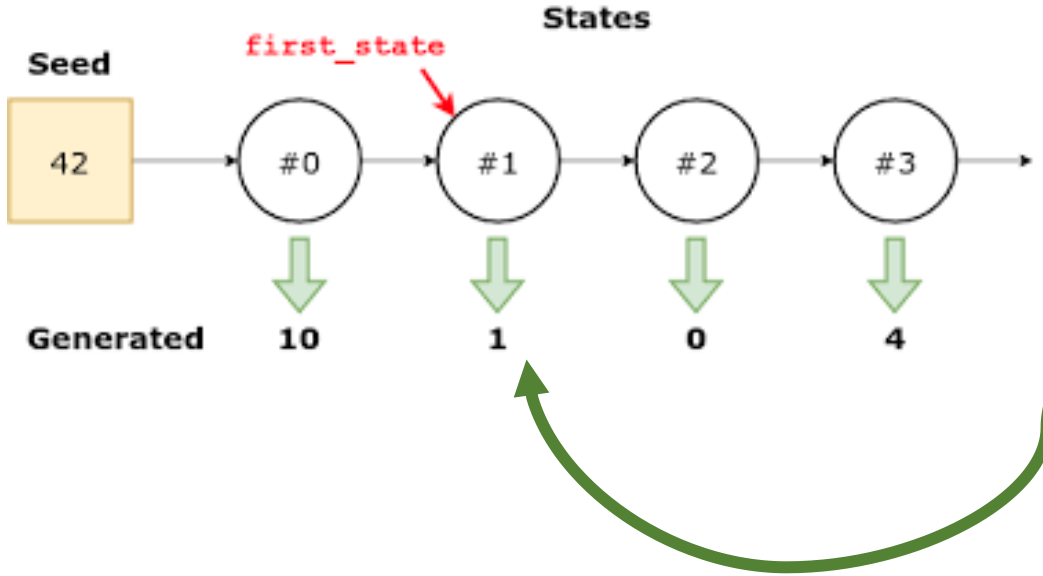
3) الگوریتم های قطعی و غیر قطعی





Deterministic Algorithm

Non-Deterministic Algorithm



× کاهش سرعت

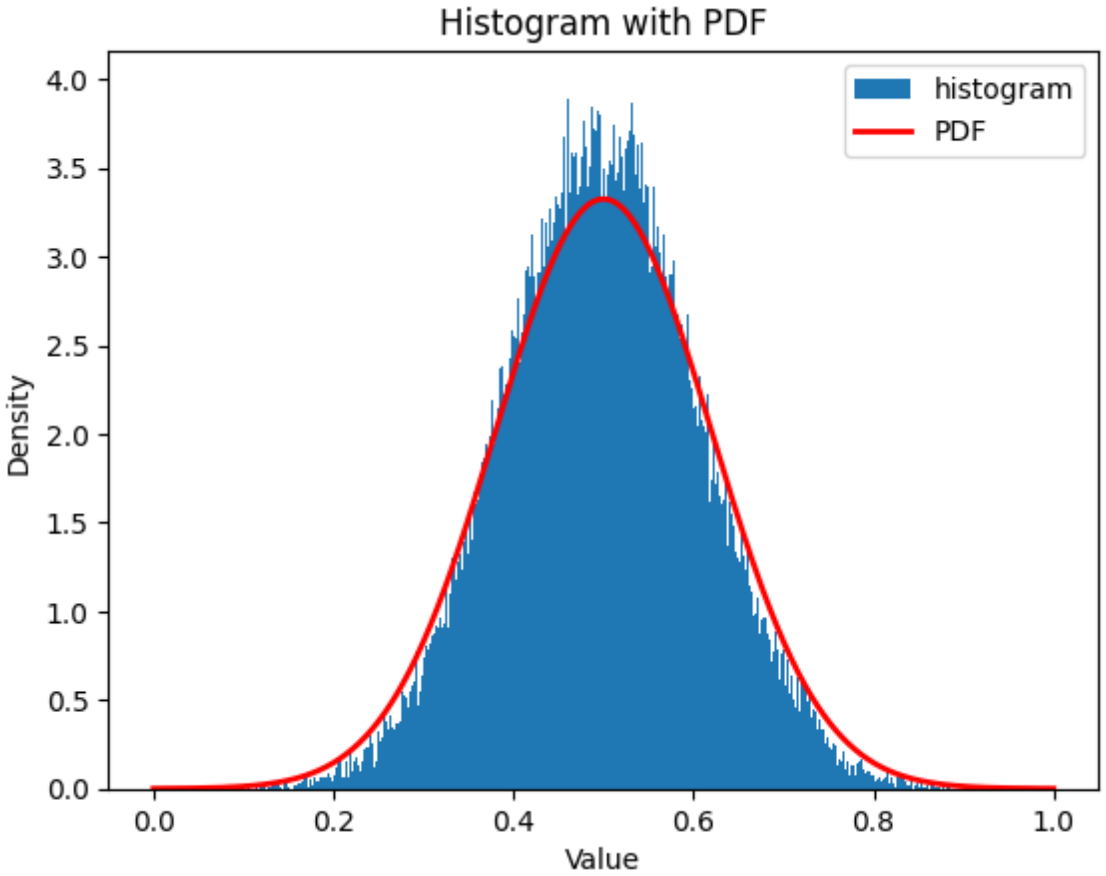
```
torch.backends.cudnn.benchmark = False
torch.use_deterministic_algorithms(True)

torch.manual_seed(42)
```

مفاهیم پایه

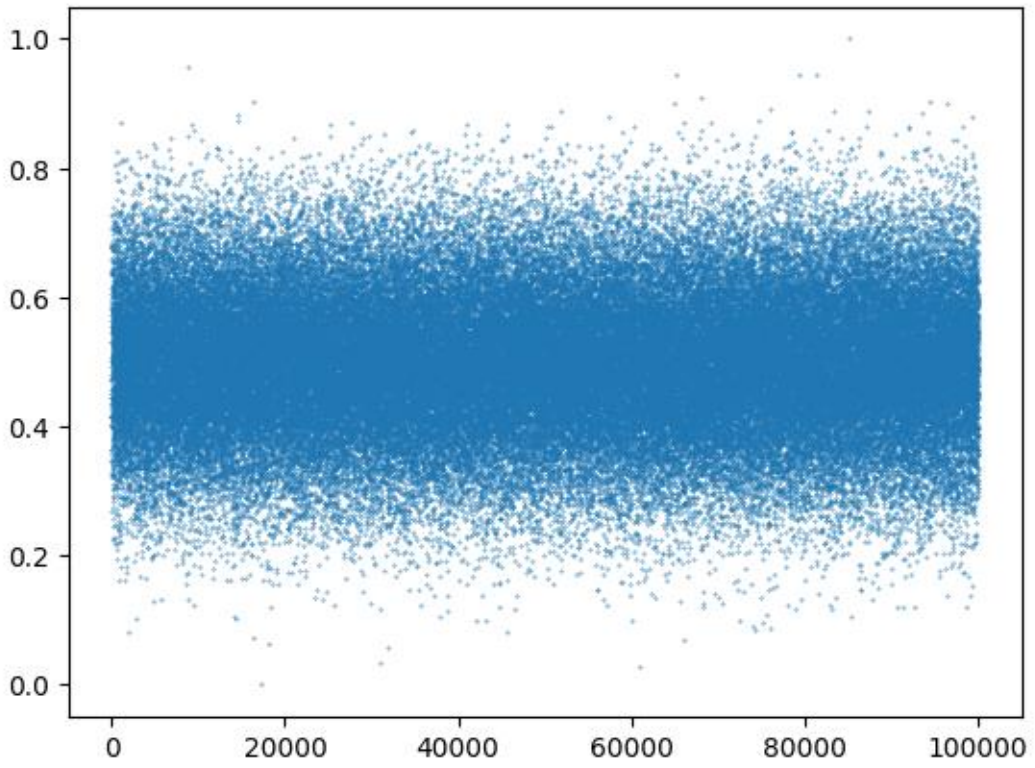
4) تابع توزیع نرمال

torch.normal(*mean*, *std*, *, *generator=None*, *out=None*) → Tensor

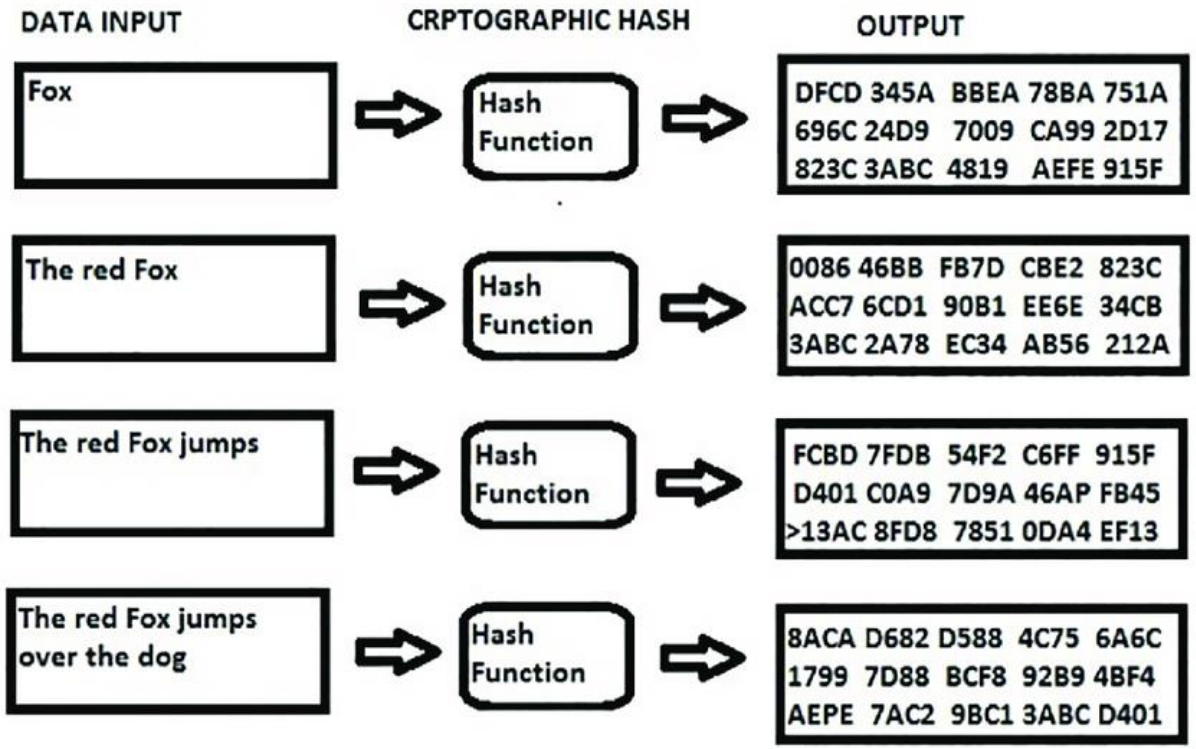
```
mu = 0.5
sigma = 0.12
torch.manual_seed(42)
s = torch.normal(mu, sigma, size = (100000,))
s = (s - s.min()) / (s.max() - s.min())
```



مقادیر تولید شده



مفاهیم پایه



5) **توابع درهم ساز**

- طول خروجی تابع هش همیشه **ثابت** است.
- تا زمانی که ورودی تغییر نکند، مقداری خروجی تابع درهم‌ساز قطعی و ثابت است.
- یک‌طرفه.

نمونه های توابع درهم‌ساز

× MD5

× SHA1

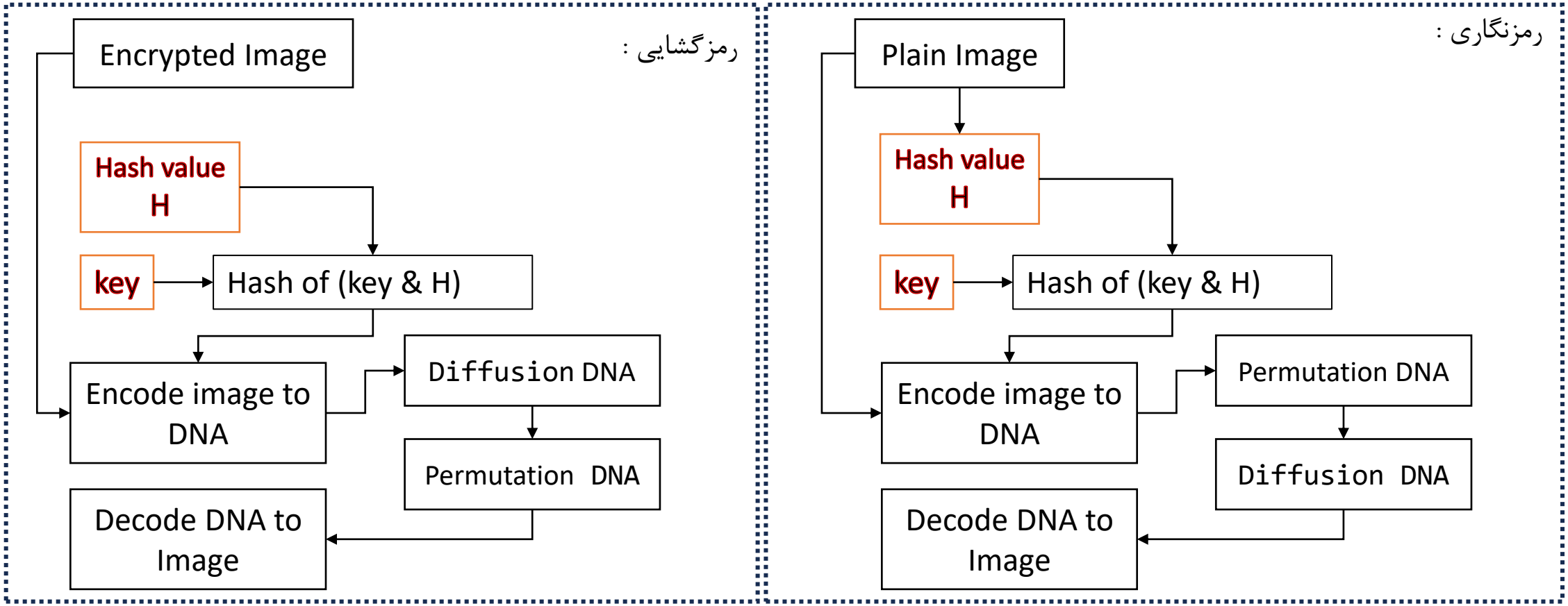
✓ SHA256

✓ SHA384

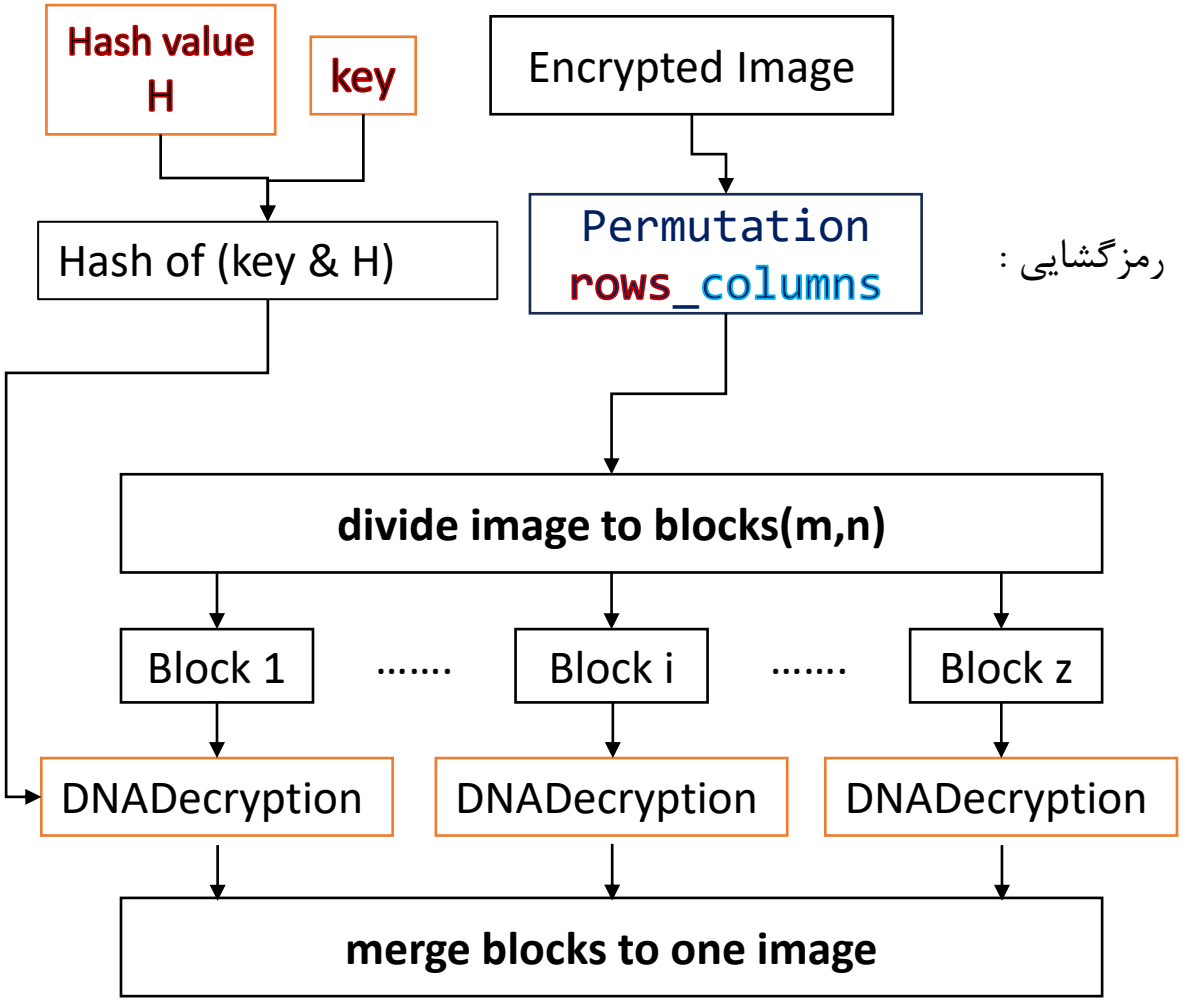
✓ SHA512

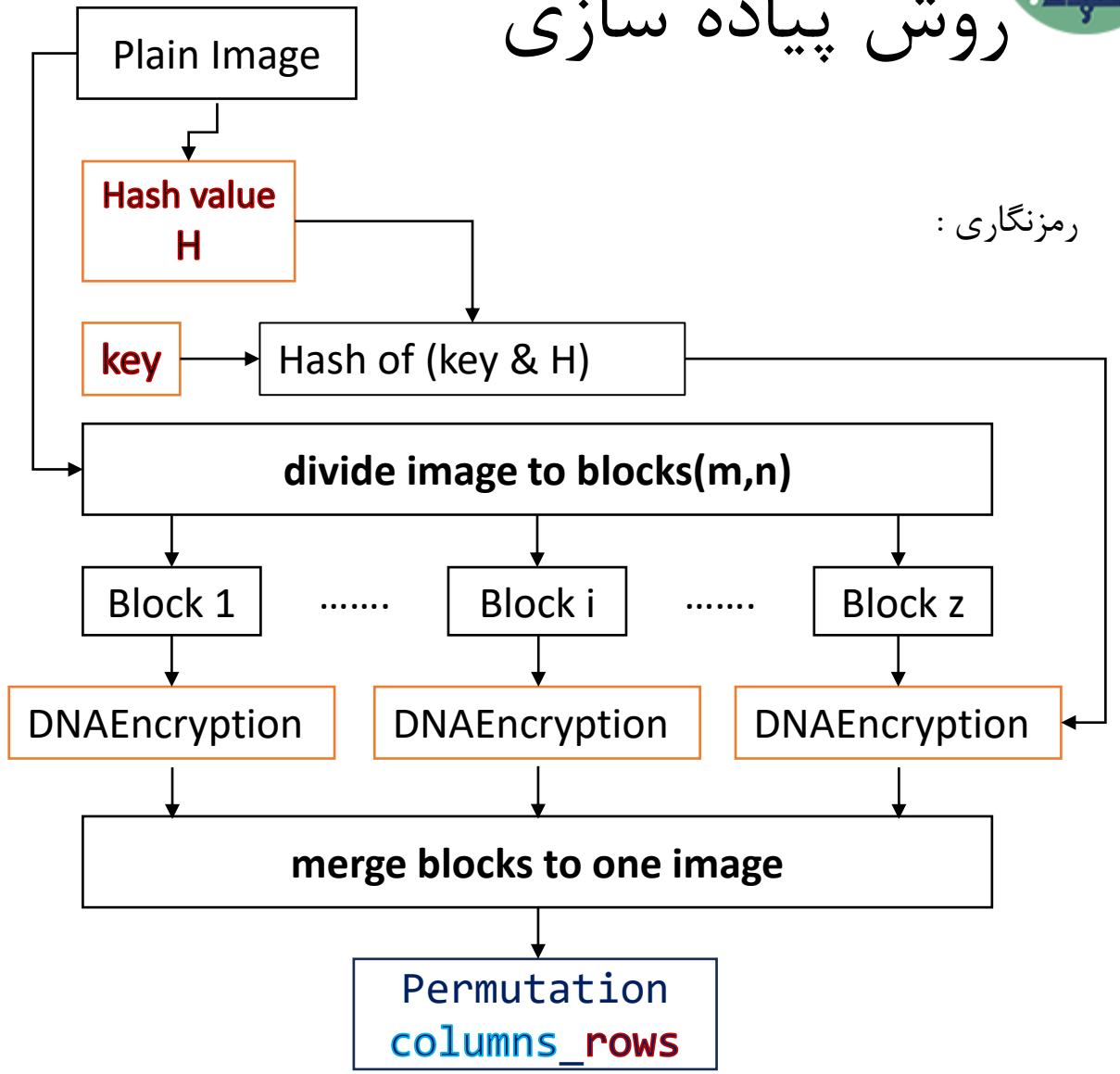
الگوریتم استفاده شده

DNADecryption | DNAEncryption



روش پیاده سازی



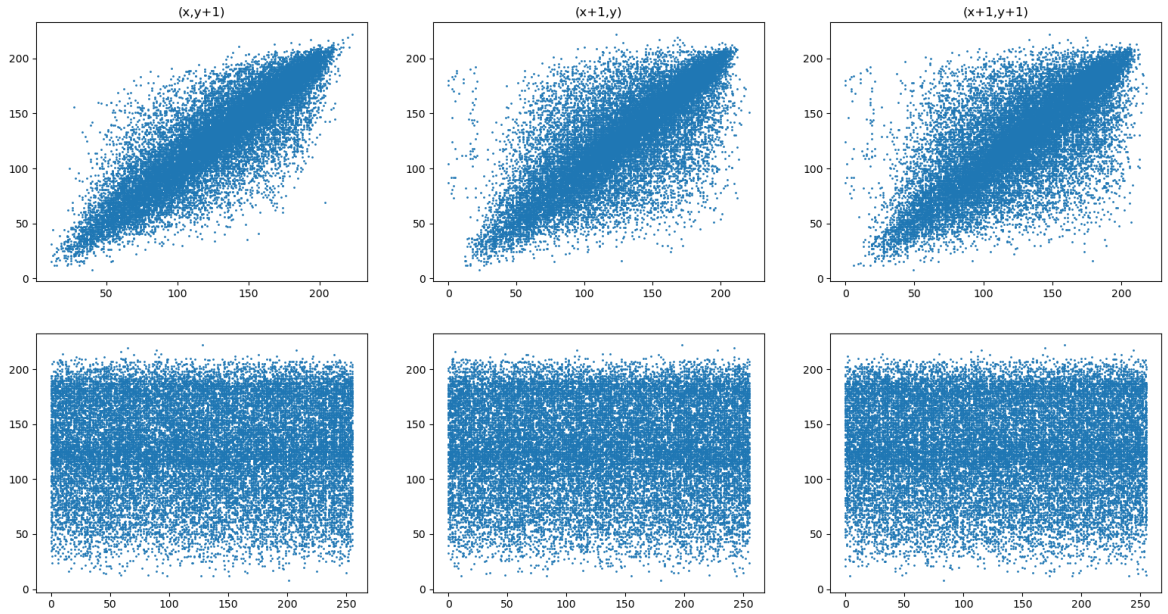


نتایج پیاده سازی

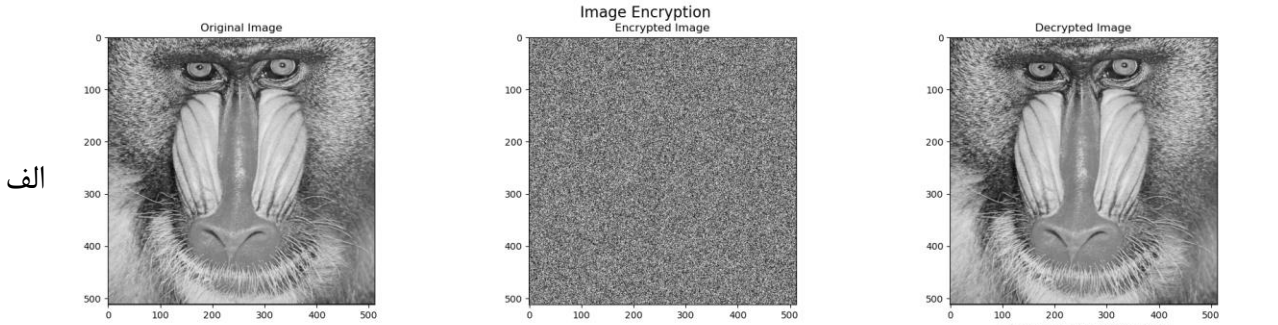
❖نتایج تحلیل هیستوگرام و همبستگی پیکسل‌ها

همبستگی پیکسل ها :

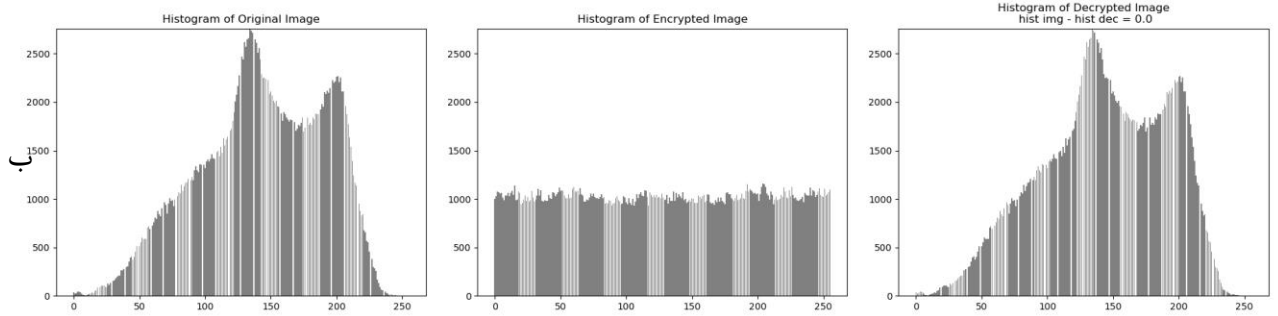
عمودی | افقی | قطری



الف



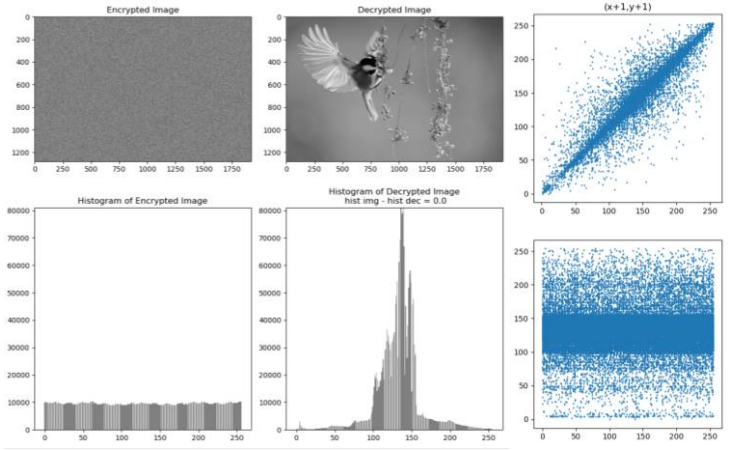
ب



نتایج پیاده سازی

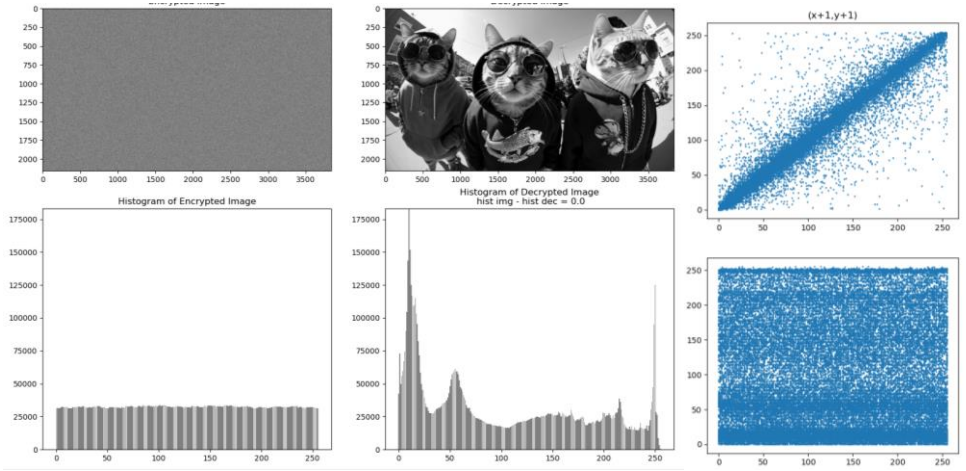
❖نتایج تحلیل هیستوگرام و همبستگی پیکسل‌ها (تصاویر بزرگ)

FHD = 2.5MP

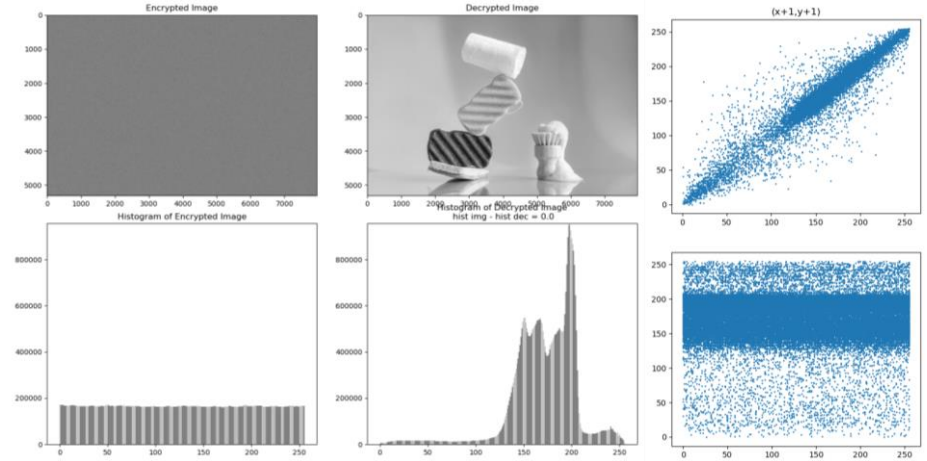


1278*1920

4k = 8 MP

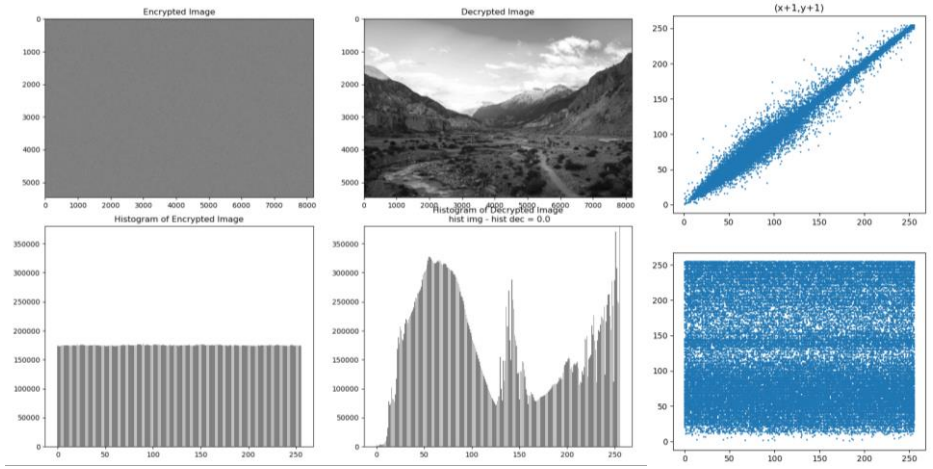


2160*3840



5304*7952

42MP



5461*8192

45MP

نتایج پیاده سازی

نام	اندازه	افقی	عمودی	قطری
لنا	262KP	0.9851	0.9733	0.9591
لنا رمز	262KP	0.0019	0.0095	0.0078
فلفل	262KP	0.9835	0.9772	0.9668
فلفل رمز	262KP	0.0003	-0.0076	0.0012
عکاس	262KP	0.9906	0.9831	0.9742
عکاس رمز	262KP	0.0024	0.0010	0.0021
بابون	262KP	0.7556	0.8661	0.7225
بابون رمز	262KP	-0.0066	0.0077	-0.0071
پرنده	2.5MP	0.9693	0.9617	0.9432
پرنده رمز	2.5MP	0.0017	-0.0021	-0.0012
گربه	8MP	0.9909	0.9912	0.9856
گربه رمز	8MP	-0.0067	-0.0028	0.0126
اسفنج	42MP	0.9814	0.9803	0.9667
اسفنج رمز	42MP	-0.0099	-0.0087	0.0008
دره	45MP	0.7556	0.8661	0.7225
دره رمز	45MP	-0.0024	-0.0071	-0.0087

❖تحلیل ضرایب همبستگی

- مقدار ضریب همبستگی در تصویر اصلی ☚ نزدیک یک
- مقدار ضریب همبستگی در تصویر رمز ☚ نزدیک صفر

نتایج پیاده سازی

نام	اندازه	آنتروپی تصویر اصلی	آنتروپی تصویر رمز شده
لنا	262KP	7.59292	7.99919
فلفل	262KP	7.57147	7.99925
عکاس	262KP	7.04230	7.99923
بابون	262KP	7.35794	7.99848
پرنده	2.5MP	6.53050	7.99897
گربه	8MP	7.70758	7.99977
اسفنج	42MP	6.79714	7.99988
دره	45MP	7.79358	7.99998

❖تحلیل آنتروپی

- مقدار ایده‌ال برای تصویر رمز ☚ 8

نتایج پیاده سازی

نام	اندازه	UACI	NPCR
لنا	262KP	33.5066	99.5934
فلفل	262KP	33.5043	99.6181
عکاس	262KP	33.5635	99.6181
بابون	262KP	33.5882	99.6052
پرنده	2.5MP	33.7374	99.6090
گربه	8MP	33.3213	99.6062
اسفنج	42MP	33.5431	99.6092
دره	45MP	33.4424	99.6093

❖تحلیل حملات تفاضلی

- **NPCR**
  - نرخ پیکسل‌های تغییریافته در تصویر رمز به ازای یک بیت تغییر در تصویر اصلی
  - مقدار ایده‌آل: 99.6094
- **UACI**
  - متوسط اختلاف شدت سطح روشنایی دو تصویر رمزشده
  - مقدار ایده‌آل: 33.4635

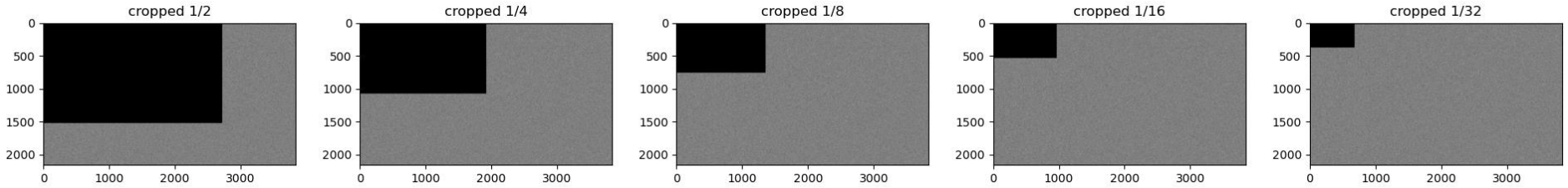
نتایج پیاده سازی

❖نتایج حمله برش

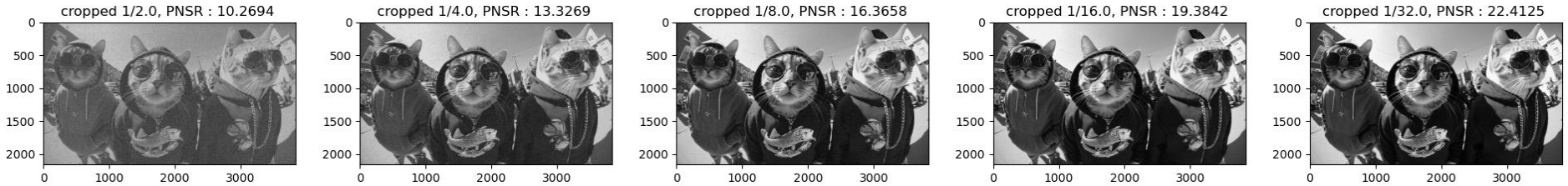
- **PSNR**
- **نسبت پیک سیگنال به نویز بین تصویر اصلی و تصویر رمزگشایی شده**

نام	اندازه	نرخ برش				
		1/32	1/16	1/8	1/4	1/2
لنا	262KP	23.4933	20.4429	17.4493	14.4590	11.5322
فلفل	262KP	23.3233	20.3055	17.3286	14.3493	11.4252
عکاس	262KP	23.8419	20.8027	17.7476	14.7042	11.6260
بابون	262KP	24.3680	21.3785	18.4002	15.4220	12.5184
پرنده	2.5MP	24.7469	21.7370	18.7736	15.8354	13.0035
گربه	8MP	22.4125	19.3842	16.3658	13.3269	10.2694
اسفنج	42MP	23.5222	20.5160	17.5383	14.5955	11.7196
دره	45MP	22.8671	19.8539	16.8488	13.8417	10.8543

تصویر رمز بعد از برش



تصویر رمزگشایی شده



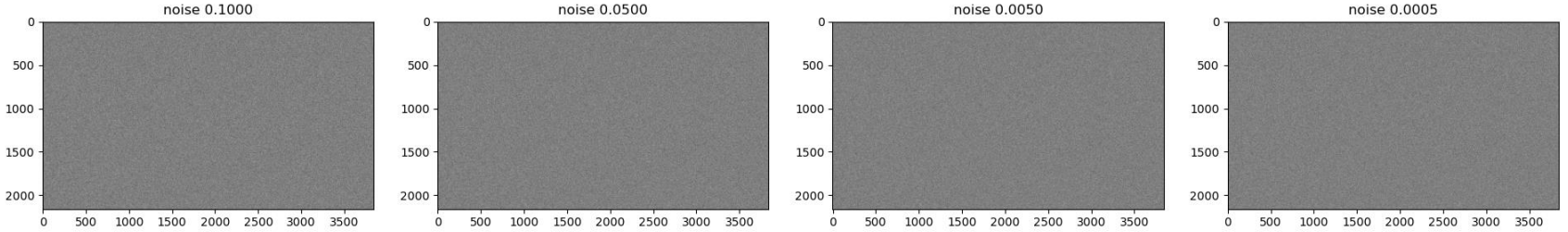
نتایج پیاده سازی

❖نتایج حمله نویز

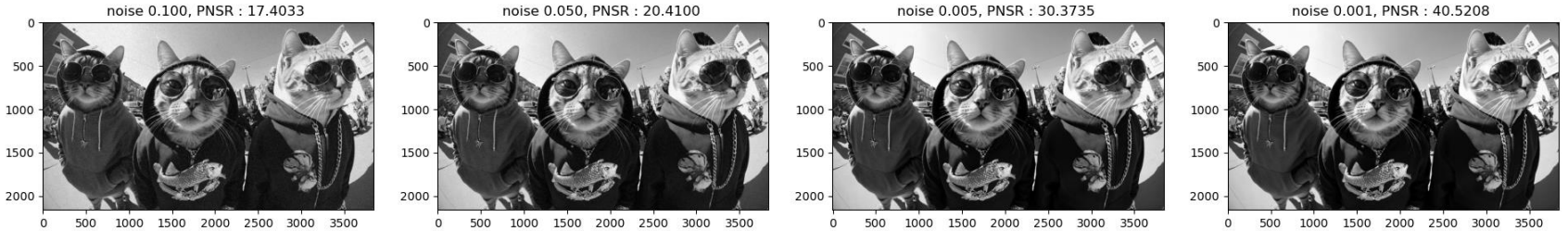
- **PSNR**
- **نسبت پیک سیگنال به نویز بین تصویر اصلی و تصویر رمزگشایی شده**

نام	اندازه	چگالی نویز فلفل و نمک			
		0.0005	0.005	0.05	0.1
لنا	262KP	41.2297	31.4630	21.5306	18.5009
فلفل	262KP	41.2108	31.4715	21.3952	18.4607
عکاس	262KP	42.1246	32.3288	21.7837	18.7943
بابون	262KP	42.0813	32.4846	22.3277	19.4459
پرنده	2.5MP	42.4080	32.6560	22.7651	19.7839
گربه	8MP	40.5208	30.3735	20.4100	17.4033
اسفنج	42MP	41.4294	31.4170	21.4476	18.4622
دره	45MP	40.8814	30.8503	20.8638	17.8608

تصویر رمز بعد از ایجاد نویز



تصویر رمزگشایی شده



نتایج پیاده سازی

❖زمان اجرا

نام	اندازه	زمان رمزنگاری	زمان رمز گشایی
لنا	262KP	0.0183	0.0183
فلفل	262KP	0.0186	0.0185
عکاس	262KP	0.0215	0.0209
بابون	262KP	0.0178	0.0179
پرنده	2.5MP	0.1893	0.1700
گربه	8MP	0.4529	0.4407
اسفنج	42MP	1.7712	1.7111
دره	45MP	2.0441	1.9798

نمونه های مشابه برای تصاویر 256KP

Table 10 Execution time analysis in the encryption and decryption process

Test image	Encryption process						Decryption process					
	Proposed	Ref. [13]	Ref. [38]	Ref. [22]	Ref. [5]	Ref. [45]	Proposed	Ref. [13]	Ref. [38]	Ref. [22]	Ref. [5]	Ref. [45]
Lena	0.8175	14.8401	15.8259	71.7947	10.8232	38.5336	1.3667	14.9266	13.3493	72.0903	10.6952	37.2344
Babcon	0.8236	14.9134	15.8617	71.3306	10.7477	38.0776	1.3645	14.9678	13.3824	71.2461	10.7146	36.5774
Peppers	0.8197	14.6393	15.7571	71.8539	10.7321	38.0822	1.3589	14.7637	13.2887	71.6227	10.6869	36.9910
Cameraman	0.8126	15.0087	15.8764	71.7842	10.8053	38.5579	1.3586	15.2032	13.4003	71.6566	10.7977	36.7060

نتیجه‌گیری

- ✓ فضای کلید در صورت استفاده از تابع درهم‌ساز SHA256 برابر با : 2^{512}
- ✓ سرعت اجرای بالا
- × نیاز به الگوریتم بهتر برای تولید اعداد تصادفی

مراجع

[1] Zefreh, E. Z (.2020.) An image encryption scheme based on a hybrid model .SpringerLink ,24993–25022

[2] Biradar, S., T. Akkasaligar, P., & Biradar , S. (2023). A Parallel DNA Crypto Algorithm for Medical Image. *SpringerLink*, 183–190.

[3] https://pytorch.org/docs/stable/index.html