عنوان ارائه:

یک سیستم رمزنگاری حفظ حریم خصوصی برای سامانه‌های مراقبت بهداشتی الکترونیکی اینترنت اشیاء

A privacy-preserving cryptosystem for IoT e-healthcare

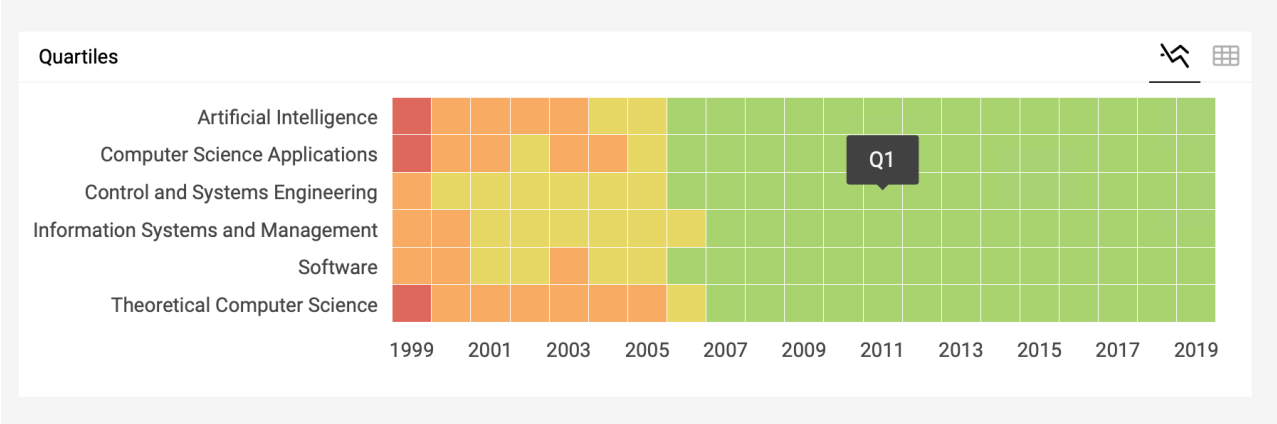
توسط: علیرضا صادقی نسب

استاد: دکتر حسین غفاریان

تاریخ ارائه: ۱۳۹۹/۱۲/۲۰

مقدمه

- اطلاعات مقاله
  - عنوان: *A privacy – preserving cryptosystem for IoT e – healthcare*
  - سال چاپ: 2020
  - تعداد ارجاع: 58
  - مجله: *Information Sciences*
  - ناشر: *Elsevier*



مقدمه

- اطلاعات نویسندگان

Rafik Hamza

NICT
Verified email at nict.go.jp - Homepage
Security & Privacy Applied Cryptography Signal Processing Chaotic systems

Citations	562	562
h-index	9	9
i10-index	9	9

Zheng Yan

Professor, Xidian University
Verified email at xidian.edu.cn - Homepage
Information and Network S… Privacy Preservation Trust Modeling and Manag…
Social Networking Mobile Communications

Citations	6974	5320
h-index	40	35
i10-index	138	111

Khan Muhammad FOLLOW

Assistant Professor, Department of Software, Sejong University, Seoul 143-747, Republic of Korea
Verified email at ieee.org - Homepage
Information Security Video Summarization Computer Vision Video Analytics Deep Learning

Citations	5426	5390
h-index	44	44
i10-index	103	103

Paolo Bellavista

Full Professor, University of Bologna
Verified email at unibo.it - Homepage
Pervasive and Mobile Com… Middleware Edge Computing Industry4.0
Online Stream Processing

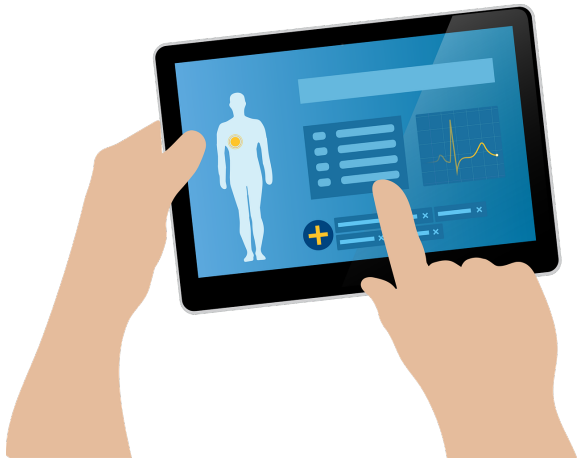
Citations	8675	4094
h-index	41	26
i10-index	143	76

فهرست مطالب

- مقدمه
- معرفی روش
- آنالیز امنیتی
- بررسی نقاط قوت و ضعف

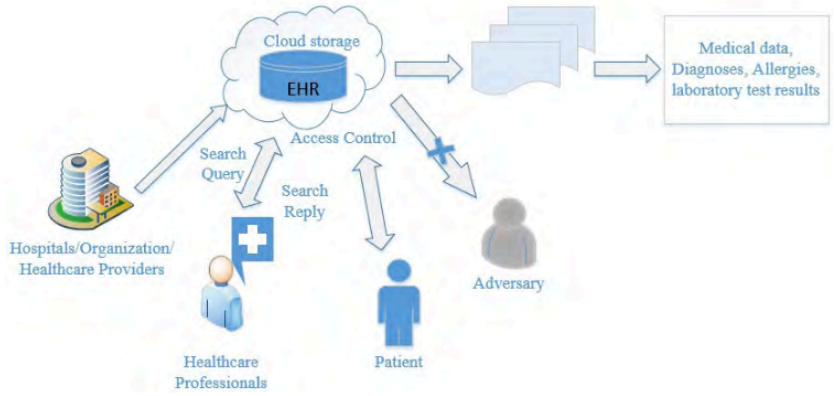
مقدمه

- سامانه‌های مراقبتی بهداشتی الکترونیکی
  - در قرن ۲۱، بسیاری از روش‌های کاغذی، تبدیل به این سامانه‌ها شدند
  - این سامانه‌ها، از جهت به اشتراک‌گذاری داده‌ها، بسیار کارآمدتر از روش‌های سنتی قبلی هستند
  - داده‌های تبدیل شده به صورت کلی شامل موارد زیر هستند:
    - سوابق پزشکی الکترونیکی (*EMR*)
    - سوابق سلامتی پزشکی (*EHR*)
    - سوابق سلامتی شخصی (*PHR*)
    - داده‌های سلامتی الکترونیک (*EHD*)



مقدمه

- لزوم حفظ حریم خصوصی در سامانه‌های مراقبت بهداشتی الکترونیکی
  - داده‌های موجود در این سامانه‌ها، شامل عکس‌ها و اطلاعات بیماران است. لذا، این داده‌ها را می‌توان در دسته داده‌های شخصی و حساس قرار داد
  - اگر فضای دسترسی به داده‌ها توسط افراد غیرقابل مجاز، وجود داشته باشد، ممکن است این داده‌ها توسط این افراد، تغییر داده شود



مقدمه

- رمزنگاری در عکس‌های دیجیتالی

- در روش متداول، فرستنده با یک کلید مخفی اقدام به رمزنگاری داده کرده و به سمت گیرنده می‌فرستد. گیرنده نیز با داشتن کلید مخفی فوق، اقدام به رمزگشایی می‌کند
- رمزنگاری در حالت بالا معمولاً توسط الگوریتم‌های رمزنگاری همگن و مبتنی بر ویژگی اتفاق می‌افتد
- در روش بالا، امنیت کاملاً وابسته به نگهداری کلید مخفی است

Level of Security ⟺ Computational Complexity

مقدمه

- ویژگی یک سیستم رمزنگاری خوب
  - ☑ نسبت به تغییرات کلید مخفی بسیار حساس باشد
  - ☑ پیچیدگی محاسباتی کمی داشته باشد
- مشکل روش‌های قدیمی چیست؟
  - ☑ روش‌های قدیمی پراستفاده معمولاً شامل *DES*, *AES* و *IDEA* هستند
  - ☑ این روش‌ها برای داده‌های متنی و یک بعدی به کار می‌روند و برای عکس مناسب نیستند
  - ☑ پیچیدگی محاسباتی زیادی دارند و مناسب سیستم‌های بلادرنگ نیستند

معرفی روش

- الگوریتم کلیدهای رمزنگاری

☆ نام: نقشه آشفته دو بعدی *Zaslavsky*

☆ مقدار طیف *lyapunov* الگوریتم بالا ۱.۵۵ محاسبه شده است. این مقدار نشان می‌دهد مشخصات آماری تصادفی خوبی دارد

☆ بنابراین، خروجی سیستم بسیار آشفته و غیرقابل پیشگویی است

✱ فرمول به صورت زیر است:

$$\begin{cases} x_{i+1} = x_i + v\ (1 + uy_i) + \varepsilon vu\ (\cos(2\pi x_i)) \bmod 1 \\ y_{i+1} = e^{-\tau}(y_i + \varepsilon \cos\ (2\pi x_i)) \\ Where, \quad u = \frac{1-e^{-\tau}}{\tau} \end{cases}$$

معرفی روش

- الگوریتم کلیدهای رمزنگاری (ادامه)

☆ نام: نقشه دو بعدی *logistic*

☆ یک سیستم گسسته پویا با رفتاری آشفته است

☆ نقشه غیرخطی فوق، رفتار تصادفی پیچیده‌تری نسبت به نقشه یک بعدی خود دارد

✱ فرمول به صورت روبه‌رو است:

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases}$$

☆ اگر مقدار r در بازه ۱.۱ تا ۱.۱۹ باشد، سیستم دوبعدی لجستیکی ما، آشفته خواهد بود

☆ مقدار طیف *lyapunov* الگوریتم ۳.۶۸ محاسبه شده است. این مقدار نشان می‌دهد خروجی سیستم، آشفته و غیرقابل پیش‌بینی است

معرفی روش

- الگوریتم کلیدهای رمزنگاری (ادامه)

☆ نام: مولد شبه اعداد تصادفی

☆ از خروجی الگوریتم برای رمزنگاری پیکسل‌های عکس ورودی استفاده می‌شود

Algorithm 1 Pseudo random numbers generator.

Input: $x_{l(0)}, y_{l(0)}, v, \varepsilon, \tau, x_{z(0)}, y_{z(0)}, r, m.$

1: $[x_l, y_l] \leftarrow [x_{l(0)}, y_{l(0)}]$

2: $[x_z, y_z] \leftarrow [x_{z(0)}, y_{z(0)}]$

3: **For** $i = 1$ to ceil(m/4)

$[x_l, y_l] \leftarrow \text{Logistic}(x_l, y_l, r)[x_z, y_z] \leftarrow \text{ZCM}(x_z, y_z, v, \varepsilon, \tau)$

$Vec(4 \times i) = round(abs(10^{14} \times x_z \times x_l \times y_l)) \bmod 256.$

$Vec(4 \times i + 1) = round(abs(10^{14} \times x_l \times x_z \times y_z)) \bmod 256.$

$Vec(4 \times i + 2) = round(abs(10^{14} \times y_z \times x_l \times y_l)) \bmod 256.$

$Vec(4 \times i + 3) = round(abs(10^{14} \times y_l \times x_z \times y_z)) \bmod 256.$

End

Output: *Vec*

Algorithm 2 The generation of encryption keys.

Input: $x_{l(0)}, y_{l(0)}, v, \varepsilon, \tau, x_{z(0)}, y_{z(0)}, r, K_{initial}, I(Plain\ image).$

1: $[h, w, e] \leftarrow size\ (I)$

2: m=max(max $(10 + h, 10 + w \times e), 1034)$

3: Vec $\leftarrow PRNG(x_{l(0)}, y_{l(0)}, v, \varepsilon, \tau, x_{z(0)}, y_{z(0)}, r, m)$

4: $[\sim, V] \leftarrow$ sort(Vec(11 : h + 10))

5: $[\sim, V'] \leftarrow$ sort(Vec(11 : e × w + 10))

6: K ← reshape(Vec(11 : 1034), 32, 32)

7: $\alpha = \sum$Vec mod 256

8: *if* $\alpha = 0$ *then*

$\alpha = \sum$Vec mod 255

End if

9: $K \leftarrow (K_{initial})_{2^8}$

10: $R \leftarrow \alpha \times K$

11: $L \leftarrow \left(R^{-1}\right)_{2^8}$

Output: V, V', α, R, L

معرفی روش

- الگوریتم رمزنگاری
  - مرحله۱: حذف *footnote* های عکس

Algorithm 3 Disruption footnotes.

Input: $I_{R,G,B}$ (*Plain image*).

1: $C_{R,G,B} \leftarrow Noise(I_{R,G,B})$

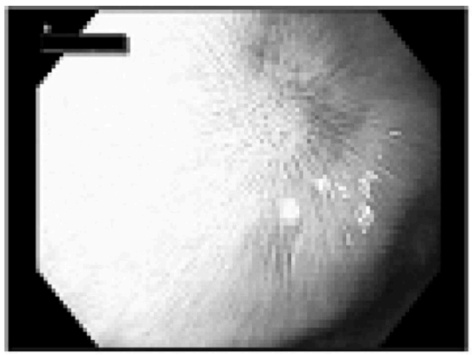
2: $C_{R,G,B}(1,1) = I_{R,G,B}(1,1)$;

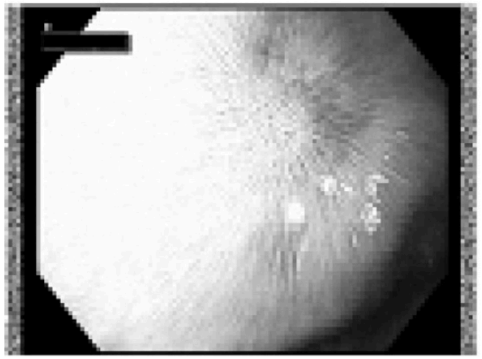
3: $C_{R,G,B}(end, end) = I_{R,G,B}(end, end)$;

4: $C_1 \leftarrow [C_R C_G C_B]$

Output: C_1

افزودن نویز با تولید اعداد تصادفی و ترکیب آن‌ها با پیکسل‌ها به وسیله عملگر XOR





معرفی روش

- الگوریتم رمزنگاری (ادامه)
  - مرحله ۲: شیفت دادن ماتریس خروجی قسمت قبل به وسیله بردارهای V و V'
  - مرحله ۳: شیفت دادن هر زیربلاک ماتریس خروجی قسمت قبل به وسیله ماتریس R
  - مرحله ۴: اجرای الگوریتم فیلدهای گالویس بر روی هر بلاک ۳۲×۳۲ ماتریس خروجی قسمت قبل به صورت: $C_4 \leftarrow (L \,.\, B_{C_3})_{2^8}$

$$GF(p^n) = [f(0) \bmod p, f(1) \bmod p, \ldots, f(p^n - 1) \bmod p, f(p^n) \bmod p]$$

for $f(x) = \sum_{i=0}^{n} x^i k_i$, i.e. an n-order polynomial with constants K.

  - مرحله ۵: تکرار مرحله ۲
  - مرحله ۶: تکرار مرحله ۶

معرفی روش

- الگوریتم رمزنگاری (ادامه)
  - مرحله ۷: $C_7 \leftarrow (B_{C_6} . K)_{2^8}$
  - مرحله ۸: تکرار مرحله ۲
  - مرحله ۹: فرم‌دهی ماتریس قسمت قبل به ۳ ماتریس $C_R C_G C_B$

- خروجی ماتریس مرحله نهم، یک عکس تصادفی و غیرقابل تشخیص خواهد بود. بنابراین، به دست آوردن هر گونه اطلاعات بیماران بدون داشتن کلیدهای مخفی، ممکن نیست و در نتیجه، حریم خصوصی کاربر در این حالت، تضمین می‌شود

معرفی روش

- الگوریتم رمزگشایی

☑ سیستم رمزنگاری معرفی شده، *lossless* است، یعنی می‌توان بدون آنکه ظاهر بصری آن به هم بخورد، آن را بازسازی کرد

- مرحله صفر: خواندن عکس رمز شده و اعمال الگوریتم‌های ۱ و ۲ بر روی آن
- مرحله۱: تغییر ۳ ماتریس خروجی به یک ماتریس واحد
- مرحله۲: اعمال برعکس مرحله دوم الگوریتم رمزنگاری، در این حالت، پیکسل‌ها ریکاور می‌شوند
- مرحله ۳: اعمال الگوریتم فیلدهای گالویس بر روی هر بلاک ۳۲×۳۲ ماتریس خروجی قسمت قبل به صورت: $D_3 \leftarrow (B_{D_2} \,.\, L)_{2^8}$
- مرحله ۴: اجرای الگوریتم مرحله سوم رمزنگاری به کمک متغیر R

معرفی روش

- الگوریتم رمزگشایی (ادامه)
  - مرحله ۵: تکرار مرحله دوم
  - مرحله ۶: اجرای مجدد الگوریتم فیلدهای گالویس به صورت: $D_6 \leftarrow (K \,.\, B_{D_5})_{2^8}$
  - مرحله ۷: تکرار مرحله چهارم
  - مرحله ۸: تکرار مرحله دوم
  - مرحله ۹: اجرای الگوریتم زیر:

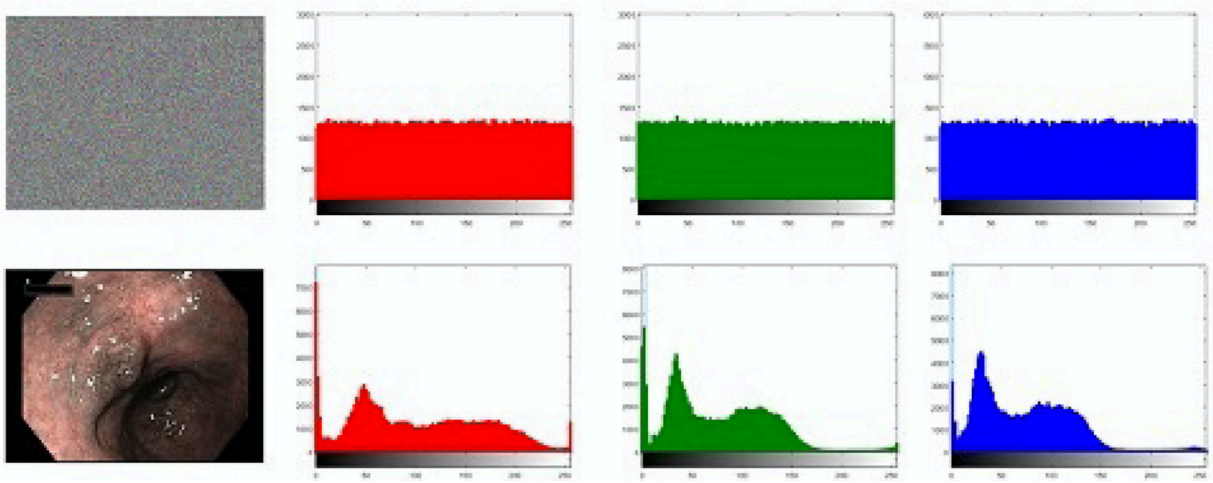
Algorithm 4 Recover footnotes blocks.

Input: D_8.
1: $[D_R\, D_G\, D_B] \leftarrow D_8$
2: $Ones \leftarrow matrix\ of\ ones\,[h,\ 21]$
3: $D_{R,G,B}(1:h,\ 1:21) \leftarrow Ones \times D_{R,G,B}(1,\ 1)$
4: $D_{R,G,B}(1:h,\ end-20:-1:end) \leftarrow Ones \times D_{R,G,B}(end,\ end)$
Output: $D_{R,G,B}$

خروجی الگوریتم، عکس D است که یک عکس رمزگشایی شده است

آنالیز امنیتی

- آنالیز هیستوگرام
  - ⭐ توزیع داده‌های عکس‌های اصلی و رمز شده بررسی شده است
  - ⭐ هیستوگرام، پیکسل‌های عکس را به صورت تعداد پیکسل‌ها در هر رنگ را به تصویر کشیده است
  - ☑ مقادیر پیکسل‌های عکس رمز شده یک توزیع یکنواخت و کاملاً متفاوت دارد



آنالیز امنیتی

- آنالیز آنتروپی اطلاعات

  - آنتروپی عکس‌های رمز شده جهت بررسی میزان تصادفی بودن، محاسبه شده است
  - از فرمول تست آنتروپی شانون استفاده شده است: $E(C) = -\sum_{i=1}^{n} P(c_i) \log_2 P(c_i)$
  - ایده‌آل‌ترین امتیاز عددی تست آنتروپی شانون، ۸ است

Table 1
The local Shannon entropy tests.

Component	Keyframe	Ciphered
R	7.2657	7.9995
G	7.0346	7.9994
B	6.9276	7.9994

Table 2
The local Shannon entropy comparison tests.

Algorithm	Proposed	Yao et al. [20]	Wei et al. [19]
Image size	[640,480,3]	[512,512,3]	[256,256,3]
Entropy(Red)	7.9995	7.9993	7.9971
Entropy(Green)	7.9994	7.9993	7.9969
Entropy(Blue)	7.9994	7.9992	7.9962

آنالیز امنیتی

- آنالیز ضریب همبستگی

  - تست ضریب همبستگی، میزان توانایی سیستم رمزنگاری برای از بین بردن ارتباط بین پیکسل‌های همسایه را نشان می‌دهد
  - ایده‌آل‌ترین حالت آن است که میزان این عدد صفر باشد (ارتباطی نداشته باشند)

Table 3
The correlation coefficient analysis.

Component	Keyframe			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
R	0.9937	0.9901	0.9854	0.0012	−0.0027	0.0002
G	0.9909	0.9834	0.9877	−0.0007	0.0021	−0.0010
B	0.9931	0.9824	0.9901	0.0015	−0.0010	0.0007

آنالیز امنیتی

- آنالیز آزمون‌های $NPCR$ و $UACI$

  - آزمون $NPCR$ به تعداد تغییر پیکسل‌ها هنگام تغییر یک پیکسل از عکس ساده اشاره دارد
  - آزمون $UACI$ به میانگین شدت تغییر بین تصویر اصلی و رمز شده، اشاره دارد
  - ایده‌آل‌ترین مقدار آزمون اول، ۹۹.۶۱ درصد و آزمون دوم، ۳۳.۴۴ درصد است

$$NPCR(C_1, C_2) = \sum_{i,j} \frac{S(i,j)}{D} \times 100\ \%$$

$$UACI(C_1, C_2) = \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255 \times D} \times 100\ \%$$

$$S(i,j) = \begin{cases} 0, & IF\ C_1(i,j) = C_2(i,j) \\ 1, & Elsewise. \end{cases}$$

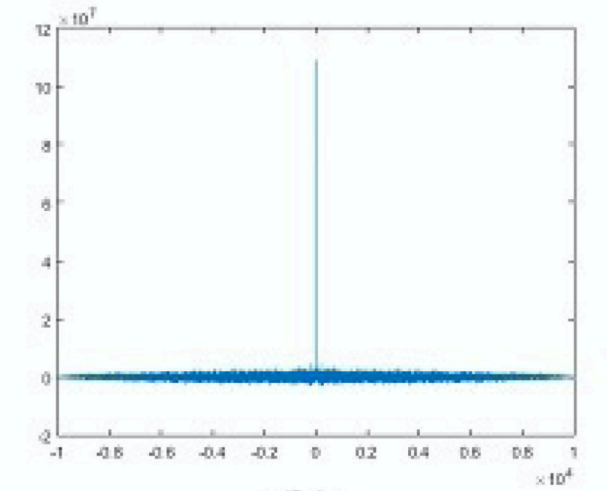
Table 4
Results of NPCR and UACI test.

	0.05-level	0.01-level	0.001-level
Expected value NPCR	>99.5693%	>99.5527%	>99.5341%
Expected value UACI	33.2824-33.6447%	33.2255-33.7016%	33.1594-33.7677%
$NPCR_{(R,G,B)}(99.6098)$	Pass	Pass	Pass
$UACI_{(R,G,B)}(33.4658)$	Pass	Pass	Pass

آنالیز امنیتی

- آنالیز تابع مولد شبه اعداد تصادفی

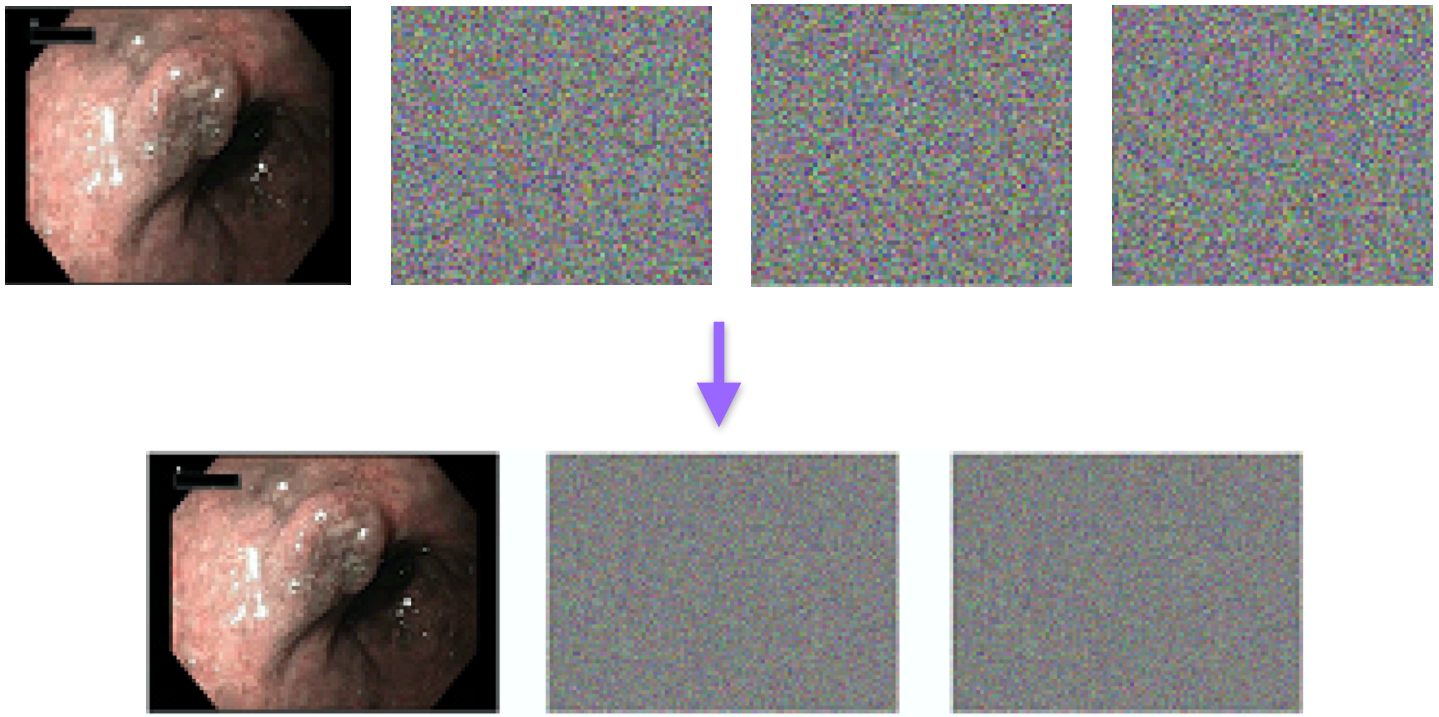
  - ☆ این آزمون برای بررسی میزان شدت وابستگی الگوریتم به کلیدهای مخفی انجام شده است
  - ☆ دو توالی خروجی این الگوریتم با کلیدهای مخفی متفاوت از هم بررسی شده است. میزان تفاوت این دو کلید در حد 10^{-14} است
  - ☆ میزان همبستگی تفاوت این دو توالی در نمودار زیر مشخص است (اکثراً صفر است)



آنالیز امنیتی

- آنالیز میزان حساسیت

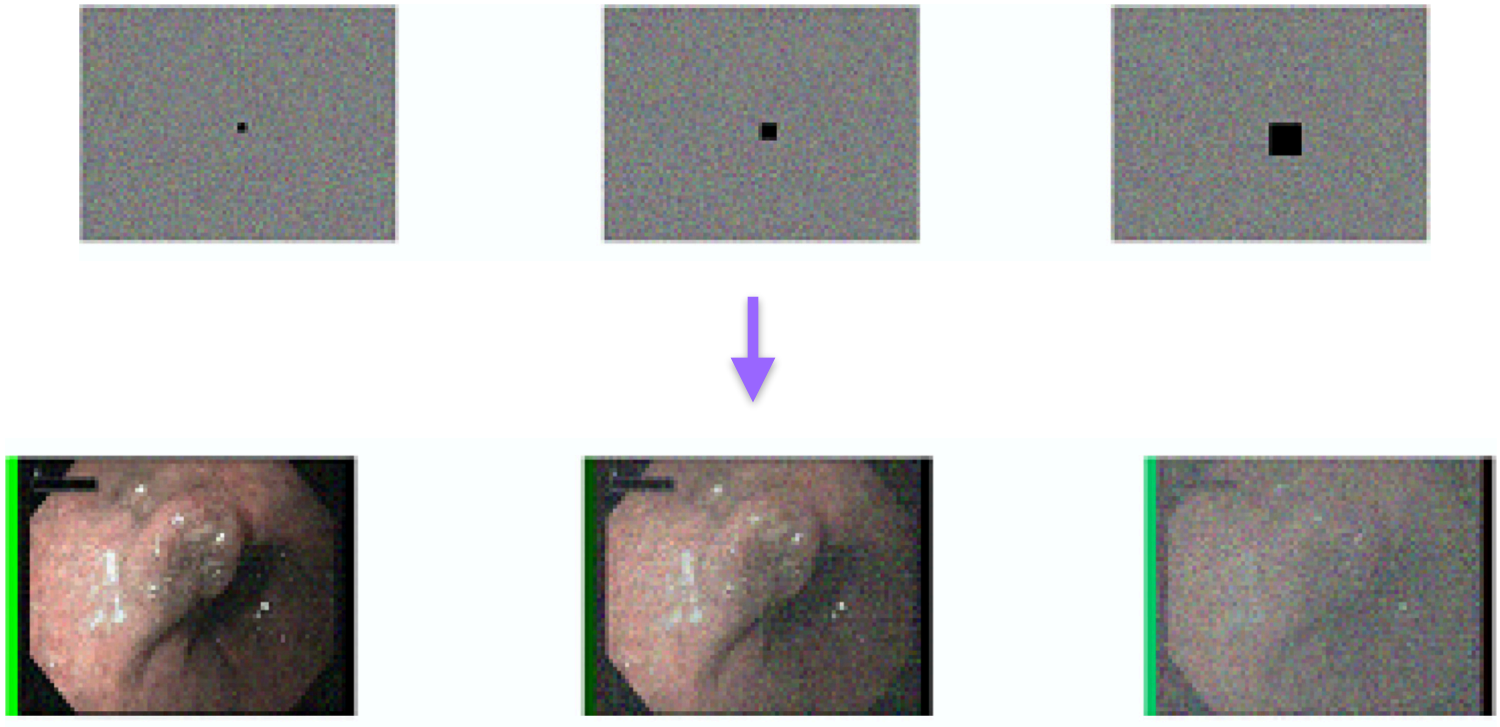
  - از ۳ کلید مخفی استفاده شده است که بسیار تفاوت ناچیزی دارند (10^{-14})



آنالیز امنیتی

- آنالیز میزان مقاومت کیفی عکس

  - در آزمایش انجام شده، تکه‌ای از پیکسل‌های عکس رمز شده، برداشته شده است



آنالیز امنیتی

- آنالیز سرعت رمزنگاری

Table 9
Encryption speed (KB/Sec) comparison.

Algorithm	Encryption
The proposed scheme	970
Belazi et al. [21]	167
Belazi et al. [22]	4.17
Hamza et al. [5]	205
Wu et al. [16]	5.12
Yao et al. [20]	437.75
Zhou et al. [17]	22.5

- مقایسه با پژوهش‌های موجود دیگر

Comparison analysis based on several analysis metrics.

Method	Image size	Key space	Speed analysis	NPCR & UACI analysis		Sensitivity analysis
Proposed	[640,480,3]	2^{372}	0.95/0.96 s	99.609	33.465	Yes
[18]	[1024,1024,1]	2^{624}	2.51/2.51 s	99.617	33.669	Yes
[5]	[256,256,1]	2^{711}	0.32/0.31	99.61	33.50	Yes
[19]	[256,256,3]	2^{233}	–	99.217	33.405	Yes
[16]	[640,480,3]	2^{256}	179.8/180.0 s	99.619	33.477	Yes
[17]	[640,480,3]	2^{256}	40.96/41.08 s	99.606	44.486	Yes

بررسی نقاط قوت و ضعف

- نقاط قوت
  - مناسب برای سیستم‌های بلادرنگ است (سریع است)
  - مقاومت بازسازی (رمزگشایی) تصویر رمزنگاری شده مخدوش شده مطلوب است
  - فضای کلیدی بالایی دارد و در نتیجه، در مقابل حملات، مقاومت بالایی دارد
  - امکان پیاده‌سازی واقعی توسط یک مدار مجتمع مانند یک *FPGA*
- نقاط ضعف
  - نبود مکانیزم کنترل دسترسی

با تشکر از توجه شما