Variant Map System of Random Sequences

Jeffrey Zheng

Abstract Sequences of random variables play a key role in probability theory, stochastic processes, and statistics to analyze dynamic behavior. Speckle patterns have emerged as useful tools to explore space–time variations of random sequences in various measurement applications of comprehensive properties in complex space–time variation events. In this chapter, a variant map system is proposed to analyze statistical properties of random sequences in visual representations. An input 0–1 sequence will be divided into multiple segments and each segment of a fixed length will be transformed into a 2-tuple pair of measures. Five measuring sets are identified and rearranged in a 1D or 2D numerical array as a histogram representing a visual map. These five types of maps consist of two types in 1D format as classical maps and three types in 2D format as variant maps. Properties are analyzed on all five types of maps. A cryptographic sequence of the AES cipher is selected as a sample stream. The five types of visual maps are generated and refined clustering characteristics are organized into four groups on changes of segmented and shifted lengths for visual comparisons on enlarged 2DP maps. Speckle patterns of various distributions are observed. Three variant maps with distinct statistic distributions could be useful to provide new visual tools to explore comprehensive cryptographic sequences on complex nonlinear dynamic behavior in global network environments.

Keywords Variant map · Visual representation · Multiple segment · Statistical probability distribution · Clustering characteristics

This work was supported by the Key Project on Electric Information and Next Generation IT Technology of Yunnan (2018ZI002), NSF of China (61362014), Yunnan Advanced Overseas Scholar Project.

J. Zheng (✉)
Key Laboratory of Quantum Information of Yunnan, Yunnan University, Kunming, China
e-mail: conjugatelogic@yahoo.com

J. Zheng
Key Laboratory of Software Engineering of Yunnan, Yunnan University, Kunming, China

J. Zheng (ed.), *Variant Construction from Theoretical Foundation to Applications*,
https://doi.org/10.1007/978-981-13-2282-2_7

1 Introduction

Associated with network communication and internet technology [1] in global applications, web communication, internet of things, cloud computing, big data, mobile phone, and smart wireless technologies [2] are significantly developed in the last decade and widely adapted over the world market. In the current situation, it is a key issue for cryptographic researchers and applications [3] to use advanced technologies of stream ciphers to protect data security of ultrafast and extra-big data streams in global network environments.

1.1 Pseudo-Random Sequences

1.1.1 From Linear Stream Ciphers

Traditional stream ciphers [4] on LFSR Linear Feedback Shift Register structure (in military cryptography) are used as pseudo-random number generators, due to the ease of implementation from simple hardware, long periods, and uniformly distributed streams. The LFSR stream ciphers are the core in classical stream ciphers through the mathematical theory of algebraic functions for system simulation and analysis.

However, an LFSR is a linear system leading to fairly easy cryptanalysis using the Berlekamp–Massey algorithm. Important LFSR-based stream ciphers use A5/1 & A5/2 in GSM cell phones and E0 in Bluetooth. But the A5/2 cipher has been broken and both A5/1 and E0 have serious weaknesses [5, 6].

1.1.2 From Nonlinear Stream Ciphers

The new generation of stream ciphers [7, 8] are widely used in advanced web communications. Three general methods are applied to improve security weaknesses in LFSR-based stream ciphers:

1. **Nonlinear Functions**: Nonlinear combination of several bits from the LFSR state [9].
2. **Nonlinear Parts**: Nonlinear combination of the output bits of two or more LFSRs or using Evolutionary algorithm for nonlinearity [10].
3. **Clock Control**: Irregular clocking of the LFSR, as in the alternating step generator [11].

With batch, a series of nonlinear algorithms have emerged [12]: nonlinear equivalence [13], evolutionary methods [10], AES cipher [14], RC4 [15], ZUC [9], cellular automata [16], and nonlinear dynamic system [17].

The new generation of stream ciphers are being shifted from the traditional mode: LFSR [4] to various nonlinear modes: NLFSR [18, 19], clock control [11], nonlinear

functions [9] etc., it is essential for ciphers to be integrated and implemented [20] to satisfy security models. However, different from LFSR with well-established linear mathematical theories and simulation tools, it is extremely difficult to use advanced nonlinear mathematical theories, recursive models, descriptive tools, and implementing schemes [17] in nonlinear dynamic environments.

How to evaluate cryptographic sequences generated from the nonlinear stream ciphers is an urgent problem for modern stream ciphers.

1.2 Truly Random Sequences from Hardware Devices and Speckle Patterns

In addition to pseudo-random sequences generated by stream ciphers, high-quality stochastic oscillators of truly random sequences are generated from special hardware devices such as laser photonics [21], nonlinear optics [22], quantum optics [23], quantum noises [24], thermal noise [25], chaos, and fractal nonlinear dynamics [26].

A list of truly random number generators are developed to extract stochastic information from speckle patterns [27], i.e., random bits from turbulence [28] to get random numbers from the speckle positions, generation of random arrays using laser speckle [29], 2D generation of random numbers by multimode fiber speckle [30], Markov speckle for efficient random bit generation [31] and dynamic laser speckle and applications [11].

Since various truly random sequences are created from specific physical models with special principles and uncertain methodologies, it is extremely difficult for cryptographic researchers to make proper measurements explore nonlinear dynamic properties.

1.3 Statistic Testing Packages on Cryptographic Sequences

Randomness has been explored for many years [32] on a series of statistic testing theories and methods. The NIST 800-22 testing package [33] is an effective statistic package on random sequences collecting a set of 16 statistic testing schemes in evaluations of statistic properties on cryptographic sequences. Statistic testing packages are very useful to catch a list of quantitative measurements evaluating randomness properties of cryptographic sequences in wider applications. However, testing schemes in various packages are mainly focused on P-value or a list of static properties of a testing sequence.

Since comprehensive behaviors in nonlinear dynamics may increase computational complexities tragically to involve complicated dynamic properties in the multivariate environment, those dynamic behaviors are completely ignored.

1.4 Gaussian Distribution and Speckle Pattern

Multivariate normal probability distribution models are the most important and powerful tools that are used to test stochastic characteristics of a random data sequence [34] under the framework of probability, stochastic process, and statistics [35] for nonlinear problems. In this kind of measuring models, when the data sequence is sufficiently long, the high-dimensional probability distribution of the sequence [36] is similar to the continuous Gaussian distribution.

A typical projection model is shown in Fig. 1a; the central part shows a Gaussian surface with an unbalanced distribution in a 2D plane distributed as $P(X, Y)$ measures with pseudo-colors and its two 1D projections shown in both horizontal $P(X)$ and vertical $P(Y)$ planes, respectively. In Fig. 1b, a standard Gaussian surface with symmetric shapes is illustrated and the 2D projection of its pseudo-color map is shown in Fig. 1c with an ideal continuous distribution of color on the map. Different from ideally continuous distributions, in Fig. 1d, a real image generated from the Laser speckle phenomena [37] is illustrated as an objective speckle pattern [38] scattered by a laser beam from a plastic surface onto a wall. It is convenient for us to compare different color maps in Fig. 1c, d, respectively.

From these set of figures, the relationship between the projection curve and two 1D Gaussian distributions can be observed in the multivariate normal probability environment. Multivariate Gaussian probability distributions may support classical schemes to analyze complex stochastic data sets of measuring sequences in many applications in continuous conditions. But speckle patterns in Fig. 1d provide intrinsically discrete random patterns that may not be easily simulated by smoothed Gaussian map in Fig. 1c, further exploration on proper simulation and control mechanisms are required.

1.5 Controlling Deterministic Chaos

Controlling deterministic chaos has been an active R&D field in nonlinear dynamics over the past decades. From the pioneering work, significant progress has been achieved in control spatiotemporal chaos [39], plasma device, laser systems [40], chemical reactions, and biological systems both spatial and temporal dependence considered. The complex Ginzburg–Landau equation (CGLE) system [41] describes universal dynamics features near a supercritical Hopf bifurcation. It exhibits defected mediate turbulence or spiral turbulence in a wide parameter region. The control by generating a spiral wave seed has been described [42, 43] to grow into a stable spiral in the CGLE system.

Systematic approaches on simulation of nonlinear behaviors, speckle phenomena in optics [37] and pattern dynamics [44] have been actively explored.

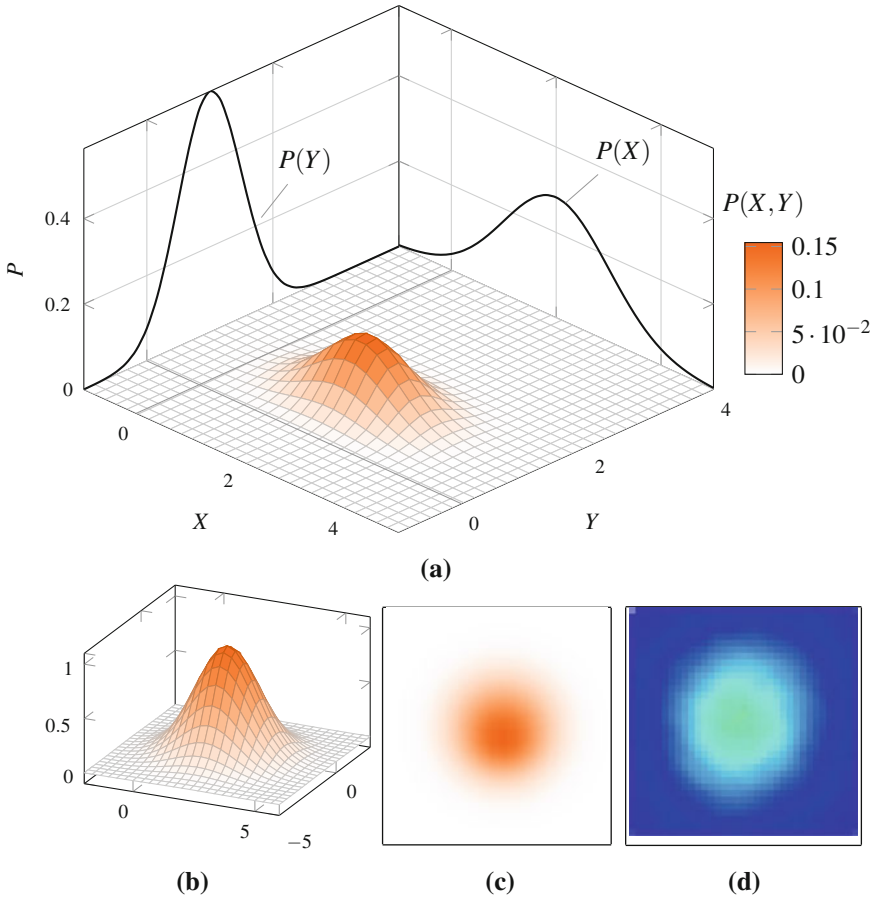


Fig. 1 Multivariate Gaussian Probability Distributions and an objective speckle pattern; **a** Bivariate normal distribution with two probability projections; **b** A symmetric bivariate normal surface with pseudo-colors; **c** A 2D pseudo-color map of the symmetric bivariate normal surface; **d** An objective speckle pattern scattered by a laser beam from a plastic surface onto a wall. [38]

1.6 Poincaré Map

From a measuring viewpoint, spatial variations of a stochastic sequence will be changed by overall macro characteristics showing statistic measurements of distributed patterns [45] in a vector space, so that a random sequence is measured by an analytic space. From an analysis viewpoint, the Poincaré section [46] corresponds to a discrete map proposed by the eminent French scientist Henri Poincaré 100 years ago.

The Poincaré map handles additional information from sequential changes of ordered measurements in the phase space of classical dynamics, nonlinear dynamic systems [47] and chaos.

The mapping mechanism of the Poincaré map may be useful to handle dynamic patterns on cryptographic sequences of stream ciphers. This mapping scheme has been applied to observe the global randomness of cellular automata sequences on 2D maps [48] 20 years ago.

1.7 Variant Framework

Various schemes following the top-down strategy are explored to use multiple measures to partition special phase spaces from a top state set to multiple bottom states via multi-levels of a hierarchy in combinatorial algorithms [49], image analysis and processing for many years.

The conjugate classification [50] is proposed to apply seven measures in a hierarchy to partition the kernels of four regular plane lattices on $n = \{4, 5, 7, 9\}$ cases for 2D binary images. For 1D cellular automata sequences, global random behaviors [48] are visualized in 2D maps.

For n-tuple bit vectors, the variant logic framework [51] was proposed and various applications were explored: 3D visual method on random number sequences [52], variant Pseudo-Random Number Generator PRNG [53, 54], computational simulation on quantum interactions [55, 56], noncoding DNA analysis [57] and bat echolocation [58].

1.8 Proposed Scheme

For the purpose of system characterization based on comprehensive measurements of cryptographic sequences, we propose a variant map system for a 0–1 stochastic sequence with length N. Multiple segments M are divided from the sequence by a given length m. A 2-tuple pair of measures can be extracted from a 0–1 segment that is the number of a single element and the number of 01 patterns in the segment. All paired measures are composed of a sequence of M pairs of measures as an ordered measuring set with M elements.

The pairs of the measuring sequence are directly separated into two independent measuring sequences to keep each parameter in the same order. Applying the pairing scheme of the Poincaré section, one single measuring sequence can be reorganized by two consequent measures as a 2-tuple pair of measures. Two measuring sequences in the Poincaré section and the original pairs of measuring sequence are arranged as the three sequences of 2-tuple measures. So a total of five sequences of distinct measures are constructed including two sequences on single measures and three sequences on 2-tuple measures.

Following this approach, two sets of single measuring sequences are sorted as two 1D numerical arrays as statistical histograms being classic 1D maps and three sets of 2-tuple measuring sequences are sorted as three 2D integer arrays as statistic histograms being three variant maps. Under the controlling operations on the changes of the segment lengths and shift displacements, multiple results of the five measuring sequences are transformed into 1D statistic histograms and 2D pseudo-color maps to show effective speckle patterns from the selected cryptographic sequence under various conditions of the combination on the two controlling parameters.

1.9 Organization of the Chapter

This chapter describes the variant map system in diagrams of the system architecture and the core modules with input/output and processing functions in Sect. 2. In Sect. 3, the relationships among measuring sequences and the five statistical distribution maps are analyzed. In Sect. 4, an AES cipher sequence is selected to form a series of statistical maps based on changes of the two control parameters. From the results of the visual maps in Sect. 4, intuitive analysis and brief comparisons are carried out in Sect. 5. Finally, in Sect. 6, the main results are summarized.

2 Framework of Variant Map System

2.1 Framework

For the variant map system, the block diagrams of the system framework and the core modules of the system are shown in Fig. 2. The framework of the system architecture in Fig. 2a is composed of three core modules: the Shift Segment Measurement SSM, the Measuring Sequence Combination MSC, and the Projective Color Map PCM. The three modules are shown in Fig. 2b–d in more detail, respectively.

2.2 Shift Segment Measurement SSM

The SSM module is shown in Fig. 2b.

Let X be a 0–1 vector with N elements as an input sequence,

$$X = X[0]X[1]\cdots X[I]\cdots X[N-1], 0 \le I < N; X[I] \in \{0, 1\} \tag{1}$$

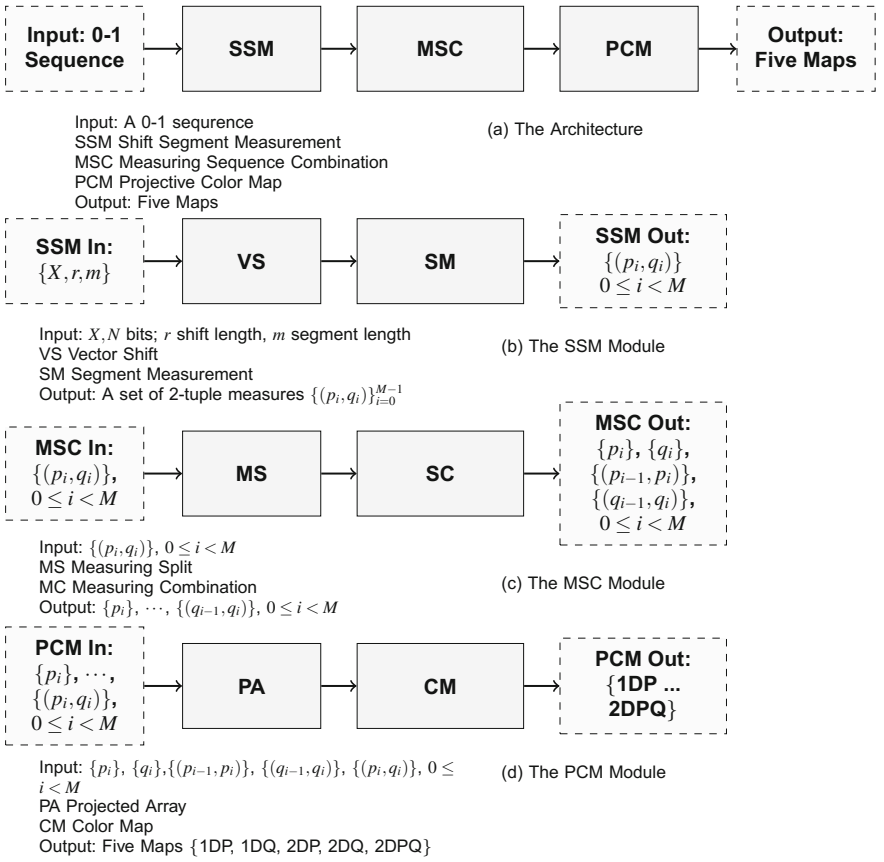


Fig. 2 The framework of the variant map system for cryptographic sequences; **a** The system architecture; **b** The SSM module; **c** The MSC module; **d** The PCM module

The SSM module consists of two processing units: the Vector Shift VS and the Segment Measurement SM, respectively. The two input control parameters: $\{r, m\}$ are defined as shift length r and segment length m.

Let Y be a 0–1 vector with N elements, this vector is generated by the shift operation under the loop displacement condition from the input sequence (i.e., a cyclic shift right + or shift left −)

$$Y = X(r), Y[I] = X[I \pm r], I \pm r(modN), 0 \le I < N; X[I], Y[I] \in \{0, 1\} \quad (2)$$

The shifted vector is inputted into the SM unit for a segmentation process. The input sequence will be divided from a long sequence with N elements into $M = \lfloor N/m \rfloor$ segments as a set of sub-vectors with m elements and each segment

contains m bits. The i-th sub-vector $0 \le i < M$ on the j-th position $0 \le j < m$ is denoted as $Y_{i,j}$.

This sequence of sub-vectors after the segmenting operation forms the following $m \times M$ matrix, m positions for the i-th complete row vector in the sequence correspond to a pair of 2-tuple measures: (p_i, q_i), and incomplete parts of the last sub-vector are ignored.

$$Y = \begin{bmatrix} Y_{0,0} & Y_{0,1} & \cdots & Y_{0,j} & \cdots & Y_{0,m-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ Y_{i,0} & Y_{i,1} & \cdots & Y_{i,j} & \cdots & Y_{i,m-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ Y_{M-1,0} & Y_{M-1,1} & \cdots & Y_{M-1,j} & \cdots & Y_{M-1,m-1} \\ \cdots & & & & & \end{bmatrix} \rightarrow \begin{bmatrix} (p_0, q_0) \\ \vdots \\ (p_i, q_i) \\ \vdots \\ (p_{M-1}, q_{M-1}) \\ \cdots \end{bmatrix} \tag{3}$$
$$= \{(p_i, q_i)\}_{i=0}^{M-1}$$

The pair of 2-tuple measures (p_i, q_i) is determined by the following formula:

$$Y_{i,j} = Y[J] \in \{0, 1\};\ J = i \times m + j,$$
$$0 \le i < M, 0 \le j < m, 0 \le J < m \times M \le N \tag{4}$$

$$p_i = \sum_{j=0}^{m-1} Y_{i,j}, Y_{i,j} \in \{0, 1\}, 0 \le p_i \le m; \tag{5}$$

$$q_i = \sum_{j=0}^{m-1} [(Y_{i,j-1}, Y_{i,j}) == (0, 1)],\ j - 1(mod\ m), 0 \le q_i \le \lfloor m/2 \rfloor; \tag{6}$$

i.e., $X = 0011010010, N = 10, M = 2, m = 5; (p_0 = 2, q_0 = 1); (p_1 = 2, q_1 = 2)$.

The parameter p_i is the number of single elements in the i-th sub-vector, the parameter q_i is the number of 01 pattern overlapped in the i-th sub-vector in a cyclic condition. For any segment $m > 0, 0 \le p_i \le m, 0 \le q_i \le \lfloor m/2 \rfloor$, all segments are transformed from a random sequence with N elements into a measuring sequence with M elements.

The SSM module outputs the ordered pairs of 2-tuple measures $\{p_i, q_i\}_{i=0}^{M-1}$.

2.3 Measuring Sequence Combination MSC

The MSC module is described in Fig. 2c, the module is composed of two units: the Measuring Split MS and the Measuring Combination MC. The MS unit processes the SSM module's output, and splits the measuring sequence with 2-tuple measures

into two independent measuring sequences: $\{p_i\}_{i=0}^{M-1}$, $\{q_i\}_{i=0}^{M-1}$ to keep the original measuring number invariant.

Recombining each single measuring sequence by overlapping consequent elements as a pair, the MC unit will form two independent measuring sequences organized in 2-tuple measures: $\{p_i\}_{i=0}^{M-1} \rightarrow \{(p_{i-1}, p_i)\}_{i=0}^{M-1}$ and $\{q_i\}_{i=0}^{M-1} \rightarrow \{(q_{i-1}, q_i)\}_{i=0}^{M-1}, i-1(mod\ M)$ to provide appropriate sequences for subsequent processing modules.

The MSC module produces the following four measure sequences: $\{p_i\}_{i=0}^{M-1}$, $\{q_i\}_{i=0}^{M-1}$, $\{(p_{i-1}, p_i)\}_{i=0}^{M-1}$, $\{(q_{i-1}, q_i)\}_{i=0)}^{M-1}$, respectively.

2.4 Projective Color Map PCM

The PCM module consists of two units: PA,CM. For five measuring sequences, 1D and 2D measures will be processed separately.

The PA unit processes relevant measuring sequences to transform them into integer arrays and the CM unit will visualize these on either normalized histograms (1D measures) or color maps (2D measures), respectively.

2.4.1 1D Measures

The 1D measures involve two measuring sequences: $\{p_i\}_{i=0}^{M-1}, \{q_i\}_{i=0}^{M-1}$. Let $P[m+1]$, $Q[\lfloor m/2 \rfloor + 1]$ and $NP[m+1]$, $NQ[\lfloor m/2 \rfloor + 1]$ be two 1D (integer, float) arrays to represent the corresponding elements, which are defined in the following.

2.4.2 1DP Map

The 1DP statistic histogram: for a sequence $\{p_i\}_{i=0}^{M-1}$, NP, P are two arrays (float, integer) with $(m+1)$ elements. The j-th elements $NP[j]$, $P[j]$, $0 \leq j \leq m$, can be obtained from the following procedure:

$$\begin{aligned} \text{Initialization: } & \forall NP[j] = 0.0,\ P[j] = 0,\ 0 \leq j \leq m; \\ \text{Calculation: } & for(i = 0; i < M; i++)\{P[p_i]++;\} \\ \text{Normalization: } & for(j = 0; j \leq m; j++)\{NP[j] = P[j]/M;\} \end{aligned}$$

In the 1DP map, the PA unit corresponds to Initialization and Calculation; the CM unit handles Normalization.

2.4.3 1DQ Map

The 1DQ statistic histogram: for a sequence $\{q_i\}_{i=0}^{M-1}$, NQ, Q are two arrays (float, integer) with $(\lfloor m/2 \rfloor + 1)$ elements. The j-th elements $NQ[j]$, $Q[j]$, $0 \le j \le \lfloor m/2 \rfloor$, can be obtained from the following procedure:

$$\begin{aligned} \text{Initialization: } & \forall NQ[j] = 0.0, Q[j] = 0, 0 \le j \le \lfloor m/2 \rfloor; \\ \text{Calculation: } & for(i = 0; i < M; i++)\{Q[q_i]++;\} \\ \text{Normalization: } & for(j = 0; j \le \lfloor m/2 \rfloor; j++)\{NQ[j] = Q[j]/M;\} \end{aligned}$$

Using P, NP, Q, NQ arrays, it is possible to generate the corresponding 1D statistical histograms as 1D maps.

In the 1DQ map, the PA unit corresponds to Initialization and Calculation; the CM unit handles Normalization.

2.4.4 2D Measures

The 2D measures specially process three measuring sequences: $\{(p_{i-1}, p_i)\}_{i=0}^{M-1}$, $\{(q_{i-1}, q_i)\}_{i=0}^{M-1}$, $\{(p_i, q_i)\}_{i=0}^{M-1}$. Let $P[m+1 : m+1]$, $Q[\lfloor m/2 \rfloor + 1 : \lfloor m/2 \rfloor + 1]$, $PQ[m+1 : \lfloor m/2 \rfloor + 1]$ be three 2D integer arrays to represent the corresponding elements, which are defined in the following.

2.4.5 2DP Map

2DP statistic histogram: for a sequence$\{(p_{i-1}, p_i)\}_{i=0}^{M-1}$, P is a 2D integer array with $(m+1)^2$ elements. The i, j-th elements $P[i, j]$, $0 \le i, j \le m$, can be obtained from the following procedure:

$$\begin{aligned} \text{Initialization: } & \forall P[i, j] = 0, 0 \le i, j \le m; \\ \text{Calculation: } & P[p_{M-1}, p_0]++; \\ & for(i = 1; i < M; i++)\{P[p_{i-1}, p_i]++;\} \\ \text{Pseudo-color: } & \text{Matching proper color } \forall P[i, j], 0 \le i, j \le m \end{aligned}$$

In the 2DP map, the PA unit corresponds to Initialization and Calculation; the CM unit handles pseudo-color.

2.4.6 2DQ Map

2DQ statistic histogram: for a sequence $\{(q_{i-1}, q_i)\}_{i=0}^{M-1}$, Q is a 2D integer array with $(\lfloor m/2 \rfloor + 1)^2$ elements. The i, j-th element $Q[i, j]$, $0 \le i, j \le \lfloor m/2 \rfloor$, can be obtained from the following procedure:

$$\begin{aligned}
\text{Initialization: } & \forall Q[i,j]=0, 0\le i,j\le \lfloor m/2\rfloor;\\
\text{Calculation: } & Q[q_{M-1},q_0]++;\\
& for(i=1;i<M;i++)\{Q[q_{i-1},q_i]++;\}\\
\text{Pseudo-color: } & \text{Matching proper color } \forall Q[i,j], 0\le i,j\le \lfloor m/2\rfloor
\end{aligned}$$

In the 2DQ map, the PA unit corresponds to Initialization and Calculation; the CM unit handles Pseudo-color.

2.4.7 2DPQ Map

2DPQ statistic histogram: for a sequence $\{(p_i,q_i)\}_{i=0}^{M-1}$, PQ is a 2D integer array with $(m+1)\times(\lfloor m/2\rfloor+1)$ elements. The i,j-th elements $PQ[i,j], 0\le i\le m$, $0\le j\le\lfloor m/2\rfloor$, can be obtained from the following procedure:

$$\begin{aligned}
\text{Initialization: } & \forall PQ[i,j]=0, 0\le i\le m, 0\le j\le\lfloor m/2\rfloor;\\
\text{Calculation: } & for(i=0;i<M;i++)\{PQ[p_i,q_i]++;\}\\
\text{Pseudo-color: } & \text{Matching proper color } \forall PQ[i,j], 0\le i\le m, 0\le j\le\lfloor m/2\rfloor
\end{aligned}$$

In the 2DPQ map, the PA unit corresponds to Initialization and Calculation; the CM unit handles Pseudo-color.

Through the PCM module, five measuring sequences are transformed into two 1D arrays and three 2D arrays with $(m+1)$, $(\lfloor m/2\rfloor+1)$, $(m+1)^2$, $(\lfloor m/2\rfloor+1)^2$ and $(m+1)\times(\lfloor m/2\rfloor+1)$ clusters, respectively.

The final results of the variant map system are five maps: 1DP, 1DQ, 2DP, 2DQ, and 2DPQ as expected statistic distributions of the input 0–1 sequence.

3 Sequence Analysis

3.1 Ideal Condition

From a viewpoint of sequence analysis, it is a classical technology to sort the $\{p_i\}_{i=0}^{M-1}$ measuring sequence as a 1D statistic histogram. When the measuring sequence meets ideal conditions, the 1D statistical distribution is a binomial distribution.

Lemma 1 *For an input 0–1 sequence, if the total number of segments is equal to $M=2^m$, and each segment of m bits appears only once in the sequence, then the 1DP array satisfies the binomial distribution:*

$$P[i]=\binom{m}{i}, 0\le i\le m \tag{7}$$

Corollary 1 *If the input sequence meets the conditions of Lemma 1, then the total number of items in the 1DP array is equal to*

$$\sum_{i=0}^{m} P[i] = 2^m = M \tag{8}$$

Lemma 2 *If the input sequence meets the conditions of Lemma 1, then the 1DQ array satisfies the following relation:*

$$Q[i] = 2\binom{m}{2i}, 0 \le i \le \lfloor m/2 \rfloor \tag{9}$$

Corollary 2 *If the input sequence meets the conditions of Lemma 1, then the total number of items in the 1DQ array is equal to*

$$\sum_{i=0}^{m/2} Q[i] = 2^m = M \tag{10}$$

3.2 General Condition

Theorem 1 *For any 0–1 sequence with N elements, a 2DP array has two projections in both vertical and horizontal directions and they are corresponding to the 1DP array.*

Proof A 2DP array is generated from a measuring sequence $\{(p_{i-1}, p_i)\}_{i=0}^{M-1}$ and the 2DP array is $\{P[i, j]\}_{i=0}^{m}{}_{j=0}^{m}$, from both directions $P[i] = \sum_{j=0}^{m} P[i, j]$, $0 \le i \le m$; $P[j] = \sum_{i=0}^{m} P[i, j], 0 \le j \le m$; so $\{P[i]\}_{i=0}^{m} = \{P[j]\}_{j=0}^{m}$. Both projections are the same 1DP array.

Corollary 3 *For an arbitrary input sequence, the total number of items in the 2DP array is equal to*

$$\sum_{i=0}^{m}\sum_{j=0}^{m} P[i, j] = \sum_{i=0}^{m} P[i] = M \tag{11}$$

Theorem 2 *For any 0–1 sequence with N elements, a 2DQ projection in both directions is the 1DQ array.*

Proof A 2DQ array is generated from a measuring sequence $\{q_{i-1}, q_i\}_{i=0}^{M-1}$ and the 2DQ array is $\{Q[i, j]\}_{i=0}^{\lfloor m/2 \rfloor}{}_{j=0}^{\lfloor m/2 \rfloor}$, from both directions $Q[i] = \sum_{j=0}^{\lfloor m/2 \rfloor} Q[i, j], 0 \le i \le \lfloor m/2 \rfloor$; $Q[j] = \sum_{i=0}^{m} Q[i, j], 0 \le j \le \lfloor m/2 \rfloor$; so $\{Q[i]\}_{i=0}^{\lfloor m/2 \rfloor} = \{Q[j]\}_{j=0}^{\lfloor m/2 \rfloor}$. Both projections are the same 1DQ array.

Corollary 4 *For an arbitrary input sequence, the total number of items in the 2DQ array is equal to*

$$\sum_{i=0}^{\lfloor m/2 \rfloor} \sum_{j=0}^{\lfloor m/2 \rfloor} Q[i, j] = \sum_{i=0}^{\lfloor m/2 \rfloor} Q[i] = M \tag{12}$$

Theorem 3 *For any 0–1 sequence with N elements, a 2DPQ projection in two directions is corresponding to either a 1DP array or a 1DQ array, respectively.*

Proof A 2DPQ array is generated from a measuring sequence $\{p_i, q_i\}_{i=0}^{M-1}$ and the 2DPQ array is $\{PQ[i, j]\}_{i=0}^{m}{}_{j=0}^{\lfloor m/2 \rfloor}$, from two directions $P[i] = \sum_{j=0}^{\lfloor m/2 \rfloor} PQ[i, j]$, $0 \le i \le m$; $Q[j] = \sum_{i=0}^{m} PQ[i, j]$, $0 \le j \le \lfloor m/2 \rfloor$. So the two projections are corresponding to either a 1DP or a 1DQ array.

Corollary 5 *For an arbitrary 0–1 input sequence, the total number of items in the 2DPQ array is equal to*

$$\sum_{i=0}^{m} \sum_{j=0}^{\lfloor m/2 \rfloor} PQ[i, j] = M = \sum_{i=0}^{m} P[i] = \sum_{j=0}^{\lfloor m/2 \rfloor} Q[j] \tag{13}$$

Corollary 6 *For an arbitrary input sequence, five measuring sequences are corresponding to two 1D and three 2D arrays. Let $|G|$ denote the number of associated possible clusters in G. If $m > 3$, then $|2DP| > |2DPQ| > |2DQ| > |1DP| > |1DQ|$ is satisfied.*

Proof Five arrays: (2DP,2DPQ, 2DQ,1DP,1DQ) contain $\{(m+1)^2, (m+1) \times (\lfloor m/2 \rfloor + 1), (\lfloor m/2 \rfloor + 1)^2, (m+1), (\lfloor m/2 \rfloor + 1)\}$ items, respectively. If $m > 3$, then the inequalities are true.

3.3 Brief Discussion

From the listed statement in lemmas, theorems, and corollaries, Lemmas 1 and 2 described an ideal input sequence where each segment is a uniform distribution which appears only once. Under this ideal condition, both 1DP and 1DQ arrays are corresponding to a binomial distribution. Corollaries 1 and 2 have shown that both 1DP and 1DQ arrays meet the number of quantitative characteristics for the ideal input sequence.

Theorems 1 and 2 establish projective conditions on any input sequence. A 2DP or 2DQ array has its 1D projection of two directions on the same array. Theorem 3 claims that for any 2DPQ array, two projections are corresponding to both 1DP and 1DQ arrays, respectively.

Corollaries 3 and 4 treat 2DP and 2DQ arrays, respectively, in the total number of summing conditions on their quantitative characteristics. Corollary 5 is associated

with Theorem 3 on a 2DPQ array to share with other four projections the same quantitative characteristics. In Corollary 5, the total number of each component on five statistic arrays is equal to the total number of segments M, a 2DPQ array occupies a central position in the projection to other arrays. Corollary 6 uses inequalities to show five scales of numbers of items in five arrays to provide the maximal number of items involved in the structure.

From a viewpoint of complex stochastic sequence analysis, this partition mode corresponds to the maximum number of clusters distinguished in the condition of multiple segments. Different from surface analysis based on the multivariate Gaussian probability distribution, variant maps provide only a limited finite number of lattice points that form space-related clusters on the projection position. Under the condition of segments in larger length, the 2DP array has the maximum number of distinct items and can be clearly distinguished among the five arrays to make the most visible map showing the largest refined distribution in details.

4 Sample Maps

Since the ideal distribution may appear merely on specific conditions, it is very difficult to use algebraic formulas to describe measuring sequences on statistical maps of an arbitrary cryptographic sequence. For complicated data sequences, the most effective scheme is using the computational approach directly to generate relevant maps and then to make feasible comparisons. Among the five maps generated from an input 0–1 sequence, more 2DP maps are selected in this section to illustrate a series of changes among segment lengths and shifting lengths for refined details.

In this section, one cryptographic sequence generated from an AES cipher is selected as a sample sequence, and various control parameters will be changed. This sample sequence has a fixed length $N = 10^6$ in one million stochastic bits. Various changes are made on the length m of segment and shift displacement r. Five maps will be applied to show their special statistical distributions.

4.1 Dramatically Changing the Segment Lengths: 1DP, 1DQ, 2DP, 2DQ, and 2DPQ Maps $m = \{8, 16, 128\}, r = 0$

Three groups of Figs. 3, 4, and 5 are involved in comparison based on the five maps.

In Fig. 3, nine maps from both 1DQ and 2DQ forms are selected in $m = \{8, 16, 128\}, r = 0$ condition; (a)–(c) showing three 1DQ maps with different segments; (d)–(f) showing 2DQ maps in normal sizes and (g)–(i) being the same 2DQ maps with enlarged sizes.

In Fig. 4, 12 maps from 1DP, 2DPQ, and 1DQ forms are selected in $m = \{8, 16, 128\}, r = 0$ condition; (a)–(c) showing three 1DQ maps with differ-

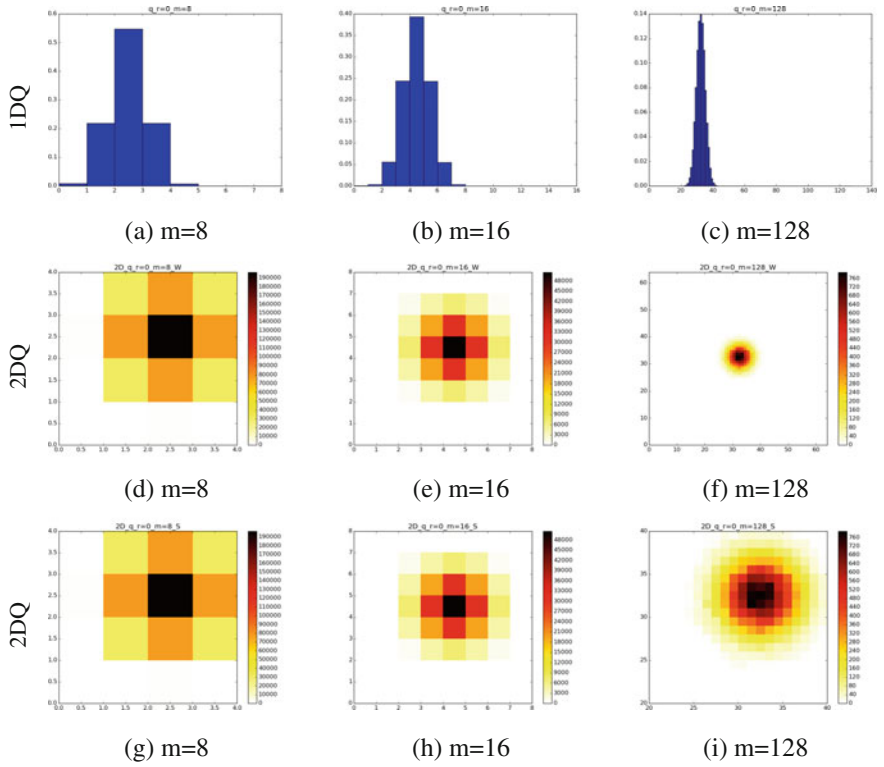


Fig. 3 1DQ and 2DQ maps on $m = \{8, 16, 128\}$, $r = 0$; **a–c** 1DQ maps; **d–f** 2DQ Regular maps; **g–i** 2DQ Enlarged maps

ent segments; (d)–(f) showing 2DPQ maps in normal sizes; (g)–(i) being the same 2DPQ maps with enlarged sizes and (j)–(l) illustrating 1DQ maps for convenient comparison.

In Fig. 5, nine maps from both 1DP and 2DP forms are selected in $m = \{8, 16, 128\}$, $r = 0$ condition; (a)–(c) showing three 1DP maps with different segments; (d)–(f) showing 2DP maps in normal sizes and (g)–(i) being the same 2DP maps with enlarged sizes.

4.2 Small Changes in Segment Lengths: 2DP Maps; Variation Series in Lengths of Segments $m = \{125, 126, 127\}$, $r = 0$

Two groups of maps are compared in Fig. 6 based on slightly changing segment lengths.

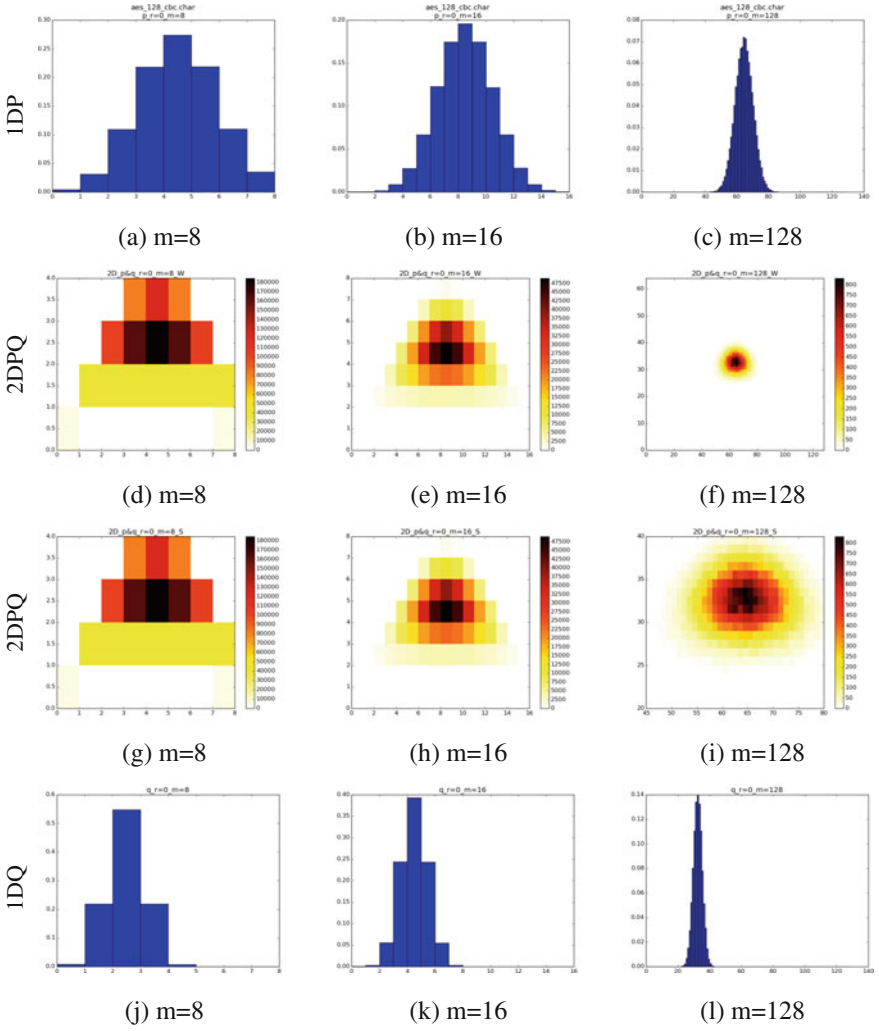
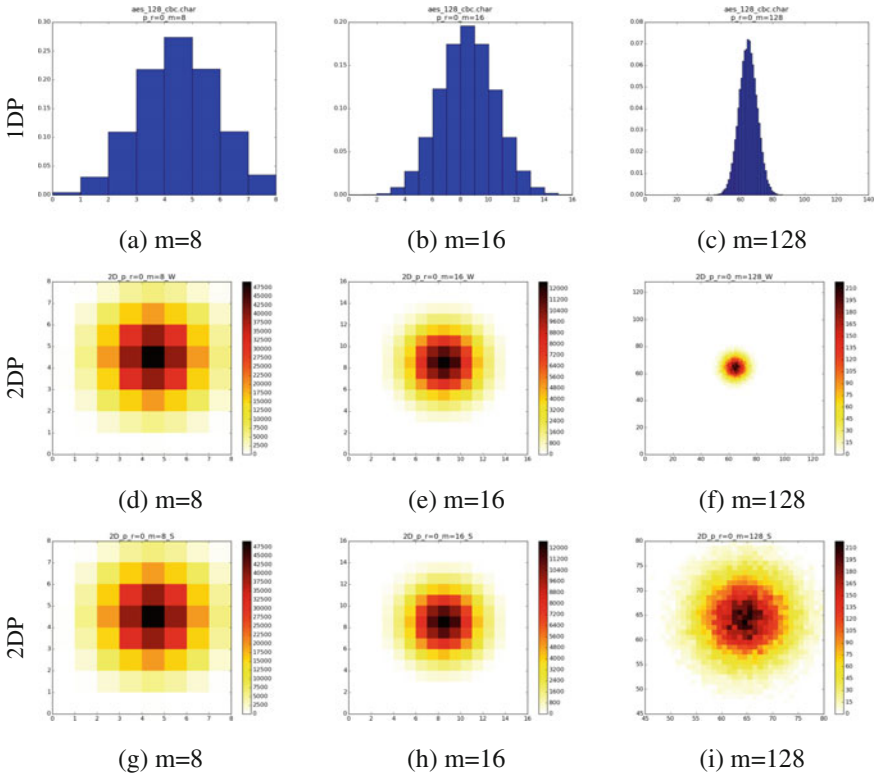


Fig. 4 1DP, 2DPQ, and 1DQ maps on $m = \{8, 16, 128\}$, $r = 0$; **a**–**c** 1DP maps; **d**–**f** 2DPQ Regular maps; **g**–**i** 2DPQ Enlarged maps; **j**–**l** 1DQ maps

In Fig. 6, nine maps from both 1DP and 2DP forms are selected in $m = \{125, 126, 127\}$, $r = 0$ condition; (a)–(c) showing three 1DP maps with different segments; (d)–(f) being 2DP maps in normal sizes and (g)–(i) showing the same 2DP maps with enlarged sizes.



(a) m=8 (b) m=16 (c) m=128

(d) m=8 (e) m=16 (f) m=128

(g) m=8 (h) m=16 (i) m=128

Fig. 5 1DP and 2DP maps on $m = \{8, 16, 128\}$, $r = 0$; **a**-**c** 1DP maps; **d**–**f** 2DP Regular maps; **g**–**i** 2DP Enlarged maps

4.3 Changing the Lengths of Shift Displacement: 2DP Maps Change on Displacement Series $m = 128$, $r = \{1, 2, 8\}$

Two groups of maps are compared in Fig. 7 under changing shift lengths.

In Fig. 7, nine maps from both 1DP and 2DP forms are selected in $m = 128$, $r = \{1, 2, 8\}$ condition; (a)–(c) showing three 1DP maps with different segments; (d)–(f) being 2DP maps in normal sizes and (g)–(i) showing the same 2DP maps with enlarged sizes.

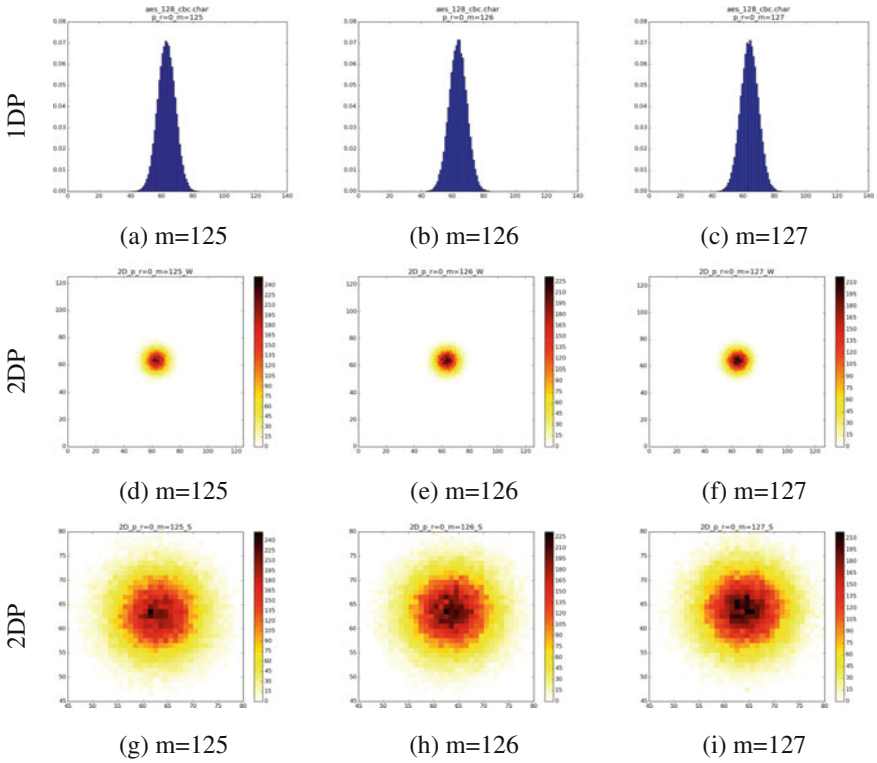


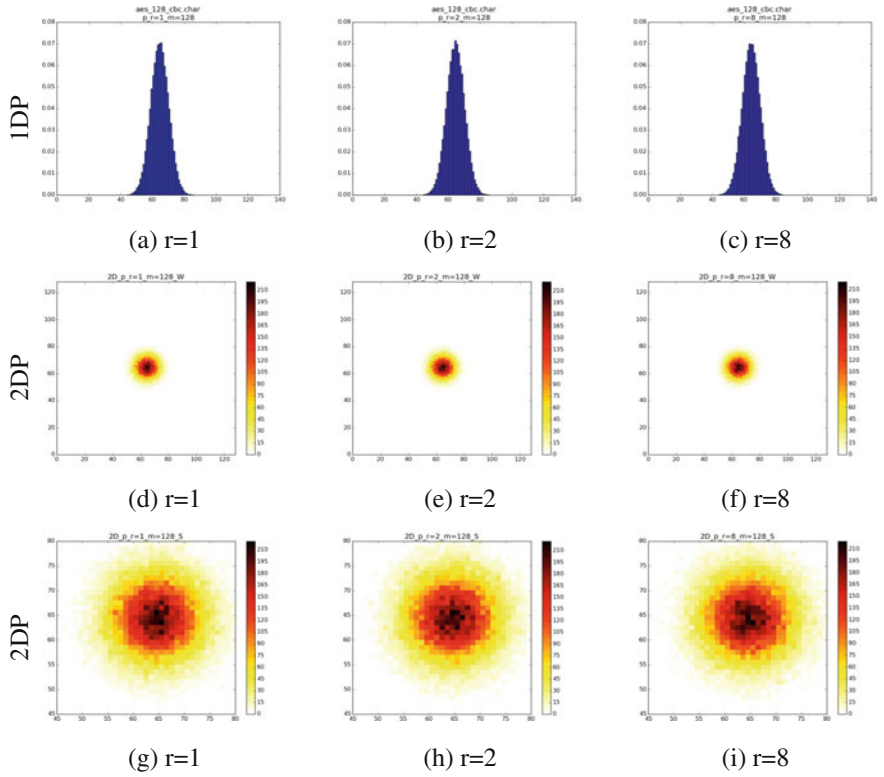
Fig. 6 1DP and 2DP maps on $m = \{125, 126, 127\}$, $r = 0$; **a**–**c** 1DP maps; **d**–**f** 2DP Regular maps; **g**–**i** 2DP Enlarged maps

4.4 Enlarged Maps: 2DP Maps on $m = \{125, 127, 128\}$, $r = \{0, 8\}$

1DP maps are selected in both Figs. 8 and 9 on enlarged forms.

In Fig. 8, four maps from the 2DP form are selected in $m = \{125, 127, 128\}$, $r = \{0, 8\}$ condition; (a) $r = 0$, $m = 125$; (b) $r = 0$, $m = 127$; (c) $r = 0$, $m = 128$, and (d) $r = 8$, $m = 128$. Four maps are showing the same 2DP maps on enlarged sizes.

In Fig. 9a and b, two maps of speckle patterns are selected from two distinct resources for comparison. (a) a larger map from the 2DP form is generated in $m = 128$, $r = 0$ condition; (b) a larger map of Fig. 1d is illustrated for a laser beam reflected from a plastic surface onto a wall. It is convenient for readers to observe the two speckle pattern maps in refined details.



(a) r=1 (b) r=2 (c) r=8

(d) r=1 (e) r=2 (f) r=8

(g) r=1 (h) r=2 (i) r=8

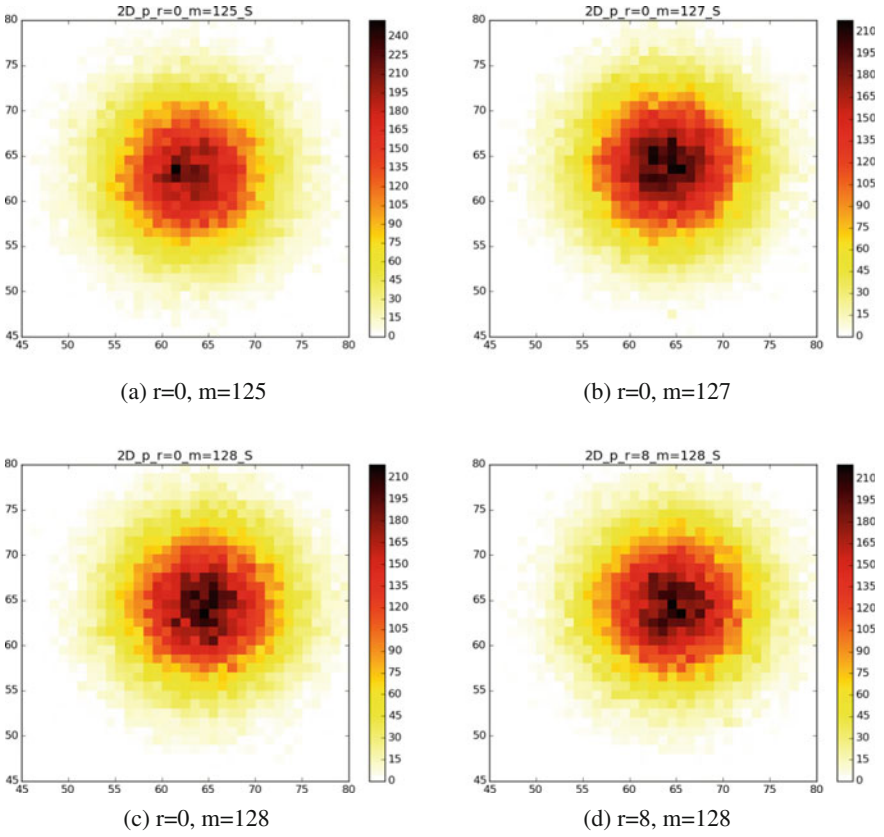
Fig. 7 1DP and 2DP maps on $m = 128$, $r = \{1, 2, 8\}$; **a–c** 1DP maps; **d–f** 2DP Regular maps; **g–i** 2DP Enlarged maps

5 Result Analysis

5.1 Figures 3, 4 and 5

In Figs. 3, 4, and 5, six maps are listed on both 1DP (Figs. 4 and 5a–c) and 1DQ (Figs. 3a–c and 4j–l) forms, their distributions are generally corresponding to binomial coefficients. Under the changes of different lengths on segments, 1D maps are showing distributions of binomial patterns in the symmetric bell curves with the maximal value on the middle area.

From Figs. 3 and 5, six 2DQ maps (Fig. 3d–i) and six 2DP maps (Fig. 5d–i) are listed, when $m = \{8, 16\}$, significant regular distributions along both horizontal and vertical directions (Figs. 3d–h and 5d–h) appear as symmetric patterns. The central cluster is collected the largest number of measures located on the center point of relevant maps. But checking maps in Figs. 3f–i and 5f–i, regular patterns with the central symmetry are severely destroyed when the length of segments is increased to



(a) r=0, m=125 (b) r=0, m=127

(c) r=0, m=128 (d) r=8, m=128

Fig. 8 2DP larger maps on $m = \{125, 127, 128\}, r = \{0, 8\}$; **a** $r = 0, m = 125$ map; **b** $r = 0, m = 127$ map; **c** $r = 0, m = 128$ map; **d** $r = 8, m = 128$ map

$m = 128$. Regarding the two maps in Figs. 3f and 5f, both maps show circular disks with the central position at the highest number of collected measures. However, the two enlarged maps in Figs. 3i and 5i clearly show that significant speckle patterns are visualized around the central areas with stochastic higher numbers of measures. By comparing the two maps in Figs. 3i and 5i, Figure 5i provides much more visible asymmetry than Fig. 3i.

Because a 2DQ map covers only a quarter of a 2DP map, the damaging ratio of its symmetric properties appears much weaker than on the 2DP map. Applying a sufficiently larger segment length, central areas are observed with random speckle patterns and visible symmetric properties significantly damaged.

In general, it is feasible for a 2DP map to observe its middle areas in an approximately rotational symmetry in small sizes. But when the segment length is big enough, significant speckle patterns emerge in the central area with stronger stochastic properties.

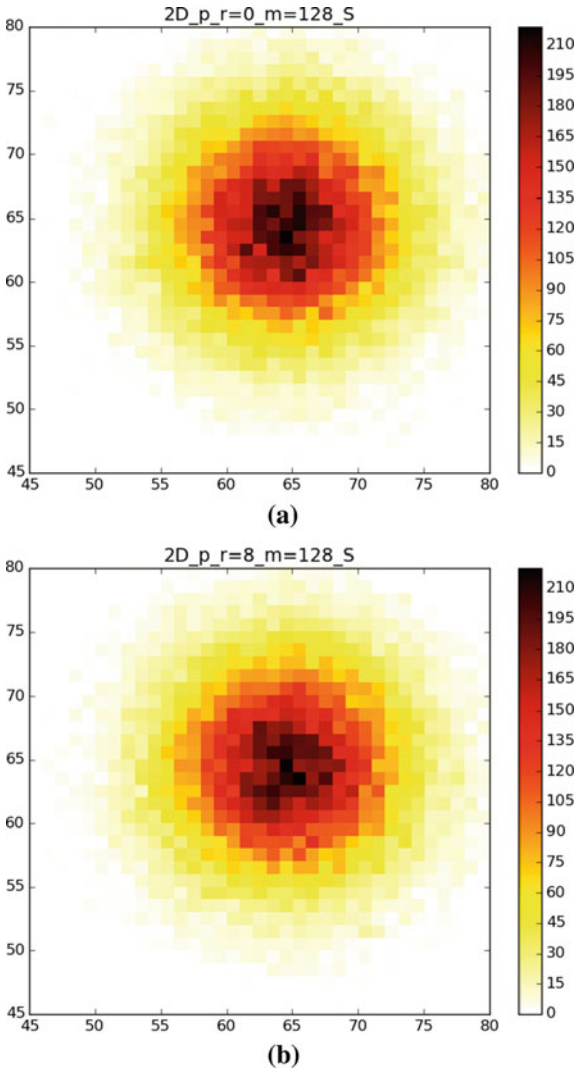


Fig. 9 Speckle patterns in enlarged maps of the 2DP form; **a** $m = 128, r = 0$; **b** $m = 128, r = 8$

In the 2DPQ maps of Fig. 4d–i, when $m = \{8, 16\}$, there appears a single central point as a key cluster to collect the maximal number with visible symmetrical patterns on the horizontal direction, but without symmetrical pattern on the vertical direction in Fig. 4d–h. However, when $m = 128$, the 2DPQ map of Fig. 4f appears as an irregular disk with higher values in the central area.

From the 2DPQ map of Fig. 4i, the enlarged map shows that stochastic speckle patterns appear in the central area with better horizontal symmetry than vertical direction with significantly damaged details.

5.2 *Figure 6*

In Fig. 6a–i, the nine maps are listed to show small changes on lengths of segments $m = \{126, 127, 128\}$. By checking the three 1DP maps in Fig. 6a–c, three middle areas appear slightly different from the bell shape: (a) left is higher than right; (b) right is higher than left; (c) right is higher than left and the middle one is lower than its nearest neighbors.

The three 2DP maps in (d)–(f) appear significantly as circular disks with an approximate symmetry and higher clusters around central areas. In the three enlarged 2DP maps in (g)–(i), there appear various speckle patterns in central areas.

Comparing the six maps of (a)–(c) and (g)–(i), speckle patterns in the three 2DP maps (g)–(i) are much easier identified than broken curving patterns in the three 1DP maps (a)–(c).

5.3 *Figure 7*

In Fig. 7a–i, the nine maps are listed to analyze changes of the parameters $m = 128, r = \{1, 2, 8\}$. By checking the three 1DP maps in Fig. 7a–c, middle areas of three maps appear slightly different from the regular bell shape: (a) left is lower than middle and middle is equal to right; (b) left and right are lower than middle, and right is higher than left; (c) left-middle-right are equal.

The three 2DP maps in (d)–(f) appear as similar circular disks with an approximate symmetry and higher clusters around central areas. In the three enlarged 2DP maps (g)–(i), there are various speckle patterns distinguishably placed in central areas.

Comparing the six maps of (a)–(c) and (g)–(i), distinguishable speckle patterns in the three 2DP maps (g)–(i) are much easier identified than broken curving patterns in the three 1DP maps (a)–(c).

5.4 *Figures 8–9*

In Fig. 8a–d, four enlarged 2DP maps are listed by using the parameters $m = \{125, 127, 128\}, r = \{0, 8\}$. Three maps (a)–(c) are created with $m = \{125, 127, 128\}$, $r = 0$ and two maps (c)–(d) with $m = 128, r = \{0, 8\}$. Four larger 2DP maps in (a)–(d) show stronger speckle patterns distinguishable in their central areas with significant distributions identified differently from mixed reflection and rotational effects.

In Fig. 9a–b, two enlarged maps of speckle patterns are selected. The map (a) with $m = 128, r = 0$ provides refined details to illustrate stochastic speckle patterns in the central area and the map (b) with $m = 128, r = 8$ has the same segment length, but a different shift length. The highest color clusters of the map (b) appear more

compact and simpler than the highest color clusters of the map (a). The two maps are showing different speckle patterns as a result of simple geometric transformations.

By comparing the two enlarged speckle pattern maps, significant similarities and differences in details could be recognized.

6 Conclusion

For any 0–1 sequence with N elements, the variant map system processes multiple segments to transform each segment in a pair of measures. Using the cryptographic sequence generated from the AES cipher, five statistic maps were created. Two 1D maps show binomial distributions to which we refer as classical maps. Three 2D maps are constructed as variant maps. Selecting smaller segmented lengths, both classical and variant maps were illustrated in four groups. With larger segmented lengths increased, there are significant speckle patterns observed. From a brief comparison of the two larger maps, the enlarged 2DP maps in Fig. 9a, b show better refined visual details than other smaller maps.

For the 2DPQ map, there are significant horizontal symmetries observed, however, there is no reflection effect in the vertical direction.

From different 2DP maps with parameters $m = \{125, \ldots, 128\}$, significant changes are observed: various speckle patterns are developed by both changes between lengths of segments and shift displacements. Enlarged maps are convenient to illustrate stochastic speckle patterns visibly. Some significant clusters are collected with speckle patterns associated to different control parameters in relevant maps.

From a viewpoint of system operation, two types of control parameters: length of segments and shift length of the sequence, provide an effective control mechanism to form clear speckle patterns on 2D distributions. It is necessary for us to put more attention on systematically exploring this type of issues, for refined researches on further directions.

The variant map system is different from both technologies: extracting information of speckle patterns to form random sequences and NIST 800-22 statistic testing package to use a single measurement of a P-value or a list of static parameters for evaluation. The variant framework provides five maps to identify complicated measurements through speckle patterns in details for any cryptographic sequence. Three refined 2D maps have more accurate properties than two 1D maps to describe nonlinear dynamic behavior as possible quantitative measurements.

In relation to the variant map system, future explorations on both theoretical foundation and key applications on cryptographic sequences are urgently required.

References

1. S. Pyne, B. Rao, S. Rao Edited, *Big Data Analytics - Methods and Applications* (Springer India, 2016)
2. L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, A.V. Vasilakos, Security and privacy for storage and computation in cloud computing. Inf. Sci. 371–386 (2014)
3. D. Puthal et al., A dynamic prime number based efficient security mechanism for big sensing data streams. J. Comput. Syst. Sci. **83**(1), 22–42 (2017)
4. S. Golomb, *Shift-Register Sequences*, Revised edn. (Aegean Park Press, Laguna Hills, California, 1982)
5. E. Barkam, E. Biham, N. Keller, Instant ciphertext-only cryptanalysis of GSM encrypted communication. J. Cryptology **21**(3), 392–429 (2008)
6. Y. Lu, W. Meier, S. Vaudenay, The conditional correlation attack: a practical attack on bluetooth encryption. Crypto **2005**(3621), 97–117 (2005)
7. https://en.wikipedia.org/wiki/ESTREAM
8. P. Junod, A. Canteaut, *Advanced Linear Cryptanalysis of Block and Stream Ciphers* (IOS Press, 2011), p. 2. ISBN 9781607508441
9. ZUC. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3: Document 2: ZUC Specification
10. A. Poorghanad, A. Sadr, A. Kashanipour, Generating high quality pseudo random number using evolutionary methods. IEEE Congr. Comput. Intell. Secur. **9**, 331–335 (2008)
11. A. de Queiroz, J. Schechtman, Elimination of nonlinear clock feed through in component-simulation switched-current circuits, in *Circuits and Systems, 1998. ISCAS '98. Proceedings of the 1998 IEEE International Symposium on*, pp. II378–II381 (1998)
12. A. Fuster-Sabater, F. Vitini, Classes of nonlinear filters for stream ciphers, chapter *Geometry, Algebra and Applications: From Mechanics to Cryptography*, Volume 161 of the series Springer Proceedings in Mathematics and Statistics, 107–119 (2016)
13. S. Ronjom, C. Cid. Nonlinear Equivalence of Stream Ciphers, in *Proceedings of Fast Software Encryption, 17th International Workshop*, FSE 2010, Seoul, Korea, Lecture Notes in Computer Science, vol. 6147 (Springer, 2010), pp. 40–54,
14. J. Nechvatal, E. Barker, L.Bassham, et al. (2000), Report on the development of the advanced encryption standard (AES), *National Institute of Standards and Technology (NIST)*, http://csrc.nist.gov/archive/aes/round2/r2report.pdf
15. G. Paul, S. Maitra. *RC4 Stream Cipher and Its Variants* (CRC Press, 2012)
16. S.D. Cardell, A. Fuster-Sabater, linear models for the self-shrinking generator based on CA. J. Cell. Automata **11**(23), 195211 (2016)
17. N. Nagaraj, One-time pad as a nonlinear dynamical system. Commun. Nonlinear Sci. Numer. Simul. **17**, 4029–4036 (2012)
18. E. Dubrova, M. Teslenko, H. Tenhunen. On analysis and synthesis of (n,k)-non-linear feedback shift registers, in *Proceedings of the Conference on Design, Automation and Test in Europe*, 1286–1291 (2008)
19. E. Dubrova, A list of maximum period NLFSRs, Cryptology ePrint Archive, Report 2012/166 (2012)
20. Y. Zhao, Y. Hu, S. Li, A new analysis method for nonlinear component of stream ciphers. J. Inf. Comput. Sci. **10**(16), 5313–5321 (2013)
21. D. Meschede. *Optics, Light and Lasers*, 2 ed. (Wiley-VCH, 2007)
22. R. Boyd. *Nonlinear Optics*, 3rd ed. (Academic Press, 2008)
23. M. Nakazawa et al., QAM quantum stream cipher using digital coherent optical transmission. Opt. Express **22**(4), 4098–4107 (2014)
24. M. Yoshida et al., Single-channel 40 Gbit/s digital coherent QAM quantum noise stream cipher transmission over 480 km. Opt. Express **241**, 652–661 (2016)
25. J. Barry, E. Lee, D.G. Messerschmitt, *Digital Communications* (Sprinter, 2004)
26. S. Lian, et al., A chaotic stream cipher and the usage in video protection.*Chaos Solitons and Fractals***34**(3), 851–859 (2007)

27. J.W. Goodman, Some fundamental properties of speckle. J. Opt. Soc. Am. **66**, 1145 (1976)
28. D.G. Marangon, G. Vallone, P. Villoresi, Random bits, true and unbiased, from atmospheric turbulence. Sci. Rep. **4**, 5490 (2014). https://doi.org/10.1038/srep05490
29. J. Marron, A.J. Martino, G.M. Morris, Generation of random arrays using clipped laser speckle. Appl. Opt. **25**, 26 (1986)
30. P. Lalanne et al., 2-D generation of random numbers by multimode fiber speckle for silicon arrays of processing elements. Opt. Commun. **76**, 387–394 (1990)
31. R. Horstmeyer, R.Y. Chen, B. Judkewitz, C. Yang, Markov speckle for efficient random bit generation. Opt. Express **20**, 26394–26410 (2012)
32. D.E. Knuth, *The Art of Computer Programming*, vol. 2: *Seminumberical Algorithms* (Addison-Wesley, 1969)
33. NIST. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST, Special Publication* (2010)
34. D. Makovoz, Noise variance estimation in signal processing, in *International Symposium on Signal Processing and Information Technology* (2006), pp. 364–369
35. K. Ito, Gaussian filter for nonlinear filtering problems, in *Conference on Decision and Control*, pp. 1218–1223 (2000)
36. F. Orieux, O. Feron, J. Giovannelli, Sampling high-dimensional gaussian distributions for general Linear inverse problems. IEEE Signal Process. Lett. **19**(5), 251–254 (2012)
37. J.W. Goodman. *Speckle Phenomena in Optics Theory and Applications*, (Ben Roberts and Cpmpany, 2007)
38. Speckle pattern, https://en.wikipedia.org/wiki/Speckle_pattern
39. M. Cross, P. Hohenberg, Science **263**, 1569 (1994)
40. P. Colet, R. Roy, K. Wiesenfeld, Phys. Rev. E **50**, 3453 (1994)
41. I.S. Aranson, L. Kramer, Rev. Mod. Phys. **74**, 99 (2002)
42. M. Jiang, X. Wang, Q. Ouyang, H. Zhang, Phys. Rev. E **69**, 056202 (2004)
43. H. Zhang, B. Hu, G. Hu, Q. Ouyang, J. Kurths, Phys. Rev. E **66**, 046303 (2002)
44. Q. Ouyang, *Introduction on Nonlinear Sciences and Pattern Dynamics* (Peking University Press, 2010) (in Chinese)
45. P.J.A. Holmes, Nonlinear oscillator with a strange attractor. Philos. Trans. Royal Soc. A **292**(1394), 419–448 (1979)
46. F. Haake. *Quantum Signatures of Chaos* (Springer-Verlag, 2010)
47. G. Teschl, *Ordinary Differential Equations and Dynamical Systems, Graduate Studies in Mathematics*, vol. 140 (Amer. Math. Soc, Providence, 2012)
48. Z.J. Zheng, C.H.C. Leung, Visualising global behaviour of 1D cellular automata image sequences in 2D Map. Phys. A **3–4**, 785–800 (1996)
49. D. E. Knuth. *The Art of Computer Programming*, vol. 4A: *Combinatorial Algorithms Part 1* (Addison-Wesley, 2011)
50. Z.J. Zheng. *Conjugate transformation of regular plan lattices for binary images*, Ph.D. Thesis, Monash University (1994)
51. J. Zheng, C. Zheng, A framework to express variant and invariant functional spaces for binary logic, Frontiers of Electrical and Electronic Engineering in China, 5(2), 163–172. Higher Educational Press and Springer-Verlag (2010). https://doi.org/10.1007/s11460-010-0011-4
52. H. Wang, J. Zheng, 3D Visual Method of Variant Logic Construction for Random Sequence, in *Australian Information Warfare and Security*, pp. 16-27 (2013)
53. W.Z. Yang, J. Zheng, Variant pseudo-random Number generator, Hakin9 Extra. Timing Attack **06**(13), 28–31 (2012)
54. J. Zheng, Novel Pseudo-Random Number Generation Using Variant Logic Framework, in *2nd International Cyber Resilience Conference*, 10bit04 (2011). http://igneous.scis.ecu.edu.au/proceedings/2011/icr/zheng.pdf
55. J. Zheng, C. Zheng, Variant simulation system using quaternion structure. J. Mod. Opti. **59**(5), 484–492 (2012)
56. J. Zheng, C. Zheng, T.L. Kunii, Interactive Maps on Variant Phase Space,in *Emerging Application of Cellular Automata*, pp. 113–196 (InTech Press, 2013)

57. J. Zheng, W. Zhang, J. Luo, W. Zhou, R. Shen, Variant map system to simulate complex properties of DNA interactions using binary sequences. Adv. Pure Math. **3**(7A), 5–24 (2013)
58. D.M. Heim, O. Heim, P.A. Zeng, J. Zheng, Successful creation of regular patterns in variant maps from bat echolocation calls. Biol. Syst.: Open Access **5**, 2 (2016). https://doi.org/10.4172/2329-6577.1000166