Neural Comput & Applic (2014) 25:1717–1722
DOI 10.1007/s00521-014-1663-4

ORIGINAL ARTICLE

A novel image encryption technique based on Hénon chaotic map and S_8 symmetric group

Majid Khan · Tariq Shah

Received: 3 November 2013 / Accepted: 5 July 2014 / Published online: 20 July 2014

Abstract The structure of cryptographically resilient substitution boxes (S-boxes) plays a central role in devising safe cryptosystems. The design of chaos-based S-boxes by means of chaotic maps obtained more devotion in current ages. We have suggested novel S-boxes based on the chaotic maps and S_8 symmetric group. We have experimented our chaos-based S-box for image encryption applications and analyze its strength with statistical analyses.

Keywords S-boxes · Chaotic maps · S_8 symmetric group

1 Introduction

Cryptography is the discipline of defending the confidentiality of information throughout communication under antagonistic situations. In the recent age of information technology and booming computer network communications, cryptography has a distinctive significance. Cryptography is regularly utilized not only to guard the data but also offers the procedures for secure communication. Since 1990s, various investigators have observed that there arises thought-provoking connection between chaos and cryptography; various assets of chaotic structures have their corresponding complements in outmoded cryptosystems [1–7].

Various ultimate features of chaos, such as the ergodicity which is an irreducibility belongings, analogous to the concepts of irreducible representation in algebra and prime number in arithmetic, mixing and exactitude assets and the sensitivity to preliminary conditions, can be linked with the confusion and diffusion features in cryptography. Therefore, it is a standard indication to use chaos to enhance the strategy of novel encryptions. Many chaotic systems have been widely considered in past years for the design of chaotic ciphers and performance analyses.

In the modern ages, chaos-based protected communication has obtained considerable devotion since it suggests potential advantages over conventional methods due to its simplicity [4, 8] and high level of unpredictability. In the literature, many chaotic systems have been presented [9–11], but few have been used in cryptography.

In the block cipher system, the plaintext is distributed into the blocks and the ciphering is carried out for the complete block. Two wide-ranging ideas of block ciphers which were proposed by Shanon's are diffusion and confusion. Diffusion is scattering of effect of plaintext bits to ciphertext bits with target to obscure the statistical configuration of plaintext. Confusion is transformation in which alterations dependency of information of ciphertext on the information of plaintext. In most cipher structures, the diffusion and confusion are attained by means of round recurrence [12–15]. Modern block encryptions comprise of four conversions: substitution, permutation, mixing and key adding [12, 16, 17].

A number of famous block ciphers are of substitution-permutation (SP) category. S-boxes are used in such cipher structures as the essential nonlinear element. A robust block cipher must be hardy to numerous attacks, such as linear and differential cryptanalysis. In SP systems, this is normally reached if the S-boxes used satisfy a number of measures. The S-box functioning in encryption procedure could be selected under the control of key, as a substitute of being static. Several random key-dependent and bijective

M. Khan (✉) · T. Shah
Department of Mathematics, Quiad-i-Azam University, Islamabad, Pakistan
e-mail: mk.cfd1@gmail.com

S-boxes are generated for encryption applications, which satisfy selected standards [17–21]. The S-box generation technique constructed on a 2D discretized chaotic Baker map was planned in [22]. Later, the 2D was further stretched to a 3D one [23]. In this work, we have suggested a new chaos-based S-boxes that are simply a combination of Hénon maps [24–26] and symmetry group S_8, which enhanced the confusion and diffusion capability of proposed designed block cipher. We have used our designed chaos-based S-boxes in image encryption application and investigate the texture features of second order [27–31].

2 Fundamental properties of chaotic systems

Chaos has been witnessed in many natural structures covering a significant amount of technical and industrial areas. These occurrences display definite possessions that mark them difficult and volatile. Chaos theory deals with constructions that progress in time to a specific kind of dynamical actions. Several authors have addressed the mathematical theory of chaos due to its vast and most applicable effects in various fields of science. In broad-spectrum, these schemes follow a definite set of procedures of improvement. Generally, chaos happens simply in certain deterministic nonlinear systems. Clearly, chaos seems when there is a continuous and disorganized looking long-term progression that fulfills definite mathematical benchmarks. There are certain set of properties that sum up the features witnessed in chaotic systems. These measured the mathematical principles that describe chaos. The most appropriate are [4]:

1. *Nonlinearity*: If a system is linear, it cannot be chaotic.
2. *Determinism*: It has deterministic fundamental rules that every future state of the system must follow.
3. *Sensitivity to initial conditions*: Slight deviations in its early state can lead to completely dissimilar performance in its last state. This "butterfly outcome" permits the opportunity that even the minor perturbation of a butterfly flapping its wings can radically disturb weather sunny or cloudy skies will prevail existences far ahead.
4. *Continued irregularity in the actions of the system*: Secret order together with a large or infinite amount of unstable periodic designs. This unseen direction forms the structure of irregular chaotic systems.
5. *Long-term prediction*: It is commonly difficult due to sensitivity to initial conditions, which can be recognized only to a limited amount of accuracy.

2.1 Chaotic Hénon maps

The Hénon map is proposed by the French astronomer and mathematician Michel Hénon [24]. The Hénon map has yielded a great deal of interesting characteristics as it was studied. At their core, the Hénon map is basically a family of functions defined from $f_{\alpha\beta} : \mathbb{R}^2 \to \mathbb{R}^2$ and denoted by:

$$f_{\alpha\beta}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y + 1 - \alpha x^2 \\ \beta x \end{pmatrix}, \quad (1)$$

where α and β are (positive) bifurcation parameters (Figs. 1, 2, 3).

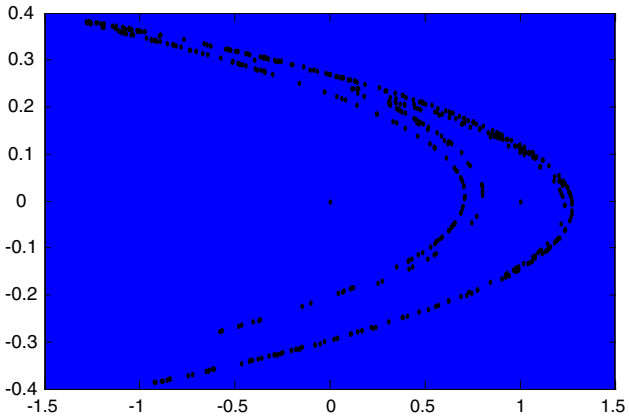

Fig. 1 The Hénon attractor

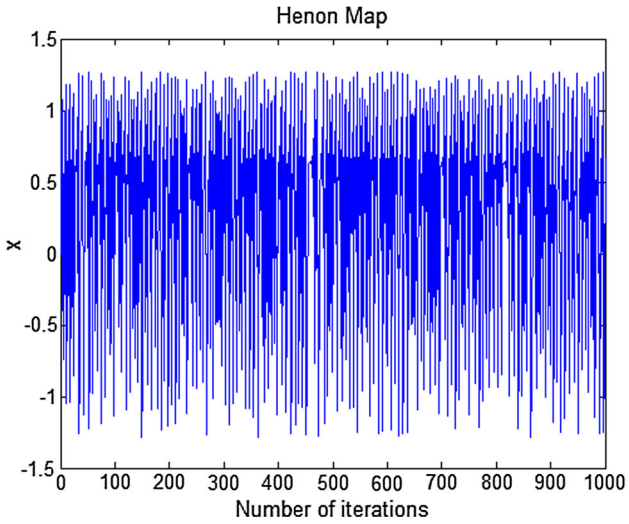

Fig. 2 Unpredictability of Hénon map along *x*-axis

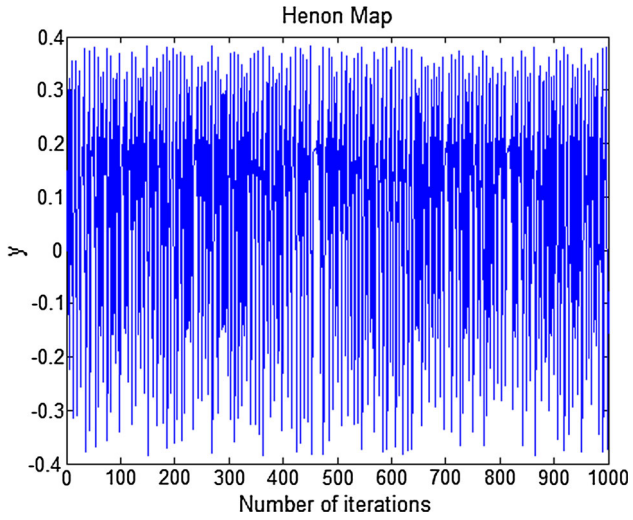

Fig. 3 Unpredictability of Hénon map along y-axis

2.2 Mathematical properties of Hénon map

1. The Hénon map is composition of three different transformations [25], usually denoted f_1, f_2 and f_3. These conversions are defined below:

$$f_1\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y + 1 - \alpha x^2 \end{pmatrix}, f_2\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \beta x \\ y \end{pmatrix} \text{ and } f_3\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix}. \quad (2)$$

   From the above definitions, we have $f_{\alpha\beta} = f_3 \circ f_2 \circ f_1$.
2. The Hénon map is one-to-one.
3. The Hénon map is invertible. It is not obvious just from inspection, but it is possible to derive an exact expression for $f_{\alpha\beta}$.
4. For $\beta \neq 0$, the inverse of $f_{\alpha\beta}$ is $f_{\alpha\beta}^{-1}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \frac{y}{\beta} & -1 + \frac{\alpha}{\beta^2}y^2 + x \end{pmatrix}^T$, and it is one-to-one.

The Hénon map has some geometrical properties which inherent stretching and folding in phase space, which offers growth to chaotic actions. The Hénon map is divided into three stages to recognize its correspondence to the stretch and fold action [26]. The following are three phases of Hénon map:

(a) *Bend up* This property mainly expresses the nonlinear bending in y coordinate given by

$$f_1(x, y) = \left(x, 1 + y - \alpha x^2\right). \quad (3)$$

Along line parallel to x-axis (y = constant), we have a parabola with the vertex at $(0,1 + y)$.

(b) *Contraction in x* The second geometrical characteristic is contraction in x-direction, which is represented by the following mathematical transformation:

$$f_2(x, y) = \left(\beta x, 1 + y - \alpha x^2\right). \quad (4)$$

The contraction factor is given by the parameter β, which is 0.3 for the Hénon attractor.

(c) *Reflection* The reflection along the diagonal is represented by

$$f_3(x, y) = (y, x). \quad (5)$$

The effect of the compression is same as apply the unique transformation one time, i.e.,

$$f(x, y) = f_3(f_2(f_1(x, y))). \quad (6)$$

A detailed relation of chaos and cryptography are given in Table 1.

Table 1 Comparison of chaotic and cryptographic properties

Chaos theory	Cryptography
Chaotic system	Pseudo-chaotic system
Nonlinear transform	Nonlinear transform
Infinite number of states	Finite states
Infinite number of iterations	Finite iterations
Initial state	Plaintext
Final states	Ciphertext
Initial conditions and/or parameters	Key
Asymptotic independence of initial and final states	Confusion
Sensitivity to initial conditions and parameters mixing	Diffusion

3 Chaos-based algorithm for S-box design and encryption algorithm

In this section, we have presented the algorithm to synthesize S-boxes that are based on Hénon chaotic map. The algorithm mainly consists of five steps starting from defining initial seed from Hénon chaotic maps to apply permutation of symmetry group to generate S-boxes. This algorithm also demonstrates the application to image encryption systems (see Table 2).

An instance of the proposed S-box is shown in Table 3. This S-box has 16 × 16 entries obtained from the Hénon chaotic map used in the proposed algorithm.

4 Statistical analyses of proposed algorithm

In this section, we mainly discussed the statistical features of an image, which are mainly texture qualities of an

image. An image texture is a set of metrics considered in image handling designed to measure the observed quality of an image. Image quality offers us evidence about the spatial organization of color or strengths in an image or designated region of an image The texture features are characteristics, which are used to capture the graphical assets of an image either comprehensively for the complete image or in the neighborhood for sections or stuffs. The graphical appearances of similar areas of real-world images are frequently identified as quality. As an image is made of pixels, texture can be defined as a unit containing jointly connected pixels or cluster of pixels and thus leading to graphical feature of images. An image can be designated with the help of measurements of first order for gray intensities of the pixels inside a locality. The instances of such qualities taken from the image histogram are mean and standard deviation (SD). The characteristics of second order are based on gray level co-occurrence matrix (GLCM) [27–31], and it is the best widespread approaches for pixel deviation information. The features of second

Table 2 Proposed chaos-based algorithm for chaotic S-boxes and image encryption

S.1: We have taken initial seed of 16 × 16 distinct values from first component of Hénon chaotic map with properly selected chaotic parameters and initial conditions
S.2: Convert each of the values in eight bits binary
S.3: Apply the permutation of symmetry group of S8 to each element in step 2
S.4: Generate the sequence $S_{n+1} = \lfloor y_{n+1} \times 40320 \rfloor$, we can get the integer sequences that ranges from 0 to 40,320
S.5: The numbers in the sequence produced by in step 4; we select the numbers as the index of the S-boxes order to accomplish the substitution encryption of an image

Table 3 The proposed chaos and permutation symmetry group S_8 S-box

33	152	0	248	1	174	231	83	43	73	230	185	70	113	58	222
86	17	34	211	21	179	177	187	66	188	254	122	165	197	191	170
146	145	129	30	64	198	6	157	252	173	82	219	132	88	101	162
100	45	19	65	77	208	194	81	192	130	171	32	53	245	37	68
4	62	41	186	212	184	150	79	183	253	94	46	131	16	60	31
36	102	169	205	237	246	144	149	90	154	14	10	24	50	240	72
223	142	117	119	148	23	22	98	178	18	96	118	105	232	155	202
249	103	161	108	199	109	203	128	106	20	47	196	176	244	42	195
49	251	54	163	29	209	48	213	216	110	137	51	217	115	168	236
38	40	15	189	59	135	134	9	39	61	139	234	210	2	180	52
207	243	55	121	8	13	166	175	147	143	3	67	85	172	107	133
226	116	95	153	78	7	228	200	111	63	159	229	126	97	141	26
92	138	112	57	76	218	204	80	125	241	27	220	89	120	167	104
127	28	12	11	255	151	214	93	193	75	239	160	250	56	69	25
201	123	140	71	225	235	233	136	35	158	224	91	242	221	215	247
164	206	5	124	74	181	238	156	227	182	84	114	190	99	44	87

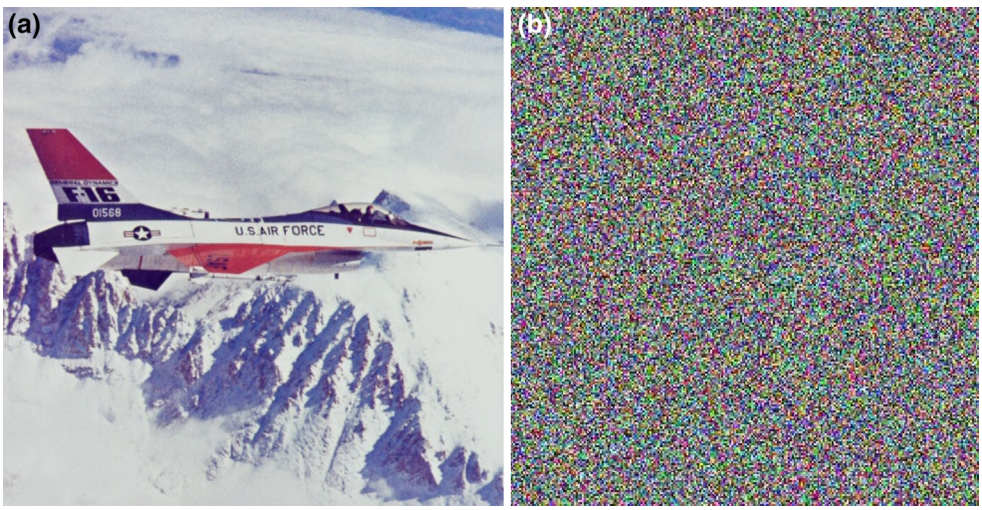

Fig. 4 Plain (**a**) and encrypted (**b**) images of size 256 × 256

order are entropy, contrast, homogeneity, energy and correlation of the gray level pixels defined as follows:

$$H = -\sum_i \sum_j p(x_i, x_j) \log_b p(x_i, x_j), \tag{7}$$

$$C = \sum_i \sum_j |i-j|^2 p(i,j), \tag{8}$$

$$H = \sum_i \sum_j \frac{p(i,j)}{1+|i-j|}, \tag{9}$$

$$E = \sum_{i,j} p(i,j)^2, \tag{10}$$

$$r = \sum_i \sum_j \frac{(i-\mu_i)(j-\mu_j)}{\sigma_i \sigma_j} p(i,j), \tag{11}$$

where i and j are two dissimilar gray levels of the image, p is the number of the co-appearance of gray levels i and j, μ_i, μ_j are mean of i and j levels of image, σ_i and σ_j are the standard deviations at i and j levels of an image. Entropy is used to measure the content of an image with higher value indicating an image with richer details. Contrast is used to measure the intensity change between a pixel and its neighbor over the entire image and is 0 for a constant image. Homogeneity processes the resemblance of grayscale levels across the image and ranging from zero to unity inclusive. Thus, higher the variations in the grayscale, the higher the GLCM difference and lower the homogeneity. GLCM energy deals with total probability of distinctive grayscale configurations in image, and its value is unity for a constant image. Correlation returns an amount of how interrelated a pixel is to its locality over the entire image, and it is used to measure the joint probability of occurrence of particular pixel sets. The range of correlation coefficient lies between [−1,1]. The encryption through the proposed algorithm is given in Fig. 4. Tables 4 and 5 give comparison of the texture features of original and encrypted images.

From the calculated values of entropy (see Table 4), we have observed that the entropy values of original images are far from ideal value of entropy, which is eight bits, since data sources are extremely redundant and thus hardly produce evenly scattered random messages, whereas the entropy values of the encrypted images are near to the best value, which means that the suggested encryption procedure is decidedly strong against entropy attacks. The value of contrast for original image is 0.298752, whereas for an encrypted image 5.20712, which clearly reflects that, intensity change between a pixel and its neighbor over the entire encrypted image is high (see Table 4). The low value of homogeneity for encrypted image shows the higher GLCM difference and higher differences in the grayscale. Energy analyses of both original and encrypted images reveal that quantity of recurring pairs is low for encrypted image, which is a significance of the proposed algorithm. Finally, we have broken the correlation among the adjacent pixels values as seen from the numerical values of correlation of an encrypted image (see Table 5).

Table 4 Texture features of plain and ciphered images

Texture features	Plain image	Cipher image
Entropy	7.431821	7.99730
Contrast	0.298752	5.20712
Homogeneity	0.896043	0.464131
Energy	0.095504	0.0282395
Correlation	0.963788	−0.00969638

5 Conclusion

In this work, we have proposed a new procedure for designing chaotic S-boxes and its application in image encryption. This procedure is based on Hénon chaotic map and S_8 permutation. Experimental assessments have been carried out with complete numerical scrutiny, which reveals the strength of the projected procedure against numerous kinds of attacks. Additionally, performance valuation investigations determine that the suggested image encryption algorithm is vastly protected. The proposed encryption scheme is capable of high-speed encryption and decryption, which is appropriate for internet encryption and broadcast applications.

Table 5 Texture features of plain and ciphered images for color components

Textures features	Plain image			Cipher image		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.301416	0.29136	0.296596	5.230890	5.423430	5.15297
Homogeneity	0.894101	0.899973	0.897468	0.463997	0.459866	0.465617
Energy	0.112931	0.096232	0.109009	0.026159	0.024618	0.026601
Correlation	0.969755	0.964698	0.956038	0.075238	0.081073	0.075988

References

1. Shanon C (1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715
2. Webster AF, Tavares SE (1986) On the design of S-boxes. In: Williams HC (ed) Advances in cryptology—CRYPTO'85. Lecture notes in computer science, vol 219. Springer, Berlin, Heidelberg, pp 523–534
3. Binder PM, Jensen RV (1986) Simulating chaotic behavior with finite-state machines. Phys Rev A 34:4460–4462
4. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos 16:2129–2151
5. Alvarez G, Amigó JM, Arroyo D, Li S (2011) Lessons learnt from cryptanalysis of chaos-based ciphers, in chaos-based cryptography. Theory, algorithms and applications. Stud Comput Intell 354:257–295
6. Alligood KT, Sauer T, Yorke JA (1997) Chaos: an introduction to dynamical systems. Springer, New York
7. Amigó JM (2009) Chaos-based cryptography. In: Kocarev L, Galias Z, Lian S (eds) Intelligent computing based on chaos. Studies in computational intelligence, vol 184. Springer, Berlin, Heidelberg, pp 291–313
8. Amigo JM, Szczepanski J (2003) Approximations of dynamical systems and their application to cryptography. Int J Bifurc Chaos 13(7):1937–1948
9. Szczepanski J, Amigo JM, Michalek T, Kocarev L (2005) Cryptographically secure substitutions based on the approximation of mixing maps. IEEE Trans CircSyst-I 52(2):443–453
10. Chen G (2008) A novel heuristic method for obtaining S-boxes. Chaos, Solitons Fractals 36:1028–1036
11. Jakimoski G, Kocarev L (2001) Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst-I 48(2):163–169
12. Masuda N, Jakimoski G, Aihara K, Kocarev L (2006) Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans Circ Syst-I 53(6):1341–1352
13. Matsui M (1994) Linear cryptanalysis method for DES ciphers. In: Helleseth T (ed) Advances in cryptology—EUROCRYPT'93. Springer, Berlin, pp 386–397
14. Menezes AJ, van Oorschot PC, Vanstone SA (1997) Handbook of applied cryptography. CRC, Boca Raton
15. Schneier B (1996) Applied cryptography: protocols, algorithms, and source code in C. Wiley, New York
16. Schneier B (1994) Description of a new variable-length key, 64-bit block cipher (Blowfish). In: Anderson R (ed) Fast software encryption. Lecture notes in computer science, vol 809. Springer, Berlin, Heidelberg, pp 191–204
17. Khan M, Shah T, Mahmood H, Gondal MA (2013) An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dyn 71:493–504
18. Khan M, Shah T, Gondal MA (2013) An efficient technique for the construction of substitution box with chaotic partial differential equation. Nonlinear Dyn 73:1795–1801
19. Khan M, Shah T, Mahmood H, Gondal MA, Hussain I (2012) A novel technique for constructions of S-boxes based on chaotic Lorenz systems. Nonlinear Dyn 70:2303–2311
20. Khan M, Shah T (2014) A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dyn 76(1):377–382
21. Khan M, Shah T (2013) An efficient construction of substitution box with fractional chaotic system. Signal Image Video Process. doi:10.1007/s11760-013-0577-4
22. Tang GP, Liao XF (2005) A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, Solitons Fractals 23:1901–1909
23. Chen G, Chen Y, Liao XF (2007) An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps. Chaos, Solitons Fractals 31:571–579
24. Hénon M (1976) A two-dimensional mapping with a strange attractor. Commun Math Phys 50:69–77
25. Al-Shameri WFH (2012) Dynamical properties of the Hénon mapping. Int J Math Anal 6:2419–2430
26. Sarmah HK, Paul R (2010) Period doubling route to chaos in a two parameter invertible map with constant Jacobian. Int J Res Rev Appl Sci 3(1):72–82
27. Haralick RM, Shanmugam K, Dinstein I (1973) Textural features for image classification. IEEE Trans Syst Man Cybern 3:610–621
28. Buf JMH, Kardan M, Spann M (1990) Texture feature performance for image segmentation. Pattern Recogn 23:291–309
29. Haddon JF, Boyce JF (1993) Co-occurrence matrices for image analysis. IEE Electron Commun Eng J 5:71–83
30. Ohanian PP, Dubes RC (1992) Performance evaluation for four class of texture features. Pattern Recogn 25:819–833
31. Haralick RM (1979) Statistical and structural approaches to texture. Proc IEEE 67:786–804