Ali Khan, Fadia and Ahmed, Jameel and Ahmad, Jawad and Khan, Jan Sher and Stankovic, Vladimir (2018) Intertwining and NCA maps based new image encryption scheme. In: IEEE International Conference on Computing, Electronics & Communications Engineering, 2018-08-16 - 2018-08-17, University of Essex. ,

Intertwining and NCA Maps Based New Image Encryption Scheme

Fadia Ali Khan
Department of Electrical Engineering
Riphah International University
Islamabad, Pakistan
fadiasohail@gmail.com

Jameel Ahmed
Department of Electrical Engineering
Riphah International University
Islamabad, Pakistan
jameel.ahmed@riphah.edu.pk

Jawad Ahmad
School of Engineering and Built Environment
Glasgow Caledonian University
Glasgow, United Kingdom
jawad.ahmad@gcu.ac.uk

Jan Sher Khan
Department of Electrical and Electronics
University of Gaziantep
27310 Gaziantep, Turkey
jskm893@gmail.com

Vladimir Stankovic
Department of Electronic and Electrical
Engineering, University of Strathclyde
Glasgow, United Kingdom
vladimir.stankovic@strath.ac.uk

Abstract—**In this digital era, the Internet is a main source of communication. Due to exponential advancement in Internet technologies, transmission of multimedia data is very common now. However, transmitting sensitive information over the Internet is always vulnerable to different kind of attacks. In order to address such issues, cryptographers are proposing encryption techniques. In encryption, data is manipulated in such a way that intruders cannot access the original information. This paper presents a secure image encryption scheme via Intertwining and Nonlinear Chaotic Maps (NCA). Both main steps i.e., confusion and diffusion are implemented using chaotic maps. Numerous security parameters are applied to the proposed improved technique and strength of the scheme is evaluated. All experimental results proved the robustness and higher security of the proposed chaos-based scheme.**

Index Terms—**NCA, Intertwining map, security, NPCR, UACI**

I. Introduction

In our daily life, modern research and communication technologies are making their roots strengthen with the passage of time. Emails, security alert systems, E-banking, education portals, online reservations and shopping catalogues are intensify these days. Today's communication and correspondence are inevitable without the Internet. The word communication conceals vast vocabulary inside it. Data, images, video content, audio signals all are different types of communication which are needed to be sent over an insecure channel, i.e., Internet. Frequent, accurate and intense data transfer needs open-ended Internet without any filters or privileges. Due to open nature of the Internet, communication data is always vulnerable to attacks. An eavesdropper can steal sensitive data and can extract valuable and meaningful data out of it.

Images, audio video and text are collectively known as multimedia data. Therefore in the area of information and network security efforts have been made to strengthen the security of multimedia contents. In past, different security algorithms are implemented to secure data in a diverse manner. However, with the evolution of computer technologies, such security algorithms are now obsolete and cannot provide sufficient security. These systems implements algorithms that are not easily predictable or breakable but still lacks either efficient implementation or stronger security. Hence, there is always a room for new techniques or improvement of the past methods. Medical images, military image data information and financial data transactions need a very high level of security.

For many decades, cryptography has played an important role in securing multimedia contents. Manipulating digital information in a non-linear way and unpredictable manner leads to a method known as *encryption*. Two techniques are very common for making digital information secure; encryption and digital water marking. In encryption, a secret key is used to encrypt the message and then can be transmitted over the insecure channel. When an encrypted message is received at the receiver side, plaintext is obtained using the secret key. The processes of making the message readable are known as decryption.

In image encryption, plaintext image pixels are permuted and substituted in such a way that original contents are hidden. When a plaintext image is encrypted the result is called ciphertext of encrypted image. Ciphertext image contains meaningful information, however, an eavesdropper can not deduce this information without the key. Over the last decades, chaos played an important role in the field of cryptography and image encryption. Ergodicity and initial condition sensitivity are most attractive attributes of chaotic maps. Due to the aforementioned properties, the chaotic map can efficiently secure multimedia contents. However, traditional chaos-based encryption schemes are not computationally secure and also have been proved weaker by some researchers [1]. Despite the fact that some of them are still secure yet computationally expensive and require high processing power. Moreover, images are different from the text and traditional encryption schemes are not well fitted for images. Due to pixels correlation and high volume data, efficient image encryption techniques are the main focus of many cryptographers.

One can hide the original content of an image via Substitution Box (S-Box) [2], [3]. Image pixel values are substituted through S-Box. However, image encryption schemes which are based only on S-box are highly vulnerable to attacks. Recently, Atta et al proposed image encryption methods which are completely based on S-Box [4]. The proposed SBox is mainly dependent on LogisticTent System (LTS) with varying exponents. From Fig. 1, it is clear that S-Box only method cannot conceal image information when an image is highly correlated. Histogram results also reveal that plaintext pixels are substituted with only two S-Box elements and hence statistical attacks are possible on such schemes.

II. Proposed Image Encryption Scheme

S-Box is used as the main source of creating confusion in plaintext images. However, many image encryption schemes which are only based on S-Box are proven to be insecure as outlined in [2]. Chaos-based confusion and diffusions are good choices in case of aforementioned issues. Randomness in the image pixels through confusion and diffusion operations can strengthen a scheme against various attacks. In the field of cryptography, Logistic map is widelu used for encryption. However, it has been found in [5] that Intertwining logistic map can overcome the shortcomings of Logistic map. The advantages of Intertwining map is already justified in [5]. Mathematically: [6], [7]:

$$\begin{aligned} x_{n+1} &= (\lambda \times \alpha \times y_n \times (1 - x_n) + z_n) mod(1), \\ y_{n+1} &= (\lambda \times \beta \times y_n + z_n \times \frac{1}{1 + (x_{n+1})^2}) mod(1), \\ z_{n+1} &= (\lambda \times (x_{n+1} + y_{n+1} + \gamma) \times sin(z_n) mod(1). \end{aligned} \quad (1)$$

where x_n, y_n and z_n $\in$ (0,1), $0 \leq \lambda \leq 3.999$, $|\alpha| > 33.5, |\beta| > 37.9, |\gamma| > 35.7$. The proposed scheme is outlined as:

Step 1: Apply cryptographic 256 bit hash (secure hash algorithm) on input image A and save result in B. The obtained B is 64 bit hexadecimal value (B = $H1H2...H64$).

Step 2: Represent hexadecimal value in binary format and set initial conditions for Intertwining map as:

$$\lambda_0 = \frac{B1 \times 2^0 + B2 \times 2^1 ... + B64 \times 2^{63}}{2^{64}},$$

$$|\alpha|_0 = \frac{B65 \times 2^0 + B50 \times 2^1 ... + B128 \times 2^{63}}{2^{64}},$$

$$|\beta|_0 = \frac{B129 \times 2^0 + B66 \times 2^1 ... + B192 \times 2^{63}}{2^{64}},$$

$$|\gamma|_0 = \frac{B193 \times 2^0 + B98 \times 2^1 ... + B256 \times 2^{63}}{2^{64}},$$

Now set $\lambda, |\alpha|, |\beta|$ and $|\gamma|$ as:
λ = $\lambda_0 \times 10^{14}$ mod (3.999)
$|\alpha|$ = $\alpha_0 \times 10^{14}$ mod (1) + 33.5
$|\beta|$ = $\beta_0 \times 10^{14}$ mod (1) + 37.9
$|\gamma|$ = $\gamma_0 \times 10^{14}$ mod (1) + 35.7

Step 3: Iterate Intertwining map $M \times N$ times using above initial conditions and save the results in random row vectors x and y, respectively. Discard values of z.

Step 4: Shuffle image A rows and column using random row vector x and y, respectively and save result in Δ.

Step 5: Iterate NCA map $M \times N$ times and save results in matrix Λ. NCA map is given as [8]:

$$x_{n+1} = (1 - \psi^{-4}).\text{cot}(\frac{\phi}{1 + \psi}).(1 + \frac{1}{\psi})^{\psi}.\text{tan}(\phi \zeta_n).(1 - \zeta_n)^{\psi}, \quad (2)$$

where the seed parameters are defined as:

$$\begin{cases} \zeta_n \in (0,1) \\ \phi \in (0, 1.4] \\ \psi \in [5, 43] \\ \text{or} \\ \zeta_n \in (0,1) \\ \phi \in (1.4, 1.5] \\ \psi \in [9, 38] \\ \text{or} \\ \zeta_n \in (0,1) \\ \phi \in (1.5, 1.57] \\ \psi \in [3, 15] \end{cases}$$

Step 6: Apply XOR operation on Δ and Λ and save the result in Γ.

Step 7: Apply advanced encryption standard S-Box on Γ. The resultant matrix is the encrypted ciphertext C.

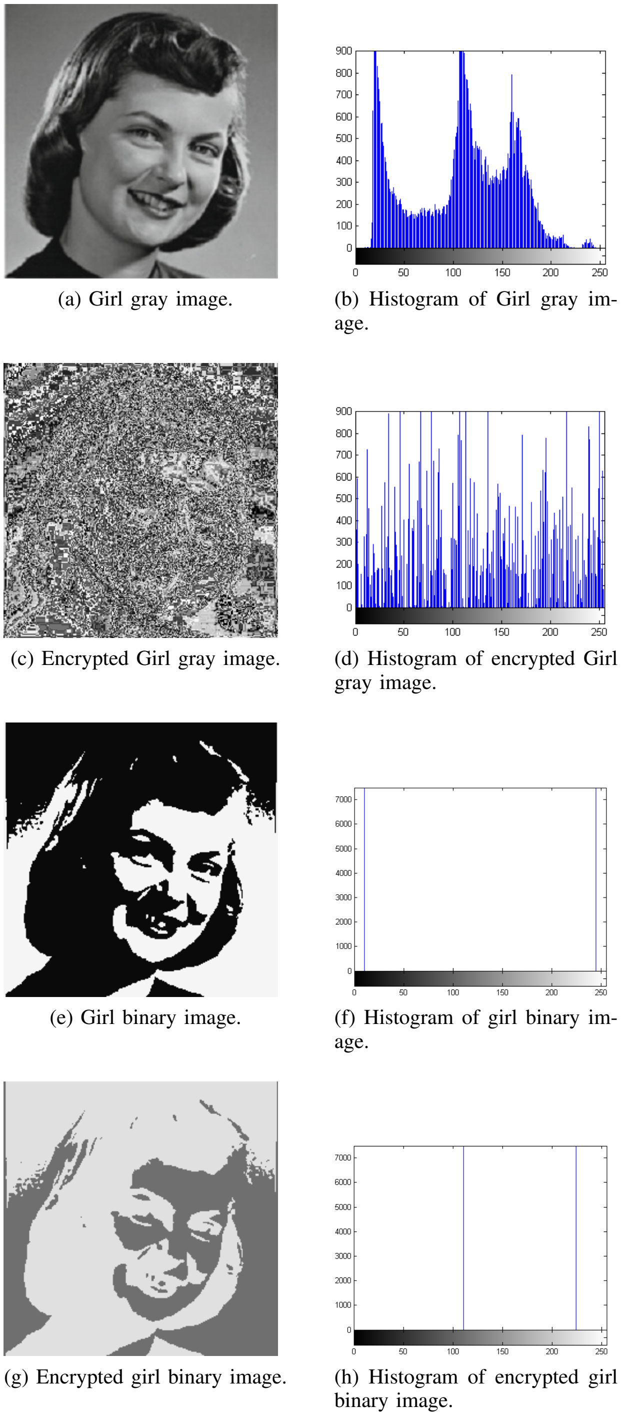
III. Security Analysis

A. Correlation Coefficient

Correlation coefficient metric determine the degree of similarity. If two variables are highly correlated then their coefficient value would be high. If both variables are less correlated then their coefficient value would be less. Mathematically, correlation coefficient can be written as [2]:

$$\text{Correlation Coefficient} = \frac{\text{Covariance}(e, f)}{\sigma_e \times \sigma_f}, \quad (3)$$

where σ_e and σ_f are standard deviation at pixel position e and f, respectively. Firstly an image is encrypted and then correlation coefficient is calculated. If the results of the correlation coefficient are -1 then this value reveals that plaintext image pixels are opposite to the ciphertext image. A value of 1 means that both plaintext and ciphertext images are similar. Ideally, zero value of correlation is required for a good encryption scheme. From Table I and II, it is obvious that the proposed scheme has a low correlation in contrast to S-Box based methods. Correlation coefficient metric proves that the values obtained in our proposed cryptosytem is near to 0.



(a) Girl gray image.

(b) Histogram of Girl gray image.

(c) Encrypted Girl gray image.

(d) Histogram of encrypted Girl gray image.

(e) Girl binary image.

(f) Histogram of girl binary image.

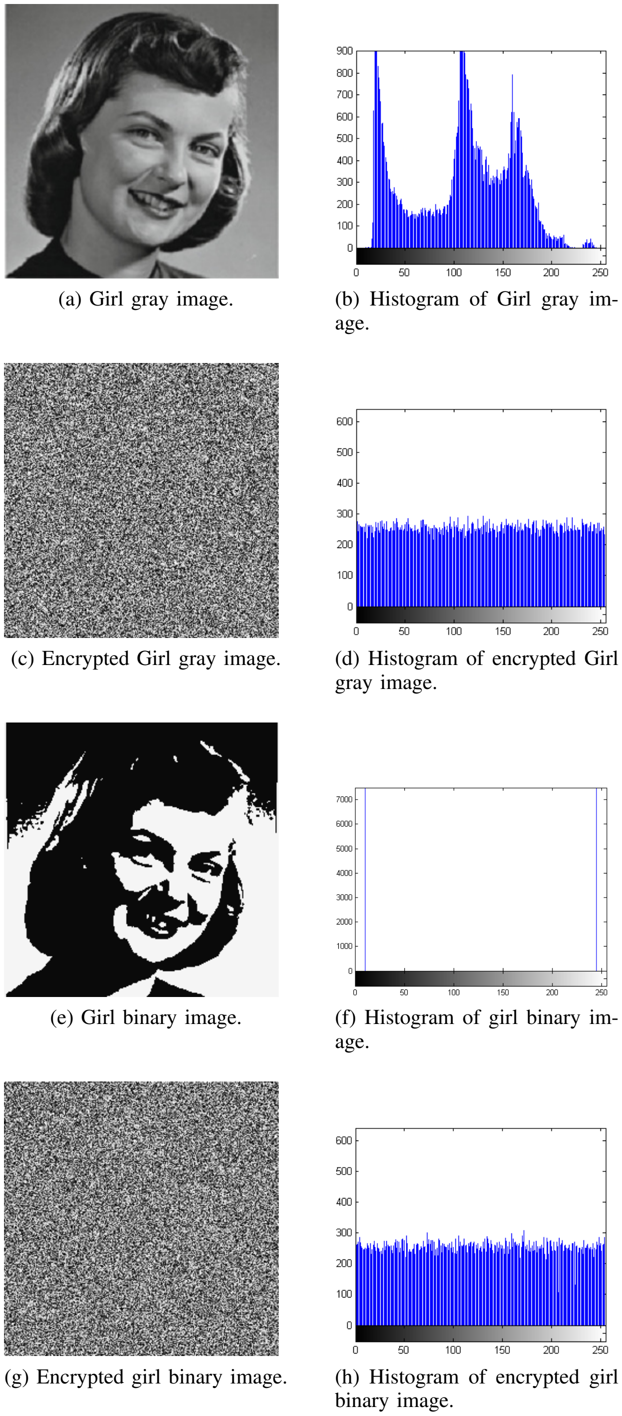
(g) Encrypted girl binary image.

(h) Histogram of encrypted girl binary image.

Fig. 1: Histogram and encryption results of S-Box Based image encryption algorithm: Girl gray and binary images.

TABLE I: Correlation coefficient comparison analysis of the proposed scheme with a conventional scheme: gray-scale Girl image.

Direction	Plaintext image	Ciphertext [4]	Ciphertext proposed
Horizontal Direction	0.9732	0.1566	-0.0011
Vertical Direction	0.9820	0.1537	0.0203
Diagonal Direction	0.9506	0.0858	-0.0267



(a) Girl gray image.

(b) Histogram of Girl gray image.

(c) Encrypted Girl gray image.

(d) Histogram of encrypted Girl gray image.

(e) Girl binary image.

(f) Histogram of girl binary image.

(g) Encrypted girl binary image.

(h) Histogram of encrypted girl binary image.

Fig. 2: Histogram and encryption results of proposed image encryption algorithm: Girl gray and binary images.

TABLE II: Correlation coefficient comparison analysis of the proposed scheme with a conventional scheme: binary Girl image

Direction	Plaintext image	Ciphertext [4]	Ciphertext proposed
Horizontal Direction	0.9740	0.9347	-0.0110
Vertical Direction	0.9883	0.9526	-0.0313
Diagonal Direction	0.9580	0.9017	-0.0163

TABLE III: Entropy analysis.

Image Type	[4]	proposed
Gray Girl	7.2974	7.9976
Binary Girl	0.9487	7.9952

B. Entropy

The ultimate goal of an encryption algorithm is to present plaintext information in such a manner that is difficult to predict. The degree of uncertainty can be measured using entropy analysis. Entropy can be written as [9]:

$$\text{Entropy} = \sum_{i=0}^{\beta-1} p(\alpha_i) \times \log_2 \frac{1}{p(\alpha_i)}, \tag{4}$$

where β represents gray levels and $p(\alpha_i)$ is the probability of occurrence. Low entropy value indicates that encryption scheme might be predictable. Table III highlights entropy values of traditional and the proposed schemes. One can confirm from Table III that the proposed scheme has high entropy values.

C. Histogram Analysis

Histogram plots show the frequency of occurrence of pixels. For binary and grey scale images, the total number of intensity levels are 2 and 256, respectively. Histogram defines the number of pixels across each intensity value. A flat histogram highlights that the number of pixels is equally distributed among intensity values. Moreover, it also verifies that the occurrence probability of each pixel is equal. Due to the equal probability of occurrence, an intruder cannot deduct the frequency information [10]–[12]. Histogram plot of plaintext and ciphertext images are outlined in Figs. 1 and 2. From plots, one can see confirm that almost flat histogram is achieved after using proposed system while S-Box based encryption schemes have replaced plaintext image with other two values only.

D. Deviation from a uniform histogram

As outlined in the previous section, uniform histogram means each intensity value has the equal number of pixel values. A robust and strong encryption scheme must have a low deviation from the ideal histogram. Large deviation indicates that encrypted pixels are not distributed uniformly. Mathematically, deviation from the ideal uniform histogram is:

$$D = \frac{\sum\limits_{C_i=0}^{\beta-1} |H_{C_i} - H_C|}{M \times N}. \tag{5}$$

where H_{C_i} is histogram value at index i, H_C is the ideal value of histogram and $M \times N$ is image size. Results of deviation from uniform histogram are shown in Table IV. Table IV verifies that the proposed scheme has low deviation when compared to S-Box only scheme.

TABLE IV: Deviation from uniform histogram analysis.

Image Type	[4]	proposed
Gray Girl	0.7700	0.0467
Binary Girl	1.9844	0.0533

TABLE V: NPCR analysis.

Image Type	[4]	proposed
Gray Girl	0	98.0042
Binary Girl	0	34.8358

E. Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI)

The extent of change in the resultant ciphertext image by changing one bit in the original image is determined by NPCR. Let us consider two encrypted texts $E1$ and $E2$ which differ in one bit with respect to the original image. Let us define difference $D(i,j)$ where $D(i,j)$ = 0 if $E1(i,j) = E2(i,j)$ otherwise $D(i,j)$ = 1 and NPCR can be evaluated as [13]:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%. \tag{6}$$

A large value of NPCR depicts good encryption quality. NPCR focuses on absolute number of differences while Unified Average Change Intensity (UACI) calculates the intensity of dissimilarities between the two images and can be defined as [14]:

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{E_1(i,j) - E_2(i,j)}{\beta - 1} \right] \times 100\%. \tag{7}$$

Tables V and VI highlights NPCR and UACI results of traditional and proposed encrypted schemes, respectively. It can be seen from Tables V and VI S-Box only encryption completed failed in NPCR and UACI tests. Consequently, S-Box only method are not secure when one bit was changed. Moreover, Table V and VI also indicates that the proposed chaos-based scheme has significant higher NPCR and UACI.

F. Contrast Analysis

In contrast analysis, intensity difference of a pixel from its neighbouring pixels is computed. Mathematically [15]:

$$\text{Contrast} = \sum_{i,j=1}^{T} |i-j|^2 p(i,j), \tag{8}$$

where $p(i,j)$ is the number of gray-level co-occurrence. Low value of contrast indicates that encrypted pixel are least distinct

TABLE VI: Unified Average Change Intensity analysis.

Image Type	[4]	proposed
Gray Girl	0	32.8188
Binary Girl	0	11.6773

TABLE VII: Contrast analysis.

Image Type	[4]	proposed
Gray Girl	8.2618	10.5540
Binary Girl	0.5221	10.4042

from its neighbouring encrypted pixels. In encryption, a high value is always desired for security. Table VII reveals that techniques that uses only S-Box in their implementation give less contrast values as compared to the proposed scheme. Hence contrast result is also in favour of the proposed scheme.

IV. Conclusion

In this paper, we have analysed a traditional S-Box based image encryption algorithm. During security analysis, most results highlights that image encryption solely based on SBox are not secured. To address this issue, we have proposed a novel Intertwining and NCA-based image encryption scheme. The proposed scheme was tested against various security parameters. Correlation coefficient, entropy, histogram, deviation from uniform histogram, NPCR, UACI and contract analyses were applied on the encrypted images. Results obtained from the security parameters demonstrate that the proposed cryptosystem is highly resistant to various attacks.

References

[1] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[2] J. S. Khan, J. Ahmad, and M. A. Khan, "Td-ercs map-based confusion and diffusion of autocorrelated data," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 93–107, 2017.

[3] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel substitution box for encryption based on lorenz equations," in *Circuits, System and Simulation (ICCSS), 2017 International Conference on*, pp. 32–36, IEEE, 2017.

[4] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dynamics*, vol. 88, no. 4, pp. 2757–2769, 2017.

[5] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, "An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box," *Journal of Modern Optics*, vol. 64, no. 5, pp. 531–540, 2017.

[6] X. Wang and D. Xu, "Image encryption using genetic operators and intertwining logistic map," *Nonlinear Dynamics*, vol. 78, no. 4, pp. 2975–2984, 2014.

[7] I. S. Sam, P. Devaraj, and R. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.

[8] J. S. Khan, M. A. Khan, J. Ahmad, S. O. Hwang, and W. Ahmed, "An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes," *Informatica*, vol. 28, no. 4, pp. 629–649, 2017.

[9] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic s-boxes and chaotic maps," *3D Research*, vol. 7, no. 1, p. 7, 2016.

[10] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and xor operation," *Neural Computing and Applications*, pp. 1–11, 2017.

[11] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices," *Neural Computing and Applications*, vol. 28, no. 1, pp. 953–967, 2017.

[12] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on lorenz equation, gingerbreadman chaotic map and s 8 permutation," *Journal of Intelligent & Fuzzy Systems*, no. Preprint, pp. 1–13, 2017.

[13] J. S. Khan, A. ur Rehman, J. Ahmad, and Z. Habib, "A new chaos-based secure image encryption scheme using multiple substitution boxes," in *Information Assurance and Cyber Security (CIACS), 2015 Conference on*, pp. 16–21, IEEE, 2015.

[14] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and s-box," in *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*, pp. 1–6, IEEE, 2015.

[15] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, M. A. Khan, and S. O. Hwang, "A new technique for designing 8× 8 substitution box for image encryption applications," in *Computer Science and Electronic Engineering (CEEC), 2017*, pp. 7–12, IEEE, 2017.