Research Article

A Novel 1D Hybrid Chaotic Map-Based Image Compression and Encryption Using Compressed Sensing and Fibonacci-Lucas Transform

Tongfeng Zhang, Shouliang Li, Rongjun Ge, Min Yuan, and Yide Ma

School of Information Science and Engineering, Lanzhou University, Lanzhou, Gansu 730000, China

Correspondence should be addressed to Yide Ma; ydma@lzu.edu.cn

Received 31 December 2015; Revised 17 April 2016; Accepted 18 April 2016

Academic Editor: Zhen-Lai Han

Copyright © 2016 Tongfeng Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

A one-dimensional (1D) hybrid chaotic system is constructed by three different 1D chaotic maps in parallel-then-cascade fashion. The proposed chaotic map has larger key space and exhibits better uniform distribution property in some parametric range compared with existing 1D chaotic map. Meanwhile, with the combination of compressive sensing (CS) and Fibonacci-Lucas transform (FLT), a novel image compression and encryption scheme is proposed with the advantages of the 1D hybrid chaotic map. The whole encryption procedure includes compression by compressed sensing (CS), scrambling with FLT, and diffusion after linear scaling. Bernoulli measurement matrix in CS is generated by the proposed 1D hybrid chaotic map due to its excellent uniform distribution. To enhance the security and complexity, transform kernel of FLT varies in each permutation round according to the generated chaotic sequences. Further, the key streams used in the diffusion process depend on the chaotic map as well as plain image, which could resist chosen plaintext attack (CPA). Experimental results and security analyses demonstrate the validity of our scheme in terms of high security and robustness against noise attack and cropping attack.

1. Introduction

With the fascinating development of computer networks and multimedia communications during the past decades, a great demand for secure image transmission is increased. Image encryption is one of effective measures to prevent unauthorized access to images [1, 2]. Since the introduction of chaos theory to cryptography and the proposal of permutation and diffusion structure by Matthews [3] and Fridrich [4], respectively, Chaos-based encryption algorithms have received remarkable attentions [5–9] for the reason that some typical features of chaos, including ergodicity, sensitivity to initial condition, and random-like behavior, can be well connected with some conventional cryptographic properties such as confusion and diffusion [10]. Chen et al. [5] have proposed an image encryption algorithm which employs the three-dimensional cat map to shuffle the positions of the image pixels and uses another chaotic map to confuse the relationship between the encrypted and its original image. Huang [6] has designed pseudorandom chaotic sequence with the created secret keys depending on each other and used a two-dimensional Chebyshev map in diffusion process. In [7], Pareek et al. have proposed a new approach for image encryption based on chaotic Logistic maps. An external secret key of 80-bit length and two chaotic Logistic maps are employed. Gao and Chen [8] presented a new image encryption scheme which employs an image total shuffling matrix to shuffle the positions of image pixels and then uses a hyperchaotic system to confuse the relationship between the plain image and the cipher image. A symmetric block cipher based on the improved standard map was derived by Lian et al. [9]. Permutation and diffusion structure are usually adopted in the cryptosystems mentioned above, which suggests iterating the permutation and diffusion stage several rounds to earn good confusion and diffusion effect, whereas the permutation in those cryptosystem is almost the same in each round and independent of plain image.

The chaotic system utilized in the cryptosystem often could be divided into one-dimensional (1D) chaos and high dimensional (HD) chaos [11]. 1D chaos such as Logistic
map [12] and Tent map [13, 14] has fast computational
performance while HD chaotic systems like Lorenz system
[15], hyperchaos [16], and chaotic standard map [17] have
large parametric space and high security. 1D chaotic maps
often have simple structures and are easy to implement. But
their intrinsic weakness such as small key space and weak
security enables image encryption algorithm feasible to be
attacked. To overcome those limitations, some improvements
on 1D chaotic system have been carried out. Mazloom
and Eftekhari-Moghadam [18] introduce a kind of coupled
nonlinear chaotic map to color image encryption. Zhou et
al. used a combination of two existing 1D chaotic maps to
generate two new 1D chaotic maps in series and parallel in
the literature [19] and [20], respectively, where the former has
two parameters but weak uniform distribution property and
the latter shows good uniform distribution property but has
only one parameter essentially.

Recently, some researchers proposed a kind of compres-
sion-combined encryption method based on compressive
sensing (CS) [21–27]. CS includes sparse representation,
linear measurement, and reconstruction processes. An image
compression-encryption scheme is proposed in [21], which
combines 2D compressive sensing with nonlinear fractional
Mellin transform. The literature [23] proposes a double-
image encryption compression scheme. The major core of
the encryption system is that two circular matrices and the
measurement matrix utilized in compressive sensing are designed
by using a two-dimensional Sine Logistic modulation map.
Liu et al. [25] present a combined compressive sensing and
optical image encryption method using double random
phase encoding-based block compressive sensing. These CS-
based image encryption methods could achieve satisfactory
security performance except for the resistance of differentia-
attack due to the absence of diffusion process. Zhang et al.
[27] apply the encryption and compression scheme into the
field of medical images. The novelties of their work lie in that
Bernoulli measurement matrix in CS is constructed by using
Chebyshev map and quantized measurements by max-Lloyd
are encrypted in diffusion phase.

Presently, we aim to design a novel 1D hybrid chaotic map
which possesses large key space and satisfies uniform distri-
bution property. Meanwhile, CS-combined with Fibonacci-
Lucas transform image encryption is put forward based on
the proposed 1D chaotic map. Bernoulli measurement matrix
in CS is derived by the 1D chaotic map. Permutation phase
is fulfilled by Fibonacci-Lucas transform, whose transform
kernel could be controlled by the hybrid 1D chaotic map. Fur-
thermore, a linear scaling on the measurement data is taken

\[
x_{n+1} = \begin{cases} 
\text{mod}(a \sin(\pi \mu x_n) + \gamma \mu x_n (1 - \mu x_n), 1) & 0 \leq x_n \leq 0.5 \\
\mu (1 - x_n) & 0.5 < x_n \leq 1 
\end{cases}
\]

where \(a\) and \(\gamma\) are its control parameters, and the three
chaotic output sequences \(x_n\) all fall within \([0, 1]\). It is obvious
that there are three different combinations for choice of
\(F(\cdot, \cdot), G(\cdot, \cdot),\) and \(H(\cdot, \cdot)\) in (1). As an example, \(F(\cdot, \cdot), G(\cdot, \cdot),\) and \(H(\cdot, \cdot)\) take the forms of Logistic map, Tent map, and Sine
map, respectively. Correspondingly, (1) can be rewritten as

\[
x_{n+1} = \begin{cases} 
\text{mod}(a \sin(\mu x_n) + \gamma x_n (1 - \mu x_n), 1) & 0 \leq x_n \leq 0.5 \\
\mu (1 - x_n) & 0.5 < x_n \leq 1 
\end{cases}
\]

The chaotic behavior of the proposed 1D map is investi-
gated by the ways of Lyapunov exponent (LE) and bifurcation
diagram. Although our 1D map cannot exhibit good chaotic

into consideration to accomplish diffusion operation. The
contributions of this work are as follows: firstly, a 1D hybrid
chaotic map is constructed; secondly, the proposed chaotic
map shows good uniform distribution and could constitute
the Bernoulli measurement matrix in CS, thus reducing the
cost of transmission and improving image recovery quality;
thirdly, Fibonacci-Lucas transform is utilized to accomplish
block scrambling, whose transform kernel is different from
each other in each permutation round; finally, the diffusion
operation related to plaintext is carried out after a linear scal-
ing of the measurements. The proposed method is described
in detail in Section 2. Section 3 presents the simulated results
and security analyses. The conclusion is drawn in Section 4.

2. Proposed Method

2.1. One-Dimensional (1D) Hybrid Chaotic Map. The pro-
posed 1D chaotic map is fulfilled by hybrid structures includ-
ing both series and parallel, as shown in Figure 1. It is a
nonlinear combination of three different 1D chaotic maps
which are considered as seed maps [18, 19]. The system is
defined by the following equation:

\[
x_{n+1} = (F(b, G(a, x_n)) + H(c, G(a, x_n))) \mod 1, \quad (1)
\]

where \(G(a, x_n), F(b, x_n),\) and \(H(c, x_n)\) are three 1D chaotic
maps (seed maps) with parameters \(a, b,\) and \(c;\) mod is modulo
operation; and \(n\) is the iteration number. The three chaotic
maps \(G(a, x_n), F(b, x_n),\) and \(H(c, x_n)\) can be chosen from
among the Tent map, Logistic map, and Sine map, who are
defined by (2a)–(2c), respectively,

\[
x_{n+1} = T(\mu, x_n) = \begin{cases} 
\mu x_n & 0 \leq x_n \leq 0.5 \\
\mu (1 - x_n) & 0.5 < x_n \leq 1 
\end{cases}, \quad (2a)
\]

\[
x_{n+1} = L(\gamma, x_n) = \gamma x_n (1 - x_n), \quad (2b)
\]

\[
x_{n+1} = S(\alpha, x_n) = \alpha \sin(\pi x_n), \quad (2c)
\]

where \(T(\cdot, \cdot), L(\cdot, \cdot),\) and \(S(\cdot, \cdot)\) represent the Tent map, Logistic
map, and Sine map, respectively, \(\mu \in (0, 2], \gamma \in (0, 4],\)
and \(a \in (0, 1]\) are their control parameters, and the three
chaotic output sequences \(x_n\) all fall within \([0, 1]\). It is obvious
that there are three different combinations for choice of
\(F(\cdot, \cdot), G(\cdot, \cdot),\) and \(H(\cdot, \cdot)\) in (1). As an example, \(F(\cdot, \cdot), G(\cdot, \cdot),\)
and \(H(\cdot, \cdot)\) take the forms of Logistic map, Tent map, and Sine
map, respectively. Correspondingly, (1) can be rewritten as
the dynamics about the chaotic map in the scope of $\mu \in [0.5 \ 0.9]$, $a \in [0.975 \ 0.995]$, and $y \in [1.19]$ is considered. The LE is numerically calculated and plotted in Figure 2. Figures 2(a)–2(c) show the 2D LEs versus parameter couples $(a, \mu)$, $(a, y)$, and $(\mu, y)$, respectively. As shown in Figure 2, the LEs are all positive in the three subplots, indicating the chaotic behavior of the proposed map for $\mu \in [0.5 \ 0.9]$, $a \in [0.975 \ 0.995]$, and $y \in [1.19]$. Further, the bifurcation diagrams with different parameters could be utilized to examine the distribution property of the chaotic series. Figures 3(a)–3(c) are the ID bifurcation diagrams with different parameters $a, \mu$, and $y$. It can be obviously seen from Figure 3 that the chaotic sequences traverse the interval $[0.975 \ 0.995]$.

$a(c)$ are the 1D bifurcation diagrams with different parameters $\gamma$. Further, the bifurcation diagrams versus parameter pairs $(a, \gamma)$, $(a, \mu)$, and $(\mu, \gamma)$, respectively. As shown in Figure 2, the LEs are all positive in the three subplots, indicating the chaotic behavior of the proposed map for $\mu \in [0.5 \ 0.9]$, $a \in [0.975 \ 0.995]$, and $y \in [1.19]$. Further, the bifurcation diagrams with different parameters could be utilized to examine the distribution property of the chaotic series. Figures 3(a)–3(c) are the ID bifurcation diagrams with different parameters $a, \mu$, and $y$. It can be obviously seen from Figure 3 that the chaotic sequences traverse the interval $[0.975 \ 0.995]$. Hence, it could be sure that the proposed 1D chaotic map possesses excellent chaotic property in terms of uniform distribution and has relatively large parametric space, which can be suitable for the field of image encryption.

2.2. Compressed Sensing Theory. The CS is a new framework for simultaneous sampling and compression of signals [28]. As for CS theory, a 1D sparse signal $x$ with length $N$ can be represented as

$$x = \sum_{i=1}^{N} \alpha_i \Psi_i = \Psi \alpha, \quad (4)$$

where $\alpha$ is the column vector of weighting coefficients and $\Psi = [\Psi_1, \Psi_2, \ldots, \Psi_N]$ is an $N \times N$ orthogonal basis matrix. $x$ and $\alpha$ are equivalent representations of the signal, with $x$ in the time or space domain and $\alpha$ in the $\Psi$ domain. If only $K$ of the $\alpha$ coefficients in (4) is nonzero, where $K \ll N$, $x$ is termed as $K$ sparse signal [29]. In CS process, an $M \times N$ measurement matrix $\Phi$ incoherent with $\Psi$ is used to obtain a nonadaptive linear map if signal $x$ is compressible. The measurement process is

$$y = \Phi x = \Phi \Psi \alpha = \Theta \alpha, \quad (5)$$

where $y$ is an $M \times 1$ vector; the sensor matrix $\Theta$ is the product of $\Phi$ and $\Psi$. To reconstruct the signal correctly, the sensor matrix $\Theta$ should satisfy restricted isometry property (RIP) [29]. To satisfy the RIP condition, Gaussian random matrix, partial Hadamard matrix, random circular matrix, or Bernoulli matrix can be selected as the stable measurement matrix. In our scheme, Bernoulli matrix serves as measure matrix and could be equivalently constructed by the proposed 1D chaotic map (3) due to its good uniform distribution property as follows:

$$\Phi(i,j) = \begin{cases} 
1 & \text{if } x_n \geq 0.5 \\
-1 & \text{if } x_n < 0.5,
\end{cases} \quad (6)$$

where $\Phi(i,j)$ and $x_n$ represent the entry of the $M \times N$ Bernoulli measure matrix and the iterative chaotic series of (3), $n = (i - 1) * N + j, \ i = 1,2, \ldots, M$ and $j = 1,2, \ldots, N$.

To recover $x$ from $y$, the reconstruction can be proceeded by solving the following $l_1$-norm minimization problem:

$$\tilde{\alpha} = \arg \min_{\alpha} \|\alpha\|_1 \quad \text{s.t. } \Theta \alpha = y. \quad (7)$$

Some reconstruction algorithms, such as orthogonal matching pursuit (OMP) [30] and Bregman iterative algorithm [31], are effective in reconstructing the signal from the encrypted result. Here Bregman iterative algorithm is adopted to recover the images.

2.3. Fibonacci-Lucas Transform. In our image encryption, Fibonacci-Lucas transform (FLT) is used to operate image scrambling.

Definition 1 (see [32]). The Fibonacci-Lucas transform can be defined as the mapping $F_{\ell} : T^2 \rightarrow T^2$ such that

$$\left[ \begin{array}{c} i' \\ j' \end{array} \right] = \left[ \begin{array}{cc} F_n & F_{n+1} \\ L_n & L_{n+1} \end{array} \right] \left[ \begin{array}{c} i \\ j \end{array} \right] \mod N, \quad (8)$$

where $(i,j), (i',j') \in \{0,1,\ldots,N-1\}$ and $N$ is the size of a digital image; $F_n$ and $L_n$ are Fibonacci series and Lucas series and can be described by

$$F_n = \begin{cases} 
1 & n = 1 \\
1 & n = 2 \\
F_{n-1} + F_{n-2} & n \geq 3,
\end{cases} \quad (9)$$

$$L_n = \begin{cases} 
1 & n = 1 \\
1 & n = 2 \\
L_{n-1} + L_{n-2} & n \geq 3,
\end{cases} \quad (10)$$

respectively.

It is clear that $L_n = F_n + F_{n-2}$ holds when $n \geq 3$. Hence, the transform kernel in formula (8) is turned into (11) as follows:

$$F_{\ell n} = \left[ \begin{array}{cc} F_n & F_{n+1} \\ F_n + F_{n-2} & F_{n+1} + F_{n-1} \end{array} \right]. \quad (11)$$

And the corresponding inverse transform of FLT is as

$$F_{\ell n}^{-1} = \left[ \begin{array}{cc} (F_{n+1} - F_{n-1}) \ast (-1)^n F_{n+1} & (F_{n+1} - F_{n-1}) \ast (-1)^{n+1} \\ (F_n + F_{n-2}) \ast (-1)^{n+1} F_n & (F_n + F_{n-2}) \ast (-1)^n \end{array} \right]. \quad (12)$$
The series $\text{FLT}_n$ form infinitely many transforms. Note that all of these transforms will be periodic in nature with a maximum possible periodicity of $N^2 - 1$ and will produce different scrambling patterns from each other [32]. Hence, we can select different transform matrix at each round permutation for consideration of high security level. It is also noted that Fibonacci-Lucas transform is only suitable to square matrices. As for rectangular matrices, we can take some measures to apply Fibonacci-Lucas transform to them. Suppose that the size of image is $M \times N$ and $m$ is the greatest common divisor (g.c.d.) of $M$ and $N$; then the image is divided into $m^2$ blocks with size of $M/m \times N/m$ and we can perform the transform on the $m \times m$ square matrix to alter the position of each block.

2.4. Encryption Procedure. The flow chart of proposed image encryption method using compressive sensing and Fibonacci-Lucas transform is shown in Figure 4. In our approach, the original image with size of $N \times N$ is firstly encrypted through CS; then the generated data is divided into $m^2$ blocks, where $m$ is the g.c.d. of $M$ and $N$. The positions of $m^2$ blocks are modified by FLT. Lastly, the scrambled image is diffused with plaintext-related keys after a linear scaling. The detailed encryption steps are as follows.

Step 1. Perform discrete wavelet transform on the plain image $P$ to get the coefficients matrix $A$.

Step 2. Iterate (3) with $(\mu, \gamma, a, x_0)$ for $2 \times M \times N + N_0$ times, where $N_0$ is constant. The first $N_0$ values are discarded due to the transient effect and we can obtain the sequence $X = (x_1, x_2, \ldots, x_{2MN})$ with length of $2MN$. The measurement matrix $\Phi$ is constructed according to

$$\Phi (i, j) = \begin{cases} 1 & x(n) \geq 0.5 \\ -1 & x(n) < 0.5, \end{cases}$$

where $n = (i - 1) \times N + j$, $i = 1, 2, \ldots, M$ and $j = 1, 2, \ldots, N$.

Step 3. Compressively sample the coefficients according to $Y = \Phi A$.

Step 4. Calculate the greatest common divisor $m$ of $M$ and $N$, then divide $Y$ into $m^2$ blocks, and scramble them for $num$
rounds using (14) to obtain $Y'$. That is to say, the $(i, j)$ block is permuted to the position $(i', j')$ every time by

$$
\begin{bmatrix}
i' \\
j'
\end{bmatrix} = 
\begin{bmatrix}
F_n & F_{n+1} \\
F_n + F_{n-2} & F_{n+1} + F_{n-1}
\end{bmatrix}
\begin{bmatrix}
i \\
j
\end{bmatrix} \mod m, \quad (14)
$$

where $i, j \in \{0, 1, \ldots, m - 1\}$. The value of $n$ in the $k$th FLT transform, denoted by $n_k$, is determined by $n_k = \text{mod}(\text{floor}(X(MN + 1 - k)) \times 10^{15}, 5) + 3$.

**Step 5.** Carry on a linear scaling on $Y'$. In general, the data of $Y'$ exceed the range of $[0, 255]$. As a simple and effective method, a linear map is considered here. Find the maximum and minimum value from $Y'$ represented by max and min and map them to 255 and 0, respectively. Let $\text{coff} a = 255 / (\text{max} - \text{min})$ and $\text{coff} b = 255 \times (\text{min} / (\text{min} - \text{max})$ and then $Y'$ is turned into $Y''$ as

$$
Y''(i, j) = \text{coff} a \times Y'(i, j) + \text{coff} b. \quad (15)
$$

Then convert $Y''$ into 1D array $p$.

**Step 6.** Perform diffusion process. In order to resist known plaintext attack and chosen plaintext attack, the diffusion

---

**Figure 4:** Flow chart of the proposed cryptosystem.

**Figure 3:** Bifurcation diagram of the proposed 1D chaotic map: (a–c) are 1D bifurcation diagrams versus $a$, $\gamma$, and $\mu$, respectively.
method proposed in the literature \[33\] is adopted, whose details are described as follows:

(I) Obtain the key stream \(k_i\) from \(x_i\) in Step 2 according to

\[
k_i = \text{mod} \left( \text{floor} \left( x_i \ast 2^{15} \right), 256 \right).
\]

(II) Conventional diffusion process is carried out to calculate the cipher-pixel value by

\[
c_i = c_{i-1} \oplus k_i \oplus \text{mod} (p_i + k_0, 256),
\]

where \(p_i\) and \(c_i\) are the currently operated pixel and output pixel, respectively; \(c_{i-1}\) is the previous cipher-pixel, and \(c_0\) is the initial value and may serve as secret key.

(III) Calculate \(t\) according to

\[
t = 1 + \text{mod} \left( c_i, 2 \right).
\]

Then, let \(x_i = x_{i+t}\) and return to step (I) until all output pixels are obtained.

*Step 7.* Execute Step 6 once again to achieve satisfactory performance and reshape the sequence \(c\) to get the final ciphered image \(C\).

Decryption is the inverse process of encryption, whose steps mainly include the following.

*Step 8.* Perform inverse diffusion according to

\[
p_i = \text{mod} \left( c_i \oplus k_i \oplus c_{i-1} - k_0, 256 \right).
\]

*Step 9.* An opposite linear scaling is carried out by

\[
Y' = \frac{(Y'' - \text{coff} b)}{\text{coff} a}.
\]

*Step 10.* Inverse Fibonacci-Lucas transform is performed by

\[
\text{IFLT}_n = \begin{bmatrix} (F_{n+1} + F_{n-1}) \ast (-1)^n & F_{n+1} \ast (-1)^{n+1} \\ (F_n + F_{n-2}) \ast (-1)^{n+1} & F_n \ast (-1)^n \end{bmatrix}.
\]

*Step 11.* The original plain image is recovered by Bregman iterative algorithm.

### 3. Simulated Results and Analyses

In this section, some simulations and performance evaluation including key space, key sensitivity, statistics analysis, differential attack, and robustness to noise attack are discussed. And all the tests in this paper are conducted under MATLAB 7.11.0 (R2010b) on a laptop with the Windows 7 operating system of 64-bit, Intel(R) Core(TM) i7-4790 CPU @ 3.20 GHz, and 4 GB RAM.

#### 3.1. Experimental Results

The gray images Lena and Cameraman with the size of 256 \(\times\) 256 and Baboon and Boat with the size of 512 \(\times\) 512 serve as test images. The DWT matrix is adopted as the basis matrix \(\Psi\). Bregman iterative algorithm is utilized to implement reconstruction. The parameters in the proposed 1D chaotic map are taken as \(a = 0.985\), \(\mu = 0.503\), and \(\gamma = 1.6\). The rounds \(num\) of FLT and the initial \(c_0\) are set to be 3 and 123, respectively. The compression ratio \(M/N\) is set to be 0.75. The experimental results of the four test images Lena, Cameraman, Baboon, and Boat are shown in Figure 5, where the first column, second column, and third column represent plain images, ciphered images, and decrypted images, respectively. It can be seen from Figure 5 that the ciphered images are well decrypted visually, indicating the validity of our scheme. In order to quantify the recovery quality, the peak signal to noise ratio (PSNR) value of the reconstructed image with the corresponding original image is considered here. The PSNR for an \(m \times n\) image can be calculated as

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255 \times 255}{\text{MSE}} \right),
\]

where MSE denotes mean square error and is expressed by

\[
\text{MSE} = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (X(i, j) - Y(i, j))^2,
\]

where \(X(i, j)\) and \(Y(i, j)\) represent the corresponding pixel values of the original and reconstructed images, respectively.

The PSNR versus the compression rate for the test images Lena with size of 256 \(\times\) 256 is plotted in Figure 6, where the size \(M\) of measurement matrix varies from 32 to 224 with step of 32. It is clear from Figure 6 that our scheme could achieve satisfactory recovery performance. Further, the methods with original Bernoulli measurement matrix and the one generated by Chebyshev chaotic map in [27] are also listed for the purpose of comparison with the one generated by the proposed chaotic map. Obviously, the recovery performance by our chaotic map almost approaches the one by Bernoulli random matrix and exceeds the one by Chebyshev chaotic map, whereas our method could achieve higher transmission efficiency in contrast to the original Bernoulli and has larger key space compared to Chebyshev chaotic map.

#### 3.2. Key Space and Key Sensitivity

The key space of a good encryption scheme should be large enough to resist the brute-force attack. As described above, the keys in our cryptosystem are comprised of the parameters \(\mu, a, \gamma\), initial \(x_0\) in the proposed 1D chaotic map, and \(c_0\) in the diffusion. The three control parameters \(\mu, a, \gamma\) take values in range of \([0.502, 0.504], [0.984, 0.986],\) and \([1.59, 1.61]\) and the practical key space approaches \(0.002 \ast 0.002 \ast 0.02 \ast 10^{10} \ast 256 = 1.67 \ast 2^{183}\) if the precision reaches \(10^{-15}\), which is enough to prevent the exhaustive searching. Thus, brute-force attack on the keys is computationally infeasible.

An efficient encryption algorithm should also be sensitive to secret keys. It means a very small change in the key will
cause a greatly significant change in the output, which is the guarantee of security. In the experiments, we make a slight change in the values of the keys $\mu$, $a$, and $\gamma$ and then try to encrypt and reconstruct the images. First, the key sensitivity to encryption is analyzed. The different keys with $+10^{-15}$ deviation to original ones are used to encrypt the original Lena image. The corresponding results are presented in Figure 7, where (a) is original Lena image, (b) is encrypted image, (c), (e), and (g) denote the encrypted images with incorrect keys $a = 0.985 + 10^{-15}$, $\mu = 0.503 + 10^{-15}$, and $\gamma = 1.6 + 10^{-15}$, respectively, (d), (f), and (h) denote the differential images between (c) and (b), (e) and (b), and (g) and (b), respectively. From (d), (f), and (h), we can see a great amount of changes happening due to the slight variation of encryption keys, which demonstrates that the keys are highly sensitive to encryption. Further, a group of key sensitivity tests for decryption are executed on Lena and Cameraman. The wrong keys with $\pm 10^{-15}$ deviation to original ones in encryption are taken to decrypt the cipher images, as shown in Figure 8. The deviations to the values of $\mu$, $a$, and $\gamma$ are $+10^{-15}$ and $-10^{-15}$ in (a1)–(a4) and (b1)–(b4), respectively. It is obvious from Figure 8 that the decrypted images cannot provide any useful information visually. As is illustrated, the proposed cryptosystem is also highly sensitive to the keys.
8 Mathematical Problems in Engineering

Bernoulli constructed by the proposed chaotic map

Original Bernoulli

Figure 6: Performance curves of PSNR with different compression ratios.

3.3. Statistical Analysis. In this subsection, statistical analysis is carried out in terms of histogram and correlation between two adjacent pixels of images.

Histogram is an important statistical feature of the images, which is often used to evaluate the performance of image encryption schemes. An encryption scheme should have the ability to transform an original image into a random-like encrypted image with relatively low correlations among neighborhood pixels. The histograms of original images and corresponding ciphered images are shown in Figure 9. From top to bottom are histograms of Lena, Cameraman, Baboon, and Boat. The left column represents the results of original image and the right column represents the corresponding results of ciphered ones. From Figure 9, one can almost see the frequency of each gray level from the histograms of original images, which can expose image information, whereas the histograms of the corresponding encrypted ones are fairly uniform in distribution. Thus, it can be said that the proposed algorithm could homogenize the original image and resist statistical attack.

The correlation coefficient of the adjacent pixels is also an important statistical feature of images. In general, there is a strong correlation between adjacent pixels in a meaningful image. The correlation coefficient \( \rho_{xy} \) between two adjacent pixels can be described as

\[
\rho_{xy} = \frac{E[(x - E(x))(y - E(y))]}{\sqrt{D(x)}\sqrt{D(y)}},
\]

where \( E(x) = (1/l)\sum_{i=1}^{l} x_i \), \( D(x) = (1/l)\sum_{i=1}^{l}(x_i - E(x))^2 \), and \( l \) is the number of total pixels.

We randomly select 2000 pairs of adjacent pixels from original image and encrypted image in horizontal, vertical, and diagonal direction, respectively. The correlation coefficients of two adjacent pixels in the original image and encrypted image in Figure 5 are listed in Table 1. Table 1 shows that the correlation among pixels in ciphered images in each direction reduces to a lower level comparing with the original image.

Further, the correlation distribution can also reveal the correlation between two adjacent pixels intuitively. Regular distribution means strong correlation while dispersed distribution means weak correlation. As an example, the correlation distributions of two adjacent pixels in different directions for original Boat and ciphered one are plotted in Figure 10. It can be seen that the correlation distribution of the cipher image performs much more dispersed property in each direction than the one of plain image. Hence, the proposed scheme could remove the tight relationship between adjacent pixels of the original image successfully. The results demonstrate that the proposed scheme can resist statistical analysis since the attackers cannot obtain useful information.

3.4. Information Entropy. Shannon [34] introduces the entropy in information theory as information entropy (IFE) to describe the information redundancy associated with feature of randomness. In an image encryption system, IFE can reflect the information redundancy of an image, defined as

\[
H(I) = \sum_{l=0}^{2^N-1} p(l) \log \frac{1}{p(l)},
\]

where \( l \) is the gray/color level within \( 2^N \) levels with \( N \) bits.

It is well-known that the larger the IFE is, the more randomness the image performs. For 256-level gray image the maximum value of IFE can reach 8. The IFEs of the original images and the encrypted images in Figure 5 are numerically calculated and listed in Table 2. It can be found that the IFEs of the four images after encryption are all close to 8. Hence, the probability for the proposed cryptosystem to divulge information is very little.

3.5. Resistance to Differential Attack. Attackers often make a tiny change in the original image and then use the proposed algorithm to encrypt the original image before and after modification, to find out the relation between the original image and the ciphered image, that is, the differential attack.
Figure 7: Results of key sensitivity test in encryption: (a) original Lena and (b) encrypted image and (c), (e), and (g) denote the encrypted images with incorrect keys $a = 0.985 + 10^{-15}$, $\mu = 0.503 + 10^{-15}$, and $\gamma = 1.6 + 10^{-15}$, respectively, and (d), (f), and (h) denote the differential images between (c) and (b), (e) and (b), and (g) and (b), respectively.

Table 2: IFEs of plain images and corresponding ciphered images.

<table>
<thead>
<tr>
<th>Information entropy</th>
<th>Lena</th>
<th>Cameraman</th>
<th>Baboon</th>
<th>Boat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain image</td>
<td>7.0542</td>
<td>7.0097</td>
<td>7.1579</td>
<td>7.1238</td>
</tr>
<tr>
<td>Ciphered image</td>
<td>7.9957</td>
<td>7.9966</td>
<td>7.9991</td>
<td>7.9991</td>
</tr>
</tbody>
</table>

In order to examine the performance of resisting differential attack, the number of pixels’ change rate (NPCR) and the unified average changing intensity (UACI) are calculated. If a tiny modification in original image can cause a significant change in encrypted image, the differential attack would be considered invalid. Let $I_1(i, j)$ and $I_2(i, j)$ denote the pixels located at $(i, j)$ in encrypted images $I_1$ and $I_2$ with the size of $m \times n$. Then the NPCR and UACI are defined as

\[
\text{NPCR} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} D(i, j)}{m \times n} \times 100\%,
\]

\[
D(i, j) = \begin{cases} 
1, & I_{e1}(i, j) \neq I_{e2}(i, j) \\
0, & I_{e1}(i, j) = I_{e2}(i, j)
\end{cases}
\]

\[
\text{UACI} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left| I_{e1}(i, j) - I_{e2}(i, j) \right| / 255}{m \times n} \times 100\%.
\]

We randomly select a pixel $I(i, j)$ from the original image and modify it through bitwise exclusive with 1, that is, $I(i, j) = I(i, j) \oplus 1$, and thus get another modified image. Note that there is only one bit difference between the original and modified one. After the four images are encrypted by our encryption scheme, the NPCR and UACI could be calculated. The corresponding results for the four original images in Figure 5 are shown in Table 3. We have found that UACI and NPCR are over 33.4% and 99.6% after two round diffusions. Hence, our encryption scheme has excellent performance in terms of resistance to differential attack.

3.6. Robustness

3.6.1. Noise Attack. It is unavoidable that the encrypted image could be contaminated by the noise during transmission and
Figure 8: Results of key sensitivity test on plain image Cameraman (a1) and Lena (b1) and (a2)–(a4) denote the decrypted images for Cameraman with wrong keys $\alpha = 0.985 + 10^{-15}$, $\mu = 0.503 + 10^{-15}$, and $\gamma = 1.6 + 10^{-15}$ and (b2)–(b4) denote the decrypted images for Lena with wrong keys $\alpha = 0.985 - 10^{-15}$, $\mu = 0.503 - 10^{-15}$, and $\gamma = 1.6 - 10^{-15}$, respectively.
Figure 9: Histograms of original images and the encrypted images. From top to bottom are histograms of Lena, Cameraman, Baboon, and Boat. The left column represents the result of original image and the right column represents the corresponding result of encrypted image.

processing. So the robustness of the proposed encryption scheme against noise attack is considered here. Suppose that the noise impacts the cipher image in the following way:

\[ C' = C + \sigma G, \]

where \( C' \) and \( C \) are the noisy encrypted image and the uncontaminated encrypted image, respectively, \( \sigma \) is the noise intensity and \( G \) is the white Gaussian noise with zero-mean and the standard deviation of 1. The decrypted results for Lena contaminated by different noise intensity are shown in Figures 11(a)–11(c). The decrypted images reserve the overall information of the original images and can be recognized...
Figure 10: Correlation distribution of two adjacent pixels in horizontal direction of (a1) original Boat and (b1) ciphered one, in vertical direction of (a2) original Boat and (b2) ciphered one, and in diagonal direction of (a3) original Boat and (b3) ciphered one.
3.6.2. Cropping Attack. The robustness of a cryptosystem against cropping attack is also required in image transmission. In general, the occlusion of the cipher can affect the decrypted images greatly. The encrypted Lena images with three different occlusions of 0.39%, 0.88%, and 1.20% are shown in Figures 12(a1), 12(a2), and 12(a3), respectively, and the corresponding decrypted images are displayed in Figures 12(b1), 12(b2), and 12(b3), respectively. The two original images can be recognized from the decrypted images (b1) and (b2). But it is blurry in (b3). Thus the proposed encryption scheme could resist cropping attack to a certain degree.

![Figure 11: Results of robustness test on noise attack: decrypted image for Lena with noise intensity (a) $\sigma = 0.2$, (b) $\sigma = 0.3$, and (c) $\sigma = 0.4$.](image1)

![Figure 12: Results of robustness test on cropping attack: (a1) 0.39% occlusion, (a2) 0.88% occlusion, and (a3) 1.20% occlusion, (b1)–(b3) are the corresponding decrypted images from (a1)–(a3), respectively.](image2)

### Table 3: UACI and NPCR.

<table>
<thead>
<tr>
<th>Test image</th>
<th>UACI (%)</th>
<th>NPCR (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>33.6125</td>
<td>99.6989</td>
</tr>
<tr>
<td>Cameraman</td>
<td>33.5663</td>
<td>99.6181</td>
</tr>
<tr>
<td>Baboon</td>
<td>33.4724</td>
<td>99.6450</td>
</tr>
<tr>
<td>Boat</td>
<td>33.4189</td>
<td>99.6002</td>
</tr>
</tbody>
</table>

visually, which demonstrates that our scheme has the ability of resisting noise attack to some extent.
3.7. Encryption Speed. Except for security analyses, the encryption speed is also important in image encryption. Actually, the encryption time depends on the factors such as programming environment and computer configurations. Thus the running speeds cannot be compared directly. In our scheme, three measures are taken to improve the running speed. The first one is to employ Bregman iterative reconstruction algorithm to reduce the time cost. The second one is to perform a simple linear scaling on the measurement data instead of max-Lloyd quantization. The last one is that block FLT is utilized to implement the scrambling. All the measures can help to improve the running speed effectively. In this paper, the proposed method is simulated via MATLAB 7.11.0 (R2010b) on a laptop with the Windows 7 operating system of 64-bit, Intel(R) Core(TM) i7-4790 CPU @ 3.20 GHz, and 4 GB RAM. The encrypted time is approximately 6.23 seconds and 40.45 seconds for the 256*256 and 512*512 gray images, respectively.

4. Conclusion

A kind of combined CS and FLT image encryption scheme is proposed based on a novel ID hybrid chaotic map. The constructed chaotic map exhibits better uniform distribution and has larger key space than existing ID chaotic map. In our method, Bernoulli measurement matrix generated by the proposed chaotic map exhibits comparatively high recovery quality. Meanwhile, FLT with variable transform kernel in each permutation round is utilized to scramble the sampling image. Further, a simple but effective linear scaling on measure data is taken into consideration before diffusion. Due to the large key space, complexity of permutation, and plaintext-related diffusion, the proposed encryption scheme can resist brute attack, statistical attack, and differential attack. Simulation results show the validity of our scheme in terms of high security and robustness against noise attack and cropping attack.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

This work was partially supported by National Natural Science Foundation of China (nos. 61175012 and 6120422), Natural Science Foundation of Gansu Province (no. 1208RJZA265), and Specialized Research Fund for the Doctoral Program of Higher Education of China (no. 201102111-0026).

References

[21] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing
and fractional Mellin transform,” *Optics Communications*, vol. 343, pp. 10–21, 2015.


