A novel noise resistant image encryption scheme

Vivek Kumar and Vineet Malik

Course: CS461 - Computer Graphics

Instructor: Amal Dev Parakkat

IIT Guwahati

Abstract

We are proposing a new image encryption scheme with a permutation phase to the 1-DCF-IES resulting in super enhanced security as well as noise resistance. A new real one-dimensional cosine fractional (1-DCF) chaotic map was proposed in (TWT20) and the 1-DCF map was used to design a permutation-less image encryption scheme for real-time encryption applications. Our proposed encryption scheme uses same chaotic map with an additional permutation phase.

Contents

1 Introduction

Nowadays, users process, save and share a large number of digital images through communication networks. As a consequence, some security and privacy issues have been prompted where an unauthorized person can easily listen to private communications and access some secret information. Such scenarios can be catastrophic for the images' owners. For example, unauthorized access to military information, bank accounts records, sensitive medical reports. Thus, ensuring the privacy of the images is an important issue that became the main focus of a large security researcher community. Unlike texts, digital images cannot be encrypted using classical cryptography algorithms due to their distinct features, such as the bulkiest size, higher information redundancy, and stronger correlation. Considering these unique features, security researchers proposed several image encryption schemes based on multiple approaches and theories, such as chaos theory (TWM20; ACP19; EAF16; LWC17; LM18), DNA encoding, quantum theory, optical systems. Among these theories, chaos theory is the most popular thanks to its unique features like ergodicity, high sensitivity to the initial conditions, unpredictability, random-like behavior, etc. These features perfectly respond to cryptography needs.

2 Foundations

2.1 Chaotic Systems

A chaotic system is defined as one that is highly sensitive to initial conditions. These type of systems exhibit deterministic chaos which can be summarized as: When the present determines the future, but the approximate present does not approximately determine the future. Small differences in initial conditions, such as those due to errors in measurements or due to rounding errors in numerical computation, can yield widely diverging outcomes for such dynamical systems, rendering long-term prediction of their behavior impossible in general. Chaotic behavior exists in many natural systems, including fluid flow, heartbeat irregularities, weather and climate.

2.2 Chaotic systems and cryptography

A chaotic dynamical system is a deterministic system that exhibits seemingly random behavior as a result of its sensitive dependence on its initial conditions and can never be specified with infinite precision. The chaotic system behavior is unpredictable; thereby it resembles noise. The close relationship between cryptography and chaos makes a chaos based cryptographic algorithm a natural candidate for secure communication and cryptography. Cryptographic algorithms and chaotic maps have similar properties such as sensitivity to changes in the initial conditions and control parameters, pseudorandom behavior and unstable periodic orbits with long periods. The basic principle of image encryption using chaos is based on the ability of some dynamic systems to produce sequence of numbers that are random in nature. Messages are encrypted using these sequences. Because of the pseudorandom behavior, the output of the system seems random in the attacker's view whereas it appears as defined in the receiver's view and decryption is possible. An important difference between cryptography and chaos maps is that encryption transformations are defined on finite sets whereas chaos maps have meaning only for real numbers. Each chaos map has parameters that are equivalent to encryption key in cryptography.

3 1-Dimensional Chaotic Map (1-DCF)

One-dimensional cosine fractional chaotic map (1-DCF) is defined by simple following iterative function:

$$f : I \to I$$
$$x_{n+1} = f(x_n) = \cos\left(\frac{\alpha}{x_n^{\beta}}\right), \ \alpha > 0, \ \beta \in N^*$$

here the interval I is equal to $[-1,\ 0[\cup]0,\ 1]$. The 1-DCF map has an infinite chaotic range thanks to its positive real control parameter α. Linear stability analysis shows map has infinite number of unstable fixed points. It also has a largely greater Lyapunov exponent value as compared to other maps. The higher the LE value is, the more sensitive is the system.

3.1 Bifurcation analysis

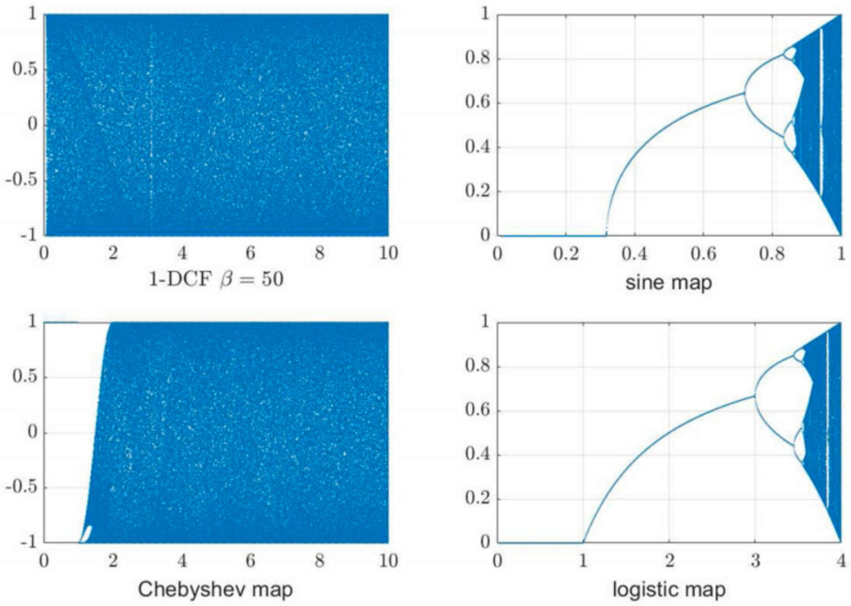

Figure 1: Bifurcation diagram of 1-DCF and some well-known chaotic maps

The bifurcation diagram is a straightforward tool to visually analyze the long-term behavior of a dynamical system (stability, instability, periodicity, or chaos) according to one of the parameter's values. Figure 3 illustrates the bifurcation diagrams of the logistic, sine, Chebyshev, and the 1-DCF maps. As one can see, the proposed map offers a larger chaotic region and a more uniform distribution.

3.2 Trajectory analysis

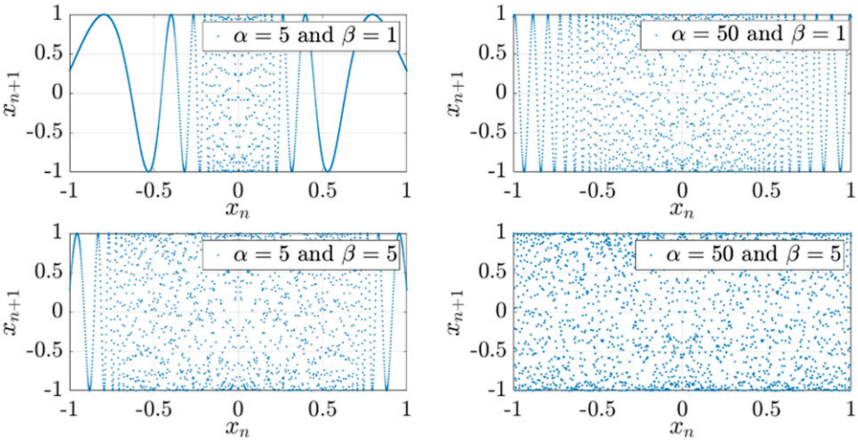

Figure 2: Trajectory diagram of 1-DCF map using different parameters' values

In Fig. 2, we plot the new map trajectory behavior in a phase space diagram. As shown in this figure, the 1-DCF map trajectory looks like a sinusoidal waveform where the wave's periodicity is variable and tends to get smaller as the control parameters get bigger. Thus, the 1-DCF trajectory looks more random- like for higher control parameter's values which makes it able to generate more uniform and unpredictable data time series.

4 Image Encrytion Scheme

We modify the image encryption scheme (DCF-IES) proposed in (TWT20). DCF-IES is based on the 1-DCF chaotic map and adopt a permutation-less architecture which significantly increases the encryption speed. To maintain a high-security level, it uses a substitution process with an extremely high sensitivity to the plain image. Instead of natural row encryption order, it follows by a random-like encryption order generated from the secret key. The control parameter of the 1-DCF map is an integer; however, due to some numbers representation limits of nowadays computers is limited to the interval (0, 50]. DCF-IES skips the traditional permutation phase. Therefore, the pixels' positions remain the same in the original and the cipher images. We bring back the permutation phase, which makes the encryption more secure.

4.1 Permutation

The shuffling algorithm given in (LM18) is used to disturb the positions of each pixel of a plain image P, which reduces the correlationship between adjacent

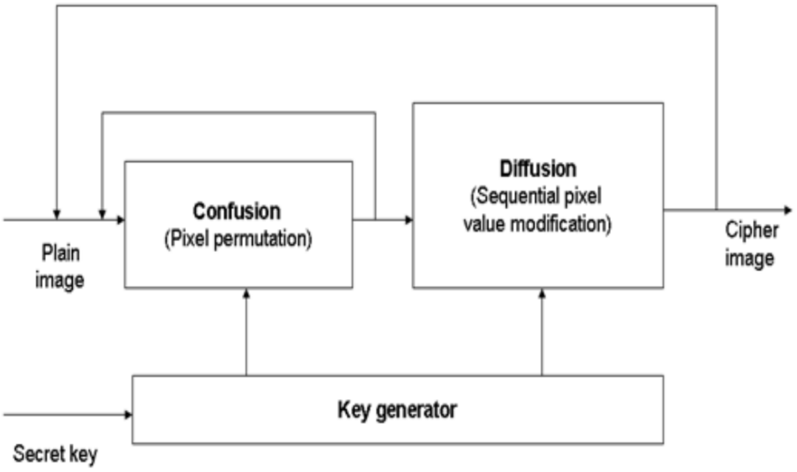

Figure 3: Architecture of Chaos based cryptosystem

pixels. We use the proposed 1-DCF chaotic map to shuffle the pixels.
Assume P_{ij} be the pixel matrix of $M \times N$ plain image P, and a real-valued sequence x_k is generated by the 1-DCF map with a given initial value and with length $M \times N$. Rearrange the sequence x_k according to the ascending order, and get the rearranged sequence: $x_{k_1}, x_{k_2}, ..., x_{kMN}$
where $x_{k_1} \leq x_{k_2} \leq ... \leq x_{kMN}$ and $k_l \in 1, 2, ..., MN, 1 \leq l \leq MN$, is different from each other. Now, the integer sequence k_l is used as the shuffling sequence.
Scanning the matrix P into a sequence b_s as
$b_{(i-1)N+j} = P_{ij}, 1 \leq i \leq M, 1 \leq j \leq N$
Then, the shuffled sequence c_t can be calculated as $c_{k_i} = b_i, 1 \leq i \leq MN$
Finally, reconstruct the sequence c_t to a matrix as $C_{ij} = c_t$
where $i = floor\frac{(t-1)}{N} + 1$ and$j = t - (i-1)N$
Thus, the matrix C is the shuffled matrix of plain image P by using our shuffling algorithm. This shuffled matrix is based on the chaotic sequence x_k, which can be regarded as unpredictable and randomness.

4.2 Encryption

The pseudo-code of the proposed image encryption scheme is presented in 1.

Algorithm 1: Encryption algorithm

```
Input: $PictureP, Key, T$
Output: $Cipher\ C, avg$
$M = countRows(P)$; $N = countColumns(P)$;
$avg = computeAvg(P)$;
/* Shuffle pixels of P (Permutation process)*/
$Shuffle(P)$;
for $r = 1...T$ do
    $x_0 = Key(0, r) + FractionalPart(Sum(Key))$;
    $\alpha = Key(1, r)$; $\beta = Key(4, r)$;
    /* Generate a random-like path using 1-DCF map*/
    $RLP = generateSeq(x_0, \alpha, \beta, M)$;
    $RLP = SortIndex(RLP)$;
    /* Generate two sequences $S_1$ and $S_2$ by 1-DCF map*/
    $x_0 = Key(2, r) + FractionalPart(avg)$;
    $S_1 = generateSeq(x_0, \alpha, \beta, N)$;
    $x_0 = Key(3, r)$;
    $S_2 = generateSeq(x_0, \alpha, \beta, N)$;
    /* Normalize $S_1$ and $S_2$*/
    $S_1 = S_1 \times 10^7 \bmod 256$; $S_2 = S_2 \times 10^7 \bmod 256$;
    $P_{RLP[1]} = P_{RLP[1]} \oplus S_1$;
    for $i = 2...M$ do
        $P_{RLP[i]} = (P_{RLP[i]} + P_{RLP[i-1]} \oplus S_2) \bmod 256$;
    end
    /* Re-generate two sequences $S_1$ and $S_2$ by 1-DCF map*/
    $x_0 = Key(3, r) + FractionalPart(avg)$;
    $S_1 = generateSeq(x_0, \alpha, \beta, N)$;
    $x_0 = Key(2, r)$;
    $S_2 = generateSeq(x_0, \alpha, \beta, N)$;
    /* Normalize $S_1$ and $S_2$*/
    $S_1 = S_1 \times 10^7 \bmod 256$; $S_2 = S_2 \times 10^7 \bmod 256$;
    $P_{RLP[M]} = P_{RLP[M]} \oplus S_1$;
    for $i = M - 1...1$ do
        $P_{RLP[i]} = (P_{RLP[i]} + P_{RLP[i+1]} \oplus S_2) \bmod 256$;
    end
end
$C = P$;
```

4.3 Decryption

In the literature, several encryption schemes use the average value function to enhance the plain-text sensitivity. In the DCF–IES scheme, the average value is used to encrypt only the first row and is calculated from the other rows. Hence, the receiver can decrypt the other rows without any additional information; then, he can easily decrypt the first row by recalculating the average value of the other rows which have been already decrypted. Thus, the decryption process can be easily achieved by inverting the encryption process and without any extra side information. Our proposed encryption scheme doesn't follow this structure, and the average value is required to be communicated to the decrypt the cipher image.

5 Results and security analysis

We have implemented our proposed image encryption scheme in Python. The implementation is available here: GitHub-Repo.

5.1 Secret key robustness analysis

Brute force is a popular and trivial type of cryptanalysis attacks, where an eavesdropper who knows the used encryption scheme can try to decrypt a cipher image using all the possible keys. To avoid such type of attacks, the secret keyspace should be very large. In our encryption scheme, each encryption round (total T rounds) uses as secret key 4 real and 1 integer values. With regard to the 1-DCF chaotic map, the precision of the intial value x_0 is 10^{-16} and the precision of the control parameter α is equal to 10^{-14}. The control parameter β is an integer included in the interval (0; 60] and can be represented using 6 bits. Therefore, the secret keyspace can be approximated as follows:

$$(10^{16\times 3} \times 10^{14} \times 2^{6})^{T} \approx 2^{192\times T}$$

So, secret key has a widely larger space than the required minimum keyspace 2^{120} and consequently can handle Brute-force attacks with nowadays computation force.

5.2 Histogram analysis

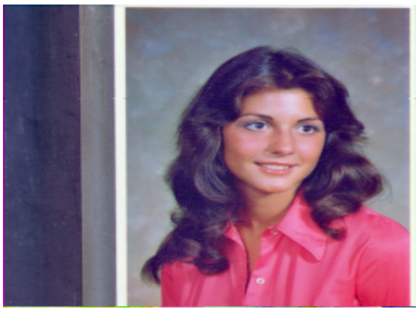

Figure 4: Original image

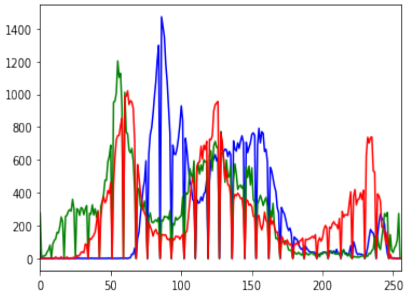

Figure 5: Original histogram

An image histogram is widely used in statistical attacks, where it can let an attacker find some eventual relations between the pixels' values distribution of the plain and its corresponding cipher image. Thus, a secure image encryption scheme should always generate cipher images having a uniform and flat histogram. Figure 4 and 5 show original image and it's image histogram and 6, 7 shows cipher image and it's image histogram respectively. As we can see,

Figure 6: Cipher image

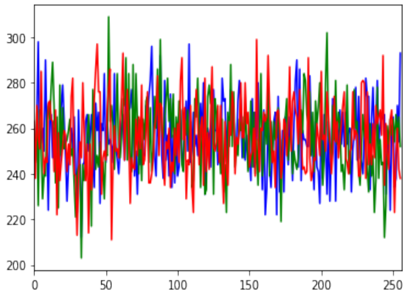

Figure 7: Cipher histogram

the DCF–IES scheme succeeds to generate cipher images with uniform pixels intensity-level distribution.

5.3 Noise Resistance

The transmitted data over communication networks could be affected by noisy signals. The transmitted cipher images can be affected by these noise interference or be blurred by attackers which can reduce the quality of the decrypted images.
DCF-IES fails to decrypt a cipher image with noise, mainly because of the fact that it decrypts some part of the image first and then uses the average pixel value of that decrypted part to decrypt the remaining part. Figure-9 shows the decrypted image output of Figure-8. Even if we modify it to use average of all pixel values and pass the average value to the receiver for decryption, the output decryted image is as shown in Figure-10.
Addition of permutation phase in the image encryption scheme leads to scattering of noise that may have been produced in the cipher image. As shown in Figure-11, when we black out some portion of cipher image, instead of a portion of original image getting missed in the decrypted image, the noise gets scattered due to permutation step involved in the scheme and we get a decrypted image with no portion of image missing and hence better visibility. Figure-12 and Figure-13 show another example of decryption of a noisy cipher image by our encrpytion scheme.

6 Limitations and Future work

Limitations: 1. Due to the additional permutation phase, our proposed encryption scheme is slow and hence is not feasible for real-time encryption. 2. Problem usually arises in the decryption process where the receiver is unable to decrypt the cipher image without the average value of the original image. Hence, a secure communication channel is mandatory to transfer the plain image pixels average value.

Future Work: 1. Devising a partial permutation method while maintaining noise resistance: Instead of permuting over the whole image, one can consider shuffling of pixels to be carried out within some blocks of image. This makes the

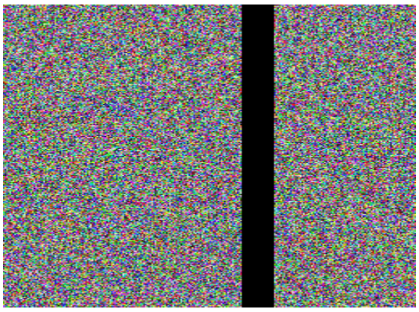

Figure 8: Cipher with vertical noise

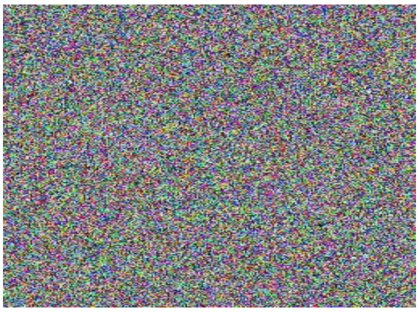

Figure 9: DCF-IES

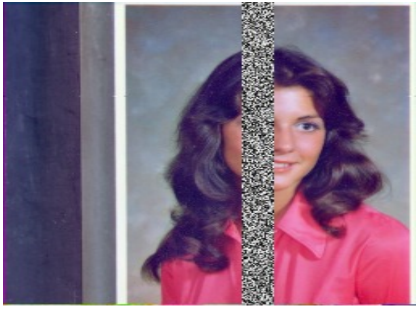

Figure 10: Modified DCF-IES, without permutation

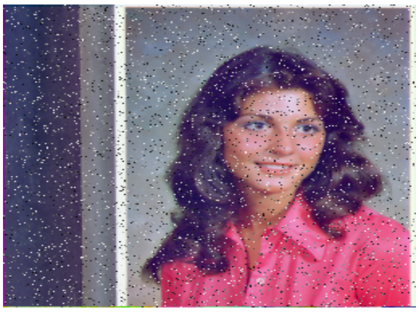

Figure 11: Modified with permutation

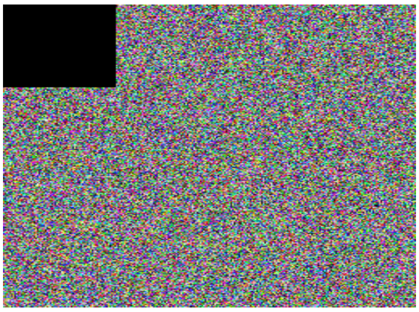

Figure 12: Cipher with noise in corner

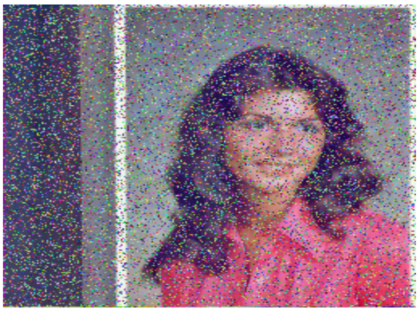

Figure 13: Decrypted image

encryption fast. But, now the noise is more concentrated as it will scatter within a block only. 2. Modifying architecture by incorporating higher dimensional chaotic maps: Depending on the number of variables, chaotic systems can be classified as low-dimensional chaotic maps and highdimensional chaotic maps. The low-dimensional chaotic maps have a simple structure characterized by a small number of variables. Low-dimensional maps are sometimes predictable and so not too interesting for cryptography where a large keyspace is needed. Unlike the former type, high-dimensional maps have more variables and offer a more massive chaotic range. However, their structure is very complex due to their large number of variables.

References

ACP19 José AP Artiles, Daniel PB Chaves, and Cecilio Pimentel. Image encryption using block cipher and chaotic sequences. *Signal Processing: Image Communication*, 79:24–31, 2019.

EAF16 Safwan El Assad and Mousa Farajallah. A new chaos-based image encryption system. *Signal Processing: Image Communication*, 41:144–157, 2016.

LM18 Lingfeng Liu and Suoxia Miao. A new simple one-dimensional chaotic map and its application for image encryption. *Multimedia Tools and Applications*, 77(16):21445–21462, 2018.

LWC17 Yueping Li, Chunhua Wang, and Hua Chen. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. *Optics and Lasers in Engineering*, 90:238–246, 2017.

TWM20 Mohamed Zakariya Talhaoui, Xingyuan Wang, and Mohamed Amine Midoun. Fast image encryption algorithm with high security level using the bülban chaotic map. *Journal of Real-Time Image Processing*, pages 1–14, 2020.

TWT20 Mohamed Zakariya Talhaoui, Xingyuan Wang, and Abdallah Talhaoui. A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. *The Visual Computer*, pages 1–12, 2020.