Studies in Mathematical Sciences
Vol. 2, No. 1, 2011, pp. 96-106
www.cscanada.org

ISSN 1923-8444 [Print]
ISSN 1923-8452 [Online]
www.cscanada.net

Image Encryption Using Novel Mappings over GF(2^n)

Liebin YAN[1]

Ruisong YE[1,*]

Abstract: Galois Field GF(2^n) is valuable to encryption and has been used in some famous encryption algorithms, such as BCH and AES. In practical application, image encryptions are used widely to protect information in transmission. This paper will propose two image encryption techniques based on two novel mappings over GF(2^n): One involves a transformation consisting of a linear transformation and a *Frobenius automorphism*, which shuffles pixels' positions, that is, a permutation, giving a good diffusion effect, and another one alters pixels' values and gives dramatic confusion effect.

Key Words: Galois field; Frobenius automorphism; Linear transformation; Confusion; Diffusion

1. INTRODUCTION

Galois Field is an appreciated tool for encryption and some famous encryption algorithms, such as BCH and AES, have made use of its virtue. In the field of image encryption, there are so many techniques proposed, such as *Wavelet transformation*, *Fourier transformation*, *Logistic mapping* and *Arnold cat mapping*. The latter two are regarded as chaotic systems. In Ref. [1], Nien et al. proposed a shuffle method that combined four chaotic systems. In Ref. [2], over Galois Field, Wang and Su introduced an encryption scheme for secret image sharing based on (r, n)-threshold scheme inspired by Shamir[3]. And they claimed that their scheme could provide adequately huge key-space and hence high security against brute-force attack holds. Nevertheless, there is little work on GF(2^n). In this paper, we specially focus on GF(2^n) and introduce two mappings mathematically and based on these mappings two techniques for image encryption are proposed. The first mapping is a transformation, involving a linear transformation and Frobenius automorphism, and another one invokes *Kronecker product* that help form a basis of $\mathbb{F}_q^{2^{2n}}$. The former one obtains great confusion on visual sensation while the latter one modifies image's distributive characteristics by making use of inner product over $\mathbb{F}_q^{2^{2n}}$.

2. NOVEL MAPPINGS OVER GF(2^n) AND NEW ENCRYPTION SCHEMES

[1] Department of Mathematics, Shantou University, Shantou 515063, Guangdong, China.
Email addresses: s_lbyan@stu.edu.cn (Liebin Yan); rsye@stu.edu.cn (Ruisong Ye).

[*] Corresponding author.

[†] Received 10 December 2010; accepted 10 January 2011.

2.1 Novel Mappings over $\mathrm{GF}(2^n)$

Galois field, denoted as $\mathrm{GF}(p^n)$, is a finite extension of degree n over a finite filed $\mathbb{Z}_p$, where p is a prime number, and $\mathrm{GF}(p^n) \simeq \mathbb{Z}_p[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$. Now we are only interesting in $\mathrm{GF}(2^n)$. By virtue of its characteristic 2, every element in $\mathrm{GF}(2^n)$, say $g(x)$, is a polynomial with degree strictly less than n with coefficients either 1 or 0, hence it is conventional to represent elements of $\mathrm{GF}(2^n)$ as binary numbers of order n, and every $g(x) \in \mathrm{GF}(2^n)$ can be denoted as $g(2)$ an integer in $\mathbb{Z}_{2^n}$ and vice versa. Addition on $\mathrm{GF}(2^n)$ is performed as normal polynomials addition with reduction modulo 2, and multiplication on $\mathrm{GF}(2^n)$ is a normal polynomials multiplication with reduction modulo an irreducible polynomial $f(x)$ as mentioned above. In this paper, let (x, y) be pixel coordinate and z be the gray-level value. For convenience, let coordinate index begin from 0 and let $\odot$ and $\oplus$ denote multiplication and addition on Galois Field $\mathrm{GF}(2^n)$ respectively as well as $a \odot b$ be ab, unless otherwise stated. Further let $\mathbb{F}_q^m$ denote m-dimensional vector space over $\mathrm{GF}(q)$, where $q = 2^n$, and v^{T} is the transpose of v.

Frobenius automorphism σ on $\mathrm{GF}(2^n)$ is defined by $\sigma(x) = x^2, x \in \mathrm{GF}(2^n)$, which generates a finite multiplicative cyclic group $\langle\sigma\rangle$ with order n, and every element $\sigma^k \in \langle\sigma\rangle$ is an automorphism on $\mathrm{GF}(2^n)$ with its inverse $\sigma^{-k}(x) = \sigma^{n-k}(x) = x^{2^{n-k}}$. In respect that $\mathrm{GF}(2^n)$ is a field, linear space and linear transformation are well defined in Refs. [4–6]. By employing linear algebra and *Frobenius automorphism*, we let ϕ be the mapping from $\mathbb{F}_q^2$ to itself, defined by

$$
\begin{aligned}
\phi\left(x, y\right) &= \left(x^{2^{k_1}}, y^{2^{k_2}}\right) \odot \begin{pmatrix} 1 & 1 \\ a & b \end{pmatrix} \oplus (c, d) \\
&= \left(x^{2^{k_1}} \oplus a y^{2^{k_2}} \oplus c,\ x^{2^{k_1}} \oplus b y^{2^{k_2}} \oplus d\right),
\end{aligned} \tag{1}
$$

and accordingly the inverse is as

$$
\begin{aligned}
\phi^{-1}\left(x, y\right) &= \begin{pmatrix} \left((a\oplus b)^{-1}(bx\oplus ay\oplus ad\oplus bc)\right)^{2^{-k_1}} \\ \left((a\oplus b)^{-1}(x\oplus y\oplus c\oplus d)\right)^{2^{-k_2}} \end{pmatrix}^{\mathrm{T}} \\
&= \begin{pmatrix} \left((a\oplus b)^{2^n-2}(bx\oplus ay\oplus ad\oplus bc)\right)^{2^{n-k_1}} \\ \left((a\oplus b)^{2^n-2}(x\oplus y\oplus c\oplus d)\right)^{2^{n-k_2}} \end{pmatrix}^{\mathrm{T}},
\end{aligned} \tag{2}
$$

where $a \neq b$, $a, b, c, d \in \mathrm{GF}(2^n)$, $0 \leqslant k_1, k_2 < n$.

For convenience, we let $\boldsymbol{a} = (a, b, c, d, k_1, k_2)$.

Let $\boldsymbol{v}(x) = \left(1, x, x^2, \ldots, x^{2^n-1}\right)^{\mathrm{T}}$ be a 2^n-dimensional vector over $\mathrm{GF}(2^n)$, then $\{\boldsymbol{v}(0), \boldsymbol{v}(1), \boldsymbol{v}(2), \ldots, \boldsymbol{v}(2^n -1)\}$ is a polynomial basis of $\mathbb{F}_q^{2^n}$[4, 6]. Note that the *Kronecker Product* of two $\mathbb{F}_q^{2^n}$ is $\mathbb{F}_q^{2^{2n}}$[7]. By applying *Kronecker Product* to $\mathbb{F}_q^{2^n}$, a basis of $\mathbb{F}_q^{2^{2n}}$, say $\{\boldsymbol{v}(x, y) | x, y \in \mathrm{GF}(2^n)\}$, as follows :

$$
\begin{aligned}
\boldsymbol{v}(x, y) = (&1, x, x^2, \ldots, x^{2^n-1}, \\
&y, yx, yx^2, \ldots, yx^{2^n-1}, \\
&\ldots, \\
&y^{2^n-2}, y^{2^n-2}x, y^{2^n-2}x^2, \ldots, y^{2^n-2}x^{2^n-1}, \\
&y^{2^n-1}, y^{2^n-1}x, y^{2^n-1}x^2, \ldots, (yx)^{2^n-1})^{\mathrm{T}}.
\end{aligned} \tag{3}
$$

We intend to obtain a basis of m-dimensional vector subspace of $\mathbb{F}_q^{2^{2n}}$, one way is to let $\boldsymbol{p} = (p_1, p_2, \ldots, p_{m-1})$ be an $(m-1)$-dimensional vector, $m \leqslant 2^n$, and define an m-dimensional vector

$$
\boldsymbol{\omega}(x, y) = (x^{p_1} y^{p_1^2 \oplus 1}, x^{p_2} y^{p_2^2 \oplus 2}, \ldots, x^{p_{m-1}} y^{p_{m-1}^2 \oplus (m-1)}, 1). \tag{4}
$$

It is easy to prove that $\{\boldsymbol{\omega}(x,y)|x,y\in \mathrm{GF}(2^n)\}$ spans $\mathbb{F}_q^m$. Firstly, $\boldsymbol{\omega}(x,y)$ is non-zero. Secondly, if for all $i\neq j$ and $p_i\neq p_j$, then $x^{p_i}y^{p_i^2\oplus i}\neq x^{p_j}y^{p_j^2\oplus j}$, else if there exists an i and a j such that $i\neq j$ but $p_i=p_j$, then $p_i^2\oplus i\neq p_j^2\oplus j$, consequently, $x^{p_i}y^{p_i^2\oplus i}\neq x^{p_j}y^{p_j^2\oplus j}$ holds.

Next apply the map ϕ to $\boldsymbol{\omega}(x,y)$, and we obtain that

$$\begin{aligned}\boldsymbol{v}(x,y) &= \boldsymbol{\omega}\left(\phi(x,y)^{\mathrm{T}}\right)\\ &= (f(x,y)^{p_1}g(x,y)^{p_1^2\oplus 1}, f(x,y)^{p_2}g(x,y)^{p_2^2\oplus 2},\\ &\quad \ldots, f(x,y)^{p_{m-1}}g(x,y)^{p_{m-1}^2\oplus(m-1)}, 1),\end{aligned} \tag{5}$$

where $f(x,y)=x^{2^{k_1}}\oplus ay^{2^{k_2}}\oplus c$, $g(x,y)=x^{2^{k_1}}\oplus by^{2^{k_2}}\oplus d$, and $a\neq b$, $a,b,c,d\in \mathrm{GF}(2^n)$, $0\leqslant k_1,k_2<n$.

Obviously, $\{\boldsymbol{v}(x,y)|x,y\in \mathrm{GF}(2^n)\}$ does span $\mathbb{F}_q^m$ as well. Further more, let $\boldsymbol{u}=(u_1,u_2,\ldots,u_m)^{\mathrm{T}}$ be a m-dimensional vector, we define a map ψ: $\mathbb{F}_q^3\mapsto \mathrm{GF}(2^n)$ as follows:

$$\begin{aligned}\psi(x,y,z) &= z\oplus \boldsymbol{v}(x,y)\odot \boldsymbol{u}\\ &= z\oplus u_m\oplus\sum_{i=1}^{m-1}u_i\odot f(x,y)^{p_i}g(x,y)^{p_i^2\oplus i},\end{aligned} \tag{6}$$

where $x,y,z\in \mathrm{GF}(2^n)$.

Further, define a new matrix $\Psi=(\psi_{i,j})$, with respect to $(\boldsymbol{a},\boldsymbol{p},\boldsymbol{u})$, denoted by $\Psi_{(\boldsymbol{a},\boldsymbol{p},\boldsymbol{u})}$ as follows:

$$\psi_{i,j}=\psi(i,j,0).$$

Clearly, $\psi(x,y,\psi(x,y,z))=z$ as $\Psi\oplus\Psi=O$.

2.2 New Encryption Schemes Based on Mappings Above

2.2.1 Diffusion on Coordinates (DC)

Remark that the map ϕ is a bijection from $\mathbb{F}_q^2$ to itself, hence a permutation upon pixel coordinates, assume that pixel coordinates are limited within $\mathbb{F}_q^2$. Suppose that the image to process is of size $M\times N$, there exists an integer n such that $2^n\leqslant \min(M,N)<2^{n+1}$. By applying some mechanism, the image can be split into blocks of size $2^n\times 2^n$ ordinally. For this reason, we assume the image to encrypt is of size $2^n\times 2^n$. we choose a key $\boldsymbol{a}$ and apply ϕ to its pixel coordinates. And accordingly, the decryption is similar to encryption, but to call ϕ^{-1} instead of ϕ. For security, we could repeat this procesure with a new key, if desired.

2.2.2 Confusion on Pixels (CP)

Now, recall the mapping ψ defined above and we propose another scheme. Assume that the image is of size $M\times N$ and an 8-bit image, in case of RGB image, we could regard it as a 3-level gray image, that is 3-level 8-bit image. Be aware of that M or N may be greater than $2^8=256$, so we have to modify the map ψ as follows:

$$\begin{aligned}\psi(x,y,z) =&z\oplus \boldsymbol{v}(\bar{x},\bar{y})\odot \boldsymbol{u}\\ =&z\oplus u_m\oplus\sum_{i=1}^{m-1}u_i\odot f(\bar{x},\bar{y})^{p_i}g(\bar{x},\bar{y})^{p_i^2\oplus i},\end{aligned} \tag{7}$$

where $\bar{w} = w \mod 256$ is a surjective ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_{256}$, $z \in \mathbb{Z}_{256}$.

The encryption procedure is the same as the decryption as follows:

1. For each level, choose a key tuple $(\boldsymbol{a}, \boldsymbol{p}, \boldsymbol{u})$:

$$\boldsymbol{a} = (a, b, c, d, k_1, k_2), \quad \boldsymbol{p} = (p_1, p_2, \dots, p_{m-1}), \quad \boldsymbol{u} = (u_1, u_2, \dots, u_m)^T. \tag{8}$$

2. For all pixels, with key above, apply ψ to them.

3. EXNERIMENTS AND ANALYSIS

3.1 Experiments

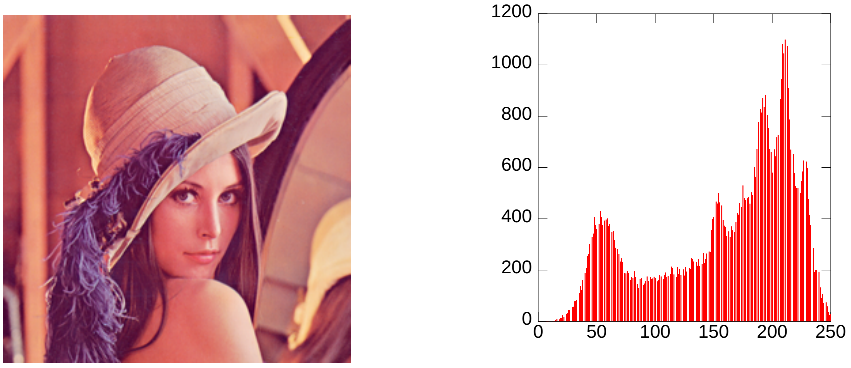
Experiments have been carried out on GNU Octave (`http://www.gnu.org/software/octave/`) and also been implemented in C with opencv (`http://sourceforge.net/projects/opencvlibrary/`). Thanks *James S. Plank* for his *Fast Galois Field Arithmetic Library* (`http://www.cs.utk.edu/~plank/plank/papers/cs-07-593/`).

Figure 1(a) is the original color image *Lena* of size 256 × 256, Figures 1(b), 1(c) and 1(d) are the RGB spectra of Figure 1(a). We make experiments on this image with our new schemes.

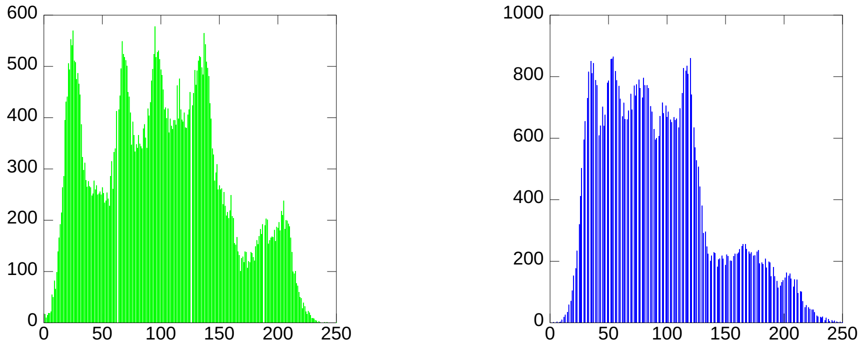
3.1.1 Experiments for Diffusion on Coordinates

Figure 2 shows the results of the scheme *Diffusion on Coordinates*. We pick up keys $\boldsymbol{a}_r$=(35, 42, 45, 222, 3, 5), $\boldsymbol{a}_g$=(5, 42, 32, 29, 6, 2), $\boldsymbol{a}_b$=(252, 4, 45, 76, 4, 7), and $\boldsymbol{a}_{r'}$=(35, 42, 45, 222, 3, 5). By applying this scheme together with these keys to Figure 1(a)'s RGB levels respectively, we obtain Figures 2(a) and 2(b) for once and twice respectively.

Figures 2(c) and 2(d) show the results when Figure 1(a) is applied with the key $\boldsymbol{a}_r$ to all levels, once and twice respectively. This makes clearly that this scheme is key sensitive.



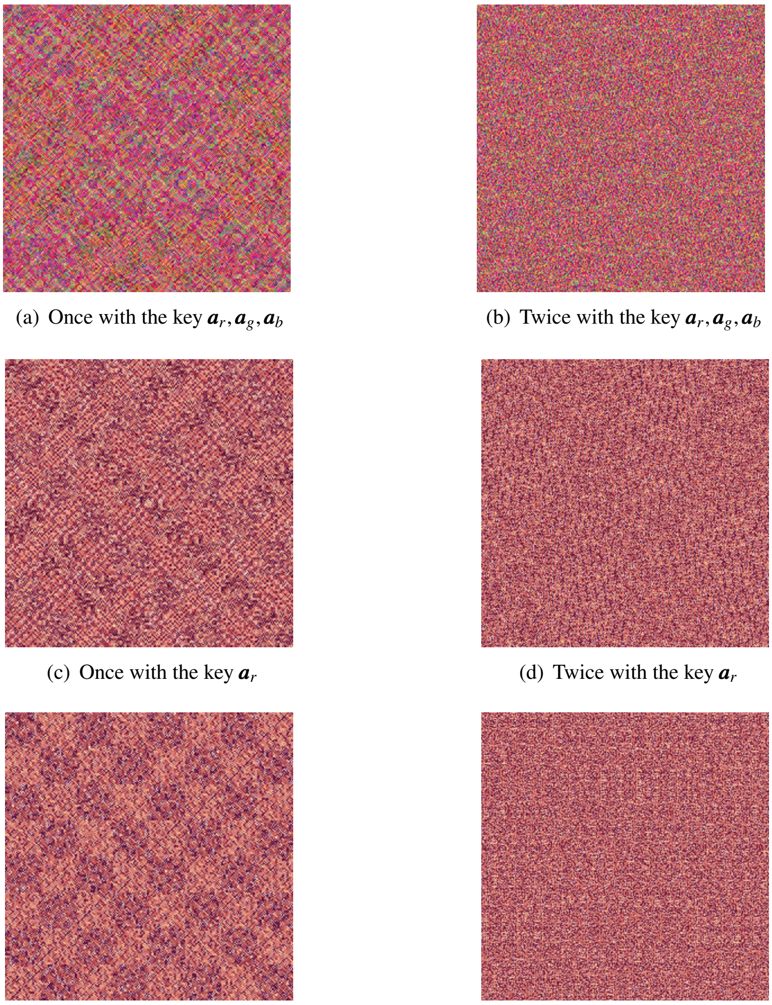
(a) Original Lena. (b) R-level spectrum



(c) G-level spectrum

(d) B-level spectrum

Figure 1: Original Lena and its RGB spectra



(a) Once with the key $\boldsymbol{a}_r, \boldsymbol{a}_g, \boldsymbol{a}_b$

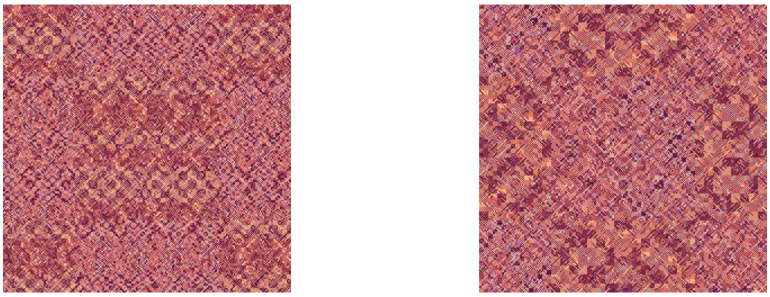
(b) Twice with the key $\boldsymbol{a}_r, \boldsymbol{a}_g, \boldsymbol{a}_b$

(c) Once with the key $\boldsymbol{a}_r$

(d) Twice with the key $\boldsymbol{a}_r$

(e) Once with the key $\boldsymbol{a}_{r'}$

(f) Twice with the key $\boldsymbol{a}_{r'}$

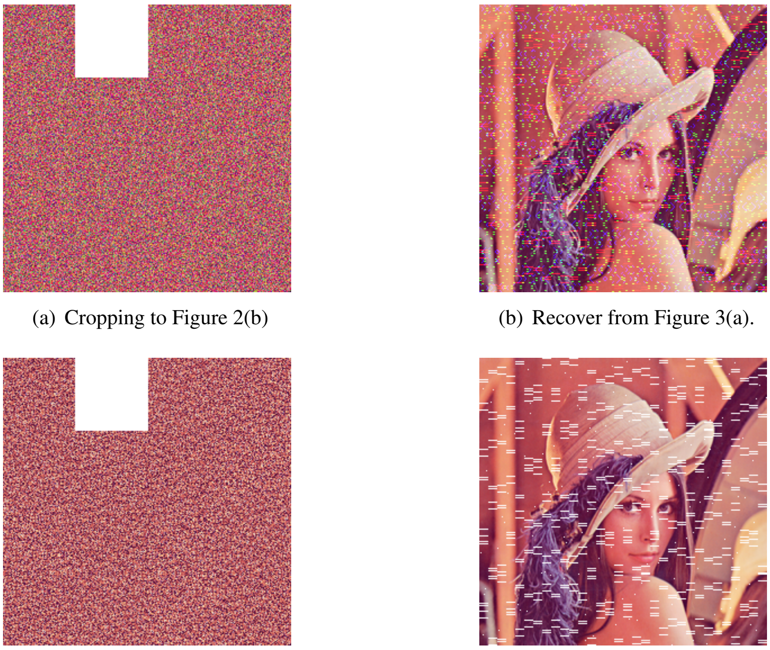


(g) Once with the key $\boldsymbol{a}_g$

(h) Once with the key $\boldsymbol{a}_b$

Figure 2: Key sensitive for *Diffusion on Coordinates* with keys: $\boldsymbol{a}_r$=(35, 42, 45, 222, 3, 5), $\boldsymbol{a}_g$=(5, 42, 32, 29, 6, 2), $\boldsymbol{a}_b$=(252, 4, 45, 76, 4, 7), $\boldsymbol{a}_{r'}$=(34, 42, 45, 222, 3, 5)

By changing the key $\boldsymbol{a}_r$ a bit, for instance $\boldsymbol{a}_{r'}$ given in Figure 2, we obtain distinct results: Figure 2(e) and Figure 2(f) To prove how diffusion effect the scheme *Diffusion on Coordinates* can bring, we invoke *Cropping* test. Figure 3 gives evidences of resistance against *Cropping*.



(a) Cropping to Figure 2(b)

(b) Recover from Figure 3(a).

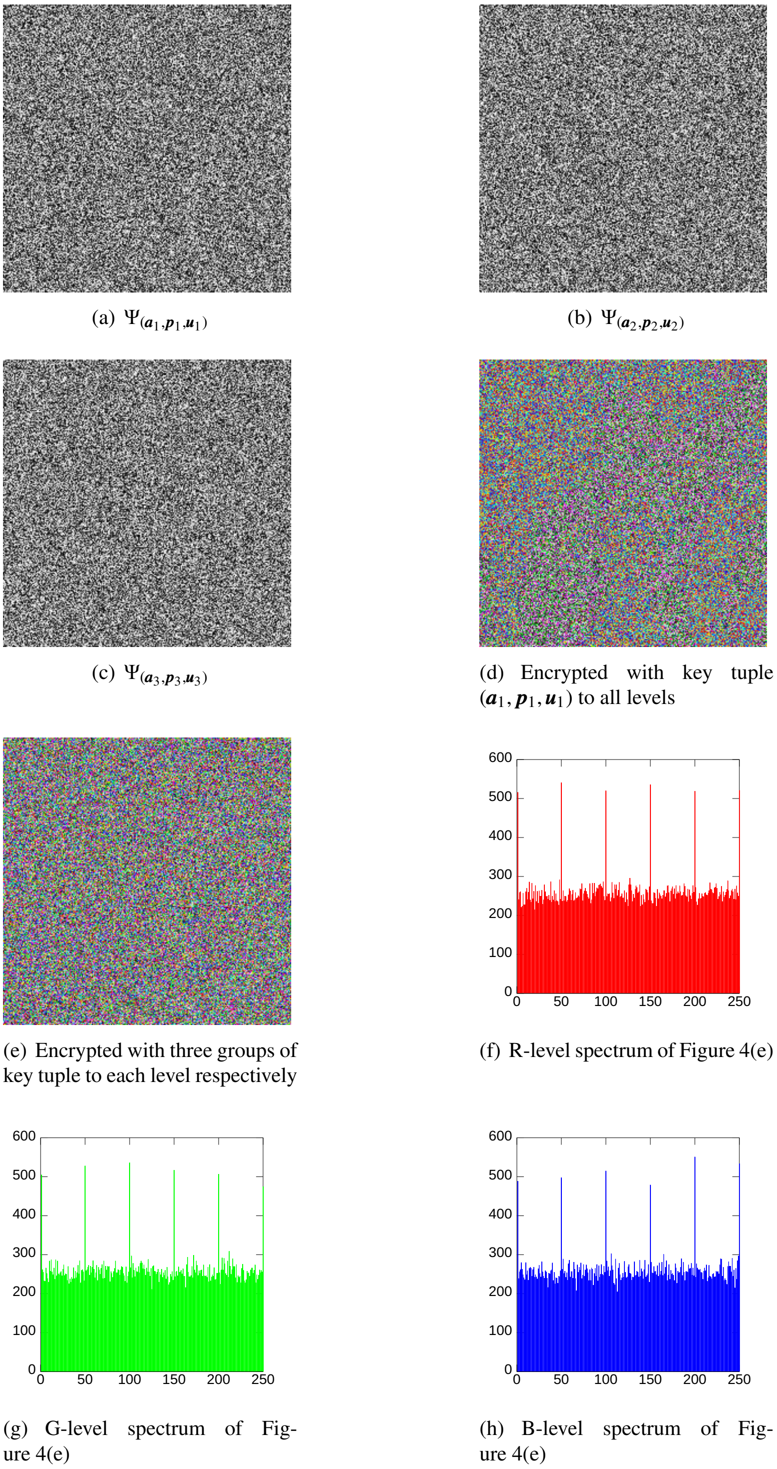
(c) Cropping to Figure 2(d)

(d) Recover from Figure 3(c).

Figure 3: Cropping test for *Diffusion on Coordinates* with keys: $\boldsymbol{a}_r$=(35, 42, 45, 222, 3, 5), $\boldsymbol{a}_g$=(5, 42, 32, 29, 6, 2), $\boldsymbol{a}_b$=(252, 4, 45, 76, 4, 7), $\boldsymbol{a}_{r'}$=(34, 42, 45, 222, 3, 5)

3.1.2 Experiments for Confusion on Pixels

Figure 4 shows the results for the second scheme *Confusion on Pixels*. We select three groups of key tuple $(\boldsymbol{a}_i, \boldsymbol{p}_i, \boldsymbol{u}_i), i = 1, 2, 3$. Figures 4(a), 4(b) and 4(c) are the images $\Psi_{(}\boldsymbol{a}_i, \boldsymbol{p}_i, \boldsymbol{u}_i)$ respectively. Figures 4(d) and 4(e) are two results, in which the former is obtained by applying *Confusion on Pixels* with key



(a) $\Psi_{(\boldsymbol{a}_1,\boldsymbol{p}_1,\boldsymbol{u}_1)}$

(b) $\Psi_{(\boldsymbol{a}_2,\boldsymbol{p}_2,\boldsymbol{u}_2)}$

(c) $\Psi_{(\boldsymbol{a}_3,\boldsymbol{p}_3,\boldsymbol{u}_3)}$

(d) Encrypted with key tuple $(\boldsymbol{a}_1, \boldsymbol{p}_1, \boldsymbol{u}_1)$ to all levels

(e) Encrypted with three groups of key tuple to each level respectively

(f) R-level spectrum of Figure 4(e)

(g) G-level spectrum of Figure 4(e)

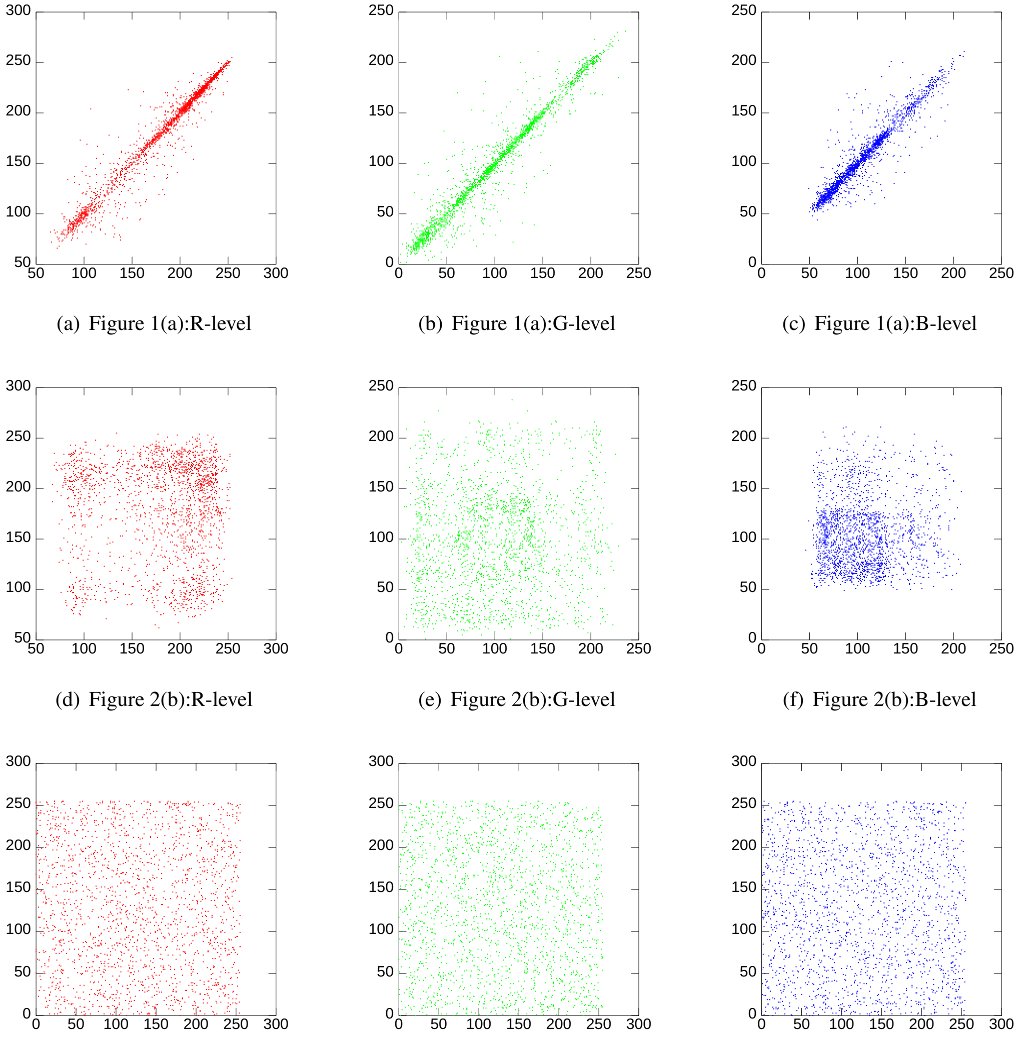
(h) B-level spectrum of Figure 4(e)

Figure 4: Confusion on Pixels: $\boldsymbol{a}_1 = (110, 213, 31, 42, 2, 3)$, $\boldsymbol{p}_1 = (7, 9, 31, 4, 220)$, $\boldsymbol{u}_1 = (8, 227, 19, 0, 5, 6)$, $\boldsymbol{a}_2 = (120, 21, 42, 57, 5, 6)$, $\boldsymbol{p}_2 = (99, 78, 31)$, $\boldsymbol{u}_2 = (61, 34, 5, 245)$, $\boldsymbol{a}_3 = (77, 49, 81, 53, 7, 4)$, $\boldsymbol{p}_3 = (54, 0, 0, 32)$, $\boldsymbol{u}_3 = (92, 71, 115, 64, 95)$

$(\boldsymbol{a}_1, \boldsymbol{p}_1, \boldsymbol{u}_1)$ to all levels of Figure 1(a) and the latter is applied with $(\boldsymbol{a}_i, \boldsymbol{p}_i, \boldsymbol{u}_i), i = 1, 2, 3$ to each level respectively. Figures 4(f), 4(g) and 4(h) are the RGB spectra of Figure 4(e). Apparently, the histograms of the encrypted image is properly uniform and significantly distinct from the original Figure 1(a).

3.2 Statistics Analysis

In following, *NPCR* (Number of Pixel Change Rate), *UACI* (Unified Average Changing Intensity) and *Correlation of two adjacent pixels* are invoked to show variants in statistical characteristics between the original image and the encrypted one with these two schemes.



(a) Figure 1(a):R-level

(b) Figure 1(a):G-level

(c) Figure 1(a):B-level

(d) Figure 2(b):R-level

(e) Figure 2(b):G-level

(f) Figure 2(b):B-level

(g) Figure 4(e):R-level

(h) Figure 4(e):G-level

(i) Figure 4(e):R-level

Figure 5: Correlations of two vertical adjacent pixels in Figure 1(a), Figure 2(b) and Figure 4(e)

3.2.1 NPCR and UACI

The Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are respectively defined by

$$\text{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\%, \tag{9}$$

$$\text{UACI} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} |A(i,j) - B(i,j)|}{255 \times m \times n} \times 100\%, \tag{10}$$

where

$$D(i,j) = \begin{cases} 0, & A(i,j) = B(i,j), \\ 1, & A(i,j) \neq B(i,j), \end{cases} \tag{11}$$

A and B are the original image and the encrypted one respectively.

We take Figure 3(b) and Figure 4(e) as the encrypted images for these two tests. Also we compare the results with [1]. Table 1 shows the results that our schemes perform as great as other two methods do in NPCR test. And in UACI test, scheme *Confusion on Pixels* performs much well while scheme *Diffusion on Coordinates* is similar to Zhu (PS).

3.2.2 Correlation of Two Adjacent Pixels

The *Correlation of two adjacent pixels* tests are performed in vertical, horizontal and diagonal directions with 2000 samples selected randomly.

Results are shown in Table 2, 3 and 4 for Figure 1(a), Figure 2(b) and Figure 4(e) respectively. Table 5 is cited from [1], which shows the correlation of two adjacent pixels in their methods. Comparing to Table 5, Table 3 and 4 show that our schemes perform very well in diffusion.

Table 1: Results of NPCR and UACI tests

Test	**NPCR (%)**			**UACI (%)**		
Level	R	G	B	R	G	B
Figure 2(b)	99.257	99.428	99.036	21.248	23.576	14.601
Figure 4(e)	98.843	98.8205	99.266	32.659	30.357	27.500
PCS[1]	99.42	99.60	99.54	27.78	27.66	24.94
Zhu (PS)[1]	99.26	99.45	99.13	21.41	23.42	15.08

Table 2: Correlation coefficients of two adjacent pixels in Figure 1(a)

Image	Figure 1(a)		
Level	R	G	B
vertical	0.97448	0.96853	0.87493
horizontal	0.95360	0.94160	0.84949
diagonal	0.92377	0.91441	0.81907

Figure 5 shows the Correlations distribution of two vertical adjacent pixels in Figure 1(a), Figure 2(b) and Figure 4(e) respectively. And Table 2, 3 and 4 show the correlation coefficients for them respectively.

Table 3: Correlation coefficients of two adjacent pixels in Figure 2(b)

Image	Figure 2(b)		
Level	R	G	B
vertical	-0.0086654	0.060830	-0.031240
horizontal	-0.044967	-0.053667	-0.0073068
diagonal	-0.021479	0.047668	0.0041064

Table 4: Correlation coefficients of two adjacent pixels in Figure 4(e)

Image	Figure 4(e)		
Level	R	G	B
vertical	-0.042666	-0.043872	-0.0008337
horizontal	0.0021105	-0.0060862	0.0041433
diagonal	0.014056	0.034820	-0.0026312

Table 5: Correlation coefficients of two adjacent pixels in PCS[1] and Zhu (PS)[1]

Method	PCS	Zhu (PS)
vertical	0.0581	0.3955
horizontal	0.1257	0.3913
diagonal	0.0504	0.3973

3.3 Key Space

The key space of *Diffusion on Coordinates* is determined by the number of the combination of the key in mapping ϕ, namely the amount of the combinations of $\boldsymbol{a}$. Clearly, It is $(2^n)^3 n^2 (2^n - 1)$. Let $f(n) = (2^n)^3 n^2 (2^n - 1) - 2^{4n}$, it is easy to prove that $f(n)$ increases with the increase of n. and $f(2) = 512$, hence $f(n)$ is greater than 2^{4n}. Consequently, the lower bound of the key space of *Diffusion on Coordinates* is 2^{4n}. For the case $n = 8$, it is 2^{32}.

Observe that the key in mapping ψ consists of $\boldsymbol{a}, \boldsymbol{p}$ and $\boldsymbol{u}$, by recalling the definitions of $\boldsymbol{p}$ and $\boldsymbol{u}$ in section 2., we obtain that the amount of combinations of $\boldsymbol{p}$ is $(2^n)^{m-1}$ and $(2^n)^m$ for $\boldsymbol{u}$, where $m \leq 2^n$. To get the upper bound of the key space of *Confusion on Pixels*, let $m = n$, consequently the upper bound $g(n)$ is $2^{4n} \times (2^n)^{2^n - 1} \times (2^n)^{2^n} = 2^{n(2^{n+1}+3)}$. Note that $g(n)$ is exponential of $n(2^{n+1} + 3)$ with base 2 and in case of $n = 8$, it is 2^{4120}, so we claim that the key space of *Confusion on Pixels* is huge enough. However, the mapping ψ is not injection, as it invokes inner product hence the lower bound is difficult to estimate.

4. CONCLUSIONS

In this paper, we propose two mappings over GF(2^n) one by one as well as two schemes that make use of them for image encryption. According to the experiment results and discussion about key space, we are sure that these two schemes are of high security, the former one is of strong resistance against cropping and of diffusion, and the latter one changes statistical characteristics significantly.

5. ACKNOWLEDGEMENTS

This work was supported by National Natural Science Foundation of China (No. 11071152) and Natural Science Foundation of Guangdong Province (No. 10151503101000023).

REFERENCES

[1] Nien, H. H., Changchien, S. K., Wu, S. Y., & Huang, C. K. (2009). *A new Pixel-Chaotic-Shuffle method for image encryption*. Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference, 883-887.

[2] Wang, R. Z., & Su, C. H. (2006). Secret image sharing with smaller shadow images. *Pattern Recognition Letters, 27*(6), 551-555.

[3] Shamir, A. (1979). How to share a secret. *Commun. ACM, 22*(11), 612-613.

[4] Wan, Z. X. (2003). *Lectures on finite fields and Galois rings*. Singapore: World Scientific Publishing Company.

[5] Grillet, P. A. (2007). *Abstract algebra* (Graduate Texts in Mathematics 242, 2nd ed.). New York: Springer.

[6] Fraleigh, J. B., & Katz, V. J. (2002). *A first course in abstract algebra*. MA: Addison-Wesley Publishing Company.

[7] Horn, R., & Johnson, C. R. (1991). *Topics in matrix analysis*. Cambridge: Cambridge University Press.