A Finite Field Cosine Transform-Based Image Processing Scheme for Color Image Encryption

Juliano B. Lima, Edmar S. da Silva, Ricardo Campello de Souza

Department of Electronics and Systems
Universidade Federal de Pernambuco

3rd IEEE Global Conference on Signal & Information Processing
Orlando/FL, USA December 14-16 2015

December 11, 2015

Outline

Introduction

- Applications for finite field and number-theoretic tranforms:
  - Signal processing: computation of error-free fast convolutions
  - Error-correcting codes: decoding in frequency domain
  - Information security: image encryption and watermarking
- In this paper, we introduce a new finite field transform:

Cosine Transform of Fields of Characteristic Two (FFCT)

- The FFCT can be applied to color images: each pixel of a 24-bit RGB image is treated as an element of $\mathrm{GF}(2^{24})$ and a 32-point 2-D FFCT is performed:
  - A transform-based scheme useful for application in image encryption is proposed.

Definition

Let $\zeta \in \mathrm{GF}(2^r)$ be an element of multiplicative order denoted by $\mathrm{ord}(\zeta)$. **The finite field cosine function** related to ζ is defined, for $x = 0, 1, \ldots, \mathrm{ord}(\zeta)$, as

$$\cos_\zeta(x) := \zeta^x + \zeta^{-x}.$$

Definition

Let $\zeta \in \mathrm{GF}(2^r)$ be an element such that $\mathrm{ord}(\zeta) = 2N - 1$. **The finite field cosine transform** of the vector $\mathbf{x} = (x_i)$, $x_i \in \mathrm{GF}(2^r)$, $i = 0, 1, \ldots, N-2$, is the vector $\mathbf{X} = (X_k)$, $X_k \in \mathrm{GF}(2^r)$, $k = 1, 2, \ldots, N-1$, whose components are

$$X_k := \sum_{i=0}^{N-2} x_i \cos_\zeta(k(i + 1/2)).$$

The components of the **inverse finite field cosine transform** are computed by

$$x_i = \sum_{k=1}^{N-1} X_k \cos_\zeta(k(i+1/2)).$$

The relationship between $\mathbf{x}$ and $\mathbf{X}$ can be expressed as

$$\mathbf{X} = \mathbf{C} \cdot \mathbf{x},$$

where $C_{k,i} = \cos_\zeta(k(i+1/2))$.

Important remarks:

- The FFCT can be related to the finite field Fourier transform (FFFT).
- Differently from the FFFT, the FFCT allows to define even-point transforms.
    - 2^r-point FFCT can be defined, which makes easier designing and implementing fast algorithms.
- While the *period* of $\mathbf{F}$ is 4, i.e., $\mathbf{F}^4 = \mathbf{I}$ (the identity matrix), matrix $\mathbf{C}$ has periods significantly larger and dependent of its dimension.
    - The FFCT can be considered as a potential candidate to be part of cryptographic schemes based on iterative transform computations.

The FFCT-Based Processing Scheme

We construct a 32-point FFCT over $\mathrm{GF}(2^{24})$:

- The field $\mathrm{GF}(2^{24})$ is generated using the element α, which is a root of the primitive polynomial $f(x) = x^{24} + x^7 + x^2 + x + 1$.
- We obtain the element $\zeta = \alpha^{\frac{2^{24}-1}{65}} = \alpha^{258111}$, such that $\mathrm{ord}(\zeta) = 65 = 2N - 1$ and $N - 1 = 32$.
- The elements of the corresponding transform matrix $\mathbf{C}$ are

$$C_{k,i} = \cos_\zeta(k(i+1/2)) = \left(\zeta^{\frac{1}{2}}\right)^{k(2i+1)} + \left(\zeta^{-\frac{1}{2}}\right)^{k(2i+1)}.$$

- The two-dimensional transform $\mathbf{M}$ of a 32×32 matrix $\mathbf{m}$ over $\mathrm{GF}(2^{24})$ is computed as

$$\mathbf{M} = \mathbf{C} \cdot \mathbf{m} \cdot \mathbf{C}^T. \qquad (1)$$

The FFCT-Based Processing Scheme

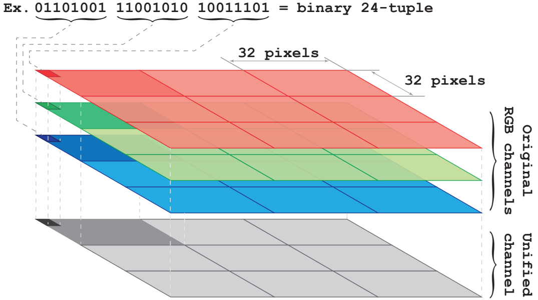


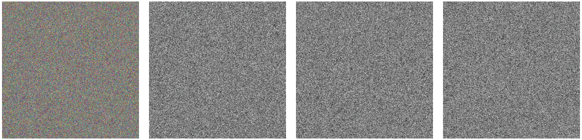
Figure: Procedure for representing an RGB image as a *unified channel* (matrix) of 24-bit numbers.

The FFCT-Based Processing Scheme

- Each binary 24-tuples of the *unified channel* is directly mapped into elements of $\mathrm{GF}(2^{24})$.
- Such a *unified channel* is divided into blocks with dimension 32×32, which are submitted to the 2-D FFCT according to Equation (1).
- The resulting transformed matrix is reconverted into a three channel transformed image denoted by $\mathbf{I}_t$.
- We expect that each channel of $\mathbf{I}_t$ has uniform histogram and low correlation among adjacent pixels.
- The original image $\mathbf{I}$ can be recovered from $\mathbf{I}_t$ using the inverse FFCT.

(a) (b) (c) (d)

Figure: (a) *lena.bmp*, (b) *peppers.bmp*, (c) *mandril.bmp*, (d) *lake.bmp*.



(a) (b) (c) (d)

Figure: Transformed versions of (a) *lena.bmp* and its (b) R, (c) G and (d) B channels.

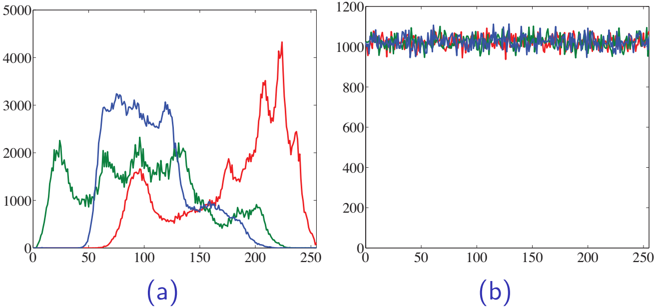
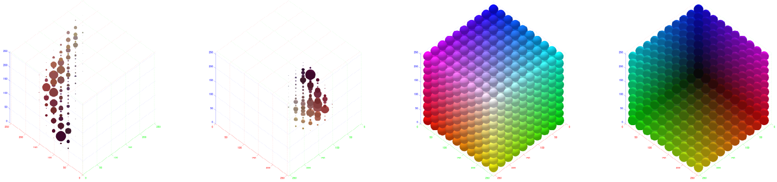


Figure: Histograms of color channels of (a) original and (b) transformed *lena.bmp*.

Computer Experiments and Security Aspects



(a) (b) (c) (d)

Figure: (a), (b) Color distributions of original *lena.bmp* in the RGB space; (c), (d) color distributions of transformed *lena.bmp* in the RGB space.

- The entropy of the color channels of the transformed images has assumed values varying from 7.9992 to 7.9994.
- These values are considerably close to 8, the entropy of a random source emitting 256 equiprobable symbols.

Table: Correlation coefficients of original (r_{xy}) and processed images ($\tilde{r}_{xy}$); (U) is related to unified-channel images; (R), (G) and (B) are related to individual channels.

Metric	*lena*	*peppers*	*house*	*mandril*
$r_{xy}(U)$	0.9671	0.9676	0.9679	0.8818
$\tilde{r}_{xy}(U)$	0.0029	-0.0016	-0.0021	0.0002
$r_{xy}(R)$	0.9892	0.9668	0.9582	0.8683
$\tilde{r}_{xy}(R)$	0.0061	-0.0070	0.0101	-0.0093
$r_{xy}(G)$	0.9825	0.9812	0.9397	0.7674
$\tilde{r}_{xy}(G)$	-0.0010	-0.0009	0.0066	0.0058
$r_{xy}(B)$	0.9571	0.9673	0.9678	0.8815
$\tilde{r}_{xy}(B)$	-0.0048	-0.0016	-0.0088	0.0008

Concluding Remarks

- We have introduced a cosine transform over fields of characteristic two and demonstrated its applicability in color image processing.
- Our approach is immune to rounding-off errors and allows using the same digital encoding scheme in both spatial and transform domains.
- The method we have proposed modifies visual and statistical properties of an image, which makes it adequate to be used as a key-independent portion of an image encryption scheme.
- A key-dependent stage must be included to perform image encryption.

Acknowledgements

- Questions?
- E-mail: juliano_bandeira@ieee.org

Universidade Federal de Pernambuco

CNPq — Conselho Nacional de Desenvolvimento Científico e Tecnológico

FACEPE — Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco