Applied Mathematics and Computation 334 (2018) 343–355

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Fresnelet approach for image encryption in the algebraic frame

Shabieh Farwa[a], Nazeer Muhammad[a,*], Nargis Bibi[b], Sajjad A. Haider[c], Syed R. Naqvi[c], Sheraz Anjum[d]

[a] Department of Mathematics, COMSATS Institute of Information Technology, Wah Campus, Pakistan
[b] Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan
[c] Department of Electrical Engineering, COMSATS Institute of Information Technology, Wah Campus, Pakistan
[d] Department of Computer Science, COMSATS Institute of Information Technology, Wah Campus, Pakistan

ARTICLE INFO

Keywords:
Fresnelet transform
Galois field
$\mathbb{F}_2{}^n$
Primitive element
Multiplicative cyclic group
Chaos

ABSTRACT

In this manuscript, a novel, more efficient method to encrypt an image in the Fresnelet domain is proposed. The uniqueness of the presented algorithm depends on the Fresnelet transform based image decomposition in conjunction with an algebraically synthesized substitution box. The high- nonlinearity induced by the eccentrically designed S-box boosts the security of proposed scheme. In this two-steps encryption algorithm, firstly, we apply the Fresnelet transform to propagate information with desired wavelength at a specified distance. This results in the decomposition of the secret image data into four complex subbands. These complex sub-bands are further partitioned into real subband data and imaginary subband data. At second step, the net subband data, produced at the first level, is diffused by a unique iterative substitution approach based on the algebraic structure of Galois field $\mathbb{F}_2^8$. In the diffusion process, the permuted image is substituted via algebraic substitution algorithm. We prove through significant analysis techniques that the proposed scheme offers a highly elevated security level in encryption.

1. Introduction

In recent years, an expeditious build-out of advanced tools for secret data exchange is observed. This evolution has made data security an integral part of digital communication process. Generally, an increased amount of confidential information is stored while using internet, so an elevated security is demanded against unwanted surveillance, thieving, and bogus publicity. In this regard, image encryption is considered to be a primitive technique which exposes images to unrecognizable ciphers. The information, converted to dummy data, can only be understood by the intended recipient only, who knows the process to unmask it by exclusive key specification. Encryption of data enables its confidentiality, integrity, and authentication [1–13].

The cryptographic developments highlight the significant contribution of the substitution box (S-box) in a substitution-permutation network [1]. An S-box plays critical role to induce nonlinearity and complexity in our data. The imperative

* Corresponding author.
E-mail addresses: drsfarwa@gmail.com (S. Farwa), nazeermuhammad@ciitwah.edu.pk, nazeer@hanyang.ac.kr (N. Muhammad), nargis@fjwu.edu.pk (N. Bibi), sajjadali@ciitwah.edu.pk (S.A. Haider), rameeznaqvi@ciitwah.edu.pk (S.R. Naqvi), drsherazanjum@gmail.com (S. Anjum).

https://doi.org/10.1016/j.amc.2018.03.105
0096-3003/

features of an S-box are used to increase confusion creating capability [14,15]. Due to the highly exigent involvement of S-box, many algorithms to constitute safer S-boxes have been focus of attention [14,16,34–38]. Further applications of S-boxes in image ciphering, water marking as well as in steganography have been trended and quite popular [4–9,13,27].

In modern literature, many advanced and comparatively more reliable techniques of image encryption have become focus of study. Liu and Wang [17] introduced image encryption algorithm using one-time keys. In [20], an encryption algorithm with spatial bit-level permutations in conjunction with high-dimension chaotic systems is proposed. [21], addresses a new technique in which R, G, B components affect the encryption of one another. In [19], the authors deploy mixed linear-nonlinear coupled map lattices in image encryption. [28] instigates the spatiotemporal non-adjacent coupled map lattices. [24,26] present image encryption using dynamic growth model and DNA sequence operations respectively. Another effective encryption method by using chaotic dynamic S-boxes is discussed in [27]. Some other most recent image encryption techniques are detailed in [2,3,18,22,23,25]. Use of DCT and FFT for encryption purposes has been studied in many techniques [29–32]. However, according to the best of our learning, there is no previous work on the applications of the Fresnelet transform in agreement with S-box cryptography. The main motivation for the presented method is to utilize the flexible features of the Fresnelet transform depending upon the subband decomposition along with high level of confusion induced in data by S-box. In this frame work, we use cryptographic structure in the Fresnelet domain to manipulate the significant information of the secret data.

Chaos theory has undoubtedly offered revolutionary advancements in the multimedia security applications. Along with many other remarkable requisitions, the use of chaotic systems in construction of stronger S-boxes is worth-studying [7–12]. A quick review of the chaos based S-box algorithms shows that extra ordinary performance parameters are achieved because of the sensitivity of chaotic maps towards the initial conditions. However it is important to investigate simpler and more straight forward dynamic structures, sensitive to initial conditions that could offer appropriate substitute to chaotic systems at low computational labour. We propose an S-box construction that shows high responsiveness to the change in initial condition. However the underlying approach attains exalted proficiency results just by an algebra based direct iterative map. We further discuss an effective application of this iterative substitution box in image encryption by a unique perspective involving Fresnelet transform.

The forward and backward combination Fresnelet has been utilized to construct the factitious sets of the secret data for obtaining the variation of intensity values [42]. The Fresnelet transform has been modeled at first place, for the purpose of rebuilding the digital holography with large resolution [43]. Thus, it perhaps workable to decompose and retrieve the content of digital multimedia for encryption purpose to give higher security and reliability [39]. Furthermore, through the Fresnelet transform by using large resolution information for an encrypted data to retrieve the meaningful information [40]. The basic aspects of the Fresnelet transform are passed down to evaluate an unambiguous knowing of concealed communication contents. At encryption phase, the resolution level of the given image data and retrieving the exact resolution at decryption phase are vital to a secure transmission of the concealed contents. By using the Fresnelet transform a multistage resolution of secret information is developed using the vigorous key specifications. Moreover, to achieve highly nonlinear encryption, S-box ciphering approach yields next level secure and private data. The important significance of the proposed method is driven of inaccessible data to get the hidden data with no means of the true keys, even if an intruder is familiar of the data-hiding algorithm.

Remaining part of the writing is arranged as follows. Section 2 provides a theoretical explanation of the Fresnelet transform. Section 3 demonstrates the detailed algorithm used to develop an algebra-based S-box. The cryptographic forte of the S-box is examined in Section 4, through some highly significant parameters. The Sections 5–9 present a comprehensive model for encryption and decryption, including simulations and evaluations. Lastly Section 10 concludes the paper.

2. Fresnelet transform

The propagation phenomena of wave are structured via diffraction principle using the Fresnel transform [43]. The Fresnel transform in wavelet domain produces the bases of Fresnelet transform. These bases are derived to restore the digital off-axis hologram with certain composition of parameters. These can be tuned to desired level of the resolution, adjusted with particular wavelength and the specific range between observing plane to the objects of propagation. Fresnelet transform is used to simulate the approximation criteria of the monochromatic waves propagation. This monochromatic wave is shown as a function $\Lambda \in \Omega_2(\mathbb{R})$, with the Fresnel transform model in terms of convolution integral as follows:

$$\widetilde{\Lambda}_\tau(p) = (\Lambda * k_\tau)(p) \quad \text{with} \quad k_\tau(p) = \frac{1}{\tau} exp\left(i\pi \frac{p^2}{\tau^2}\right), \tag{1}$$

The kernel $k_\tau(p)$ is the one-dimensional wave propagation with the parameter of normalization $\tau > 0$, where, τ depends on the propagating range d, and the wavelength value λ as shown:

$$\tau = \sqrt{\lambda d} \tag{2}$$

Moreover, the kernel $k_\tau(p)$ can be extended to two-dimensional wave propagation using the tensor product for $\Lambda \in \Omega_2(\mathbb{R}^2)$, as follows:

$$\widetilde{\Lambda}_\tau(p,q) = (\Lambda * K_\tau)(p,y) \tag{3}$$