Spiral-Phase Masked Optical Image Healthcare Encryption System for Medical Images Based on Fast Walsh-Hadamard Transform for Security Enhancement

Mehak Khurana, The NorthCap University, Gurgaon, India
Hukum Singh, The NorthCap University, Gurgaon, India

ABSTRACT

This article describes how a new digital spiral phase masked encryption scheme is proposed for healthcare system based on the Fast Walsh-Hadamard transform (FWHT) to enhance the security of the health-related information systems. The proposed encryption system uses the brain scan image to encrypt brain information from the unauthorized access. Spiral mask used here is a hybrid of Radial Hilbert Mask (RHM) and Toroidal Zone Plate (TZP) Mask which makes the key strong and enhances the security. Proposed schemes not only increase the key space but also increases the number of parameters which makes it difficult for an attacker to find exact key to recover original image. Another advantage of this proposed scheme is FWHT which reduces the quantization error that helps in reconstructing the brain image and information perfectly. The robustness of the proposed cryptosystem has been analysed by simulating on MATLAB 8.1.0(R2012b). The experimental results are provided to highlight the effectiveness, robustness and suitability of the proposed cryptosystem that prove the system can be used in healthcare data encryption.

KEYWORDS

Fast Walsh Hadamard Transform, Spiral Mask, Radial Hilbert Mask, Symmetric Key Algorithm, Toroidal zone plate Mask

1. INTRODUCTION

The digital communication has become challenge to transmit the data securely. Digital images are used in many applications such as healthcare, biometric, military applications, police identification etc. Healthcare data is an important digital data when it comes to storing sensitive personal data. These personal health data images can easily be accessed by unauthorized person or hacker and can be transmitted over a communication network. Health care data encryption is required in the form of data security whereby electronic medical records (EHR) should be disguised so that unauthorized users may not be able to read or make sense of them. Personal health information (PHI) including medical diagnoses, surgeries and other sensitive health data needs to be secured to guard against malicious motives as well as confidentiality breaches that can result in huge fines. Therefore, optical image encryption can be used as secure method for communication. Many new optical image encryption (Matoba et al., 2009; Alfalou & Brosseau, 2009; Millan & Perez-Cabre, 2011) (Javidi et al, 2016) schemes for reliable and secure transmission in this direction have been proposed. Double Random
Phase Encoding (DRPE) is one of the well-known and successful classical optical image encryption technique proposed by Refregier and Javidi (Refregier & Javidi, 1995) so far. In DRPE, aim is to encode the plain image by converting it into stationary white noise called cipher image by applying two random phase diffusers (masks), one in input plane and another in Fourier plane in 4-f system. DRPE with Fourier suffers from many attacks and other security issues. Therefore DRPE was further performed with different transformations such as Fractional Fourier transform (Unnikrishnan et al., 2000; Liu et al., 2014; Zhou et al., 2010; Singh, 2016), Fresnel transform (Matoba & Javidi, 1999; Situ & Zhang, 2004; Singh H et al., 2015), Gyrorator transforms (Rodrigo et al., 2007; Singh et al., 2014; Singh et al., 2015), Cosine transform (Wu et al., 2010), Hartley transform Chen & Zhao, 2006), Arnold transform (Abuturab, 2013) and Mellin transform (Zhon et al., 2011; Zhou et al., 2015; Vashisth et al., 2014) to enhance the security. Due to its symmetric and linear nature this technique brings fatal damage to the reliability as it is vulnerable to many attacks such as chosen plain image attack, chosen cipher image attacks, known plain image attack and cipher image only attack (Kumar et al., 2016; Peng X et al., 2006; Carnicer et al., 2005) and suffered from various practical problems. To overcome these issues several other optical image encryption techniques based on DRPE concepts have also been proposed in the literature. They are digital holography (Nishchal et al., 2004), multiplexing (Situ & Zhang, 2005; Matoba & Javidi, 2004; Chen & Zhao, 2006), polarized light (Gopinathan et al., 2006), and interferometry (Li, 2009; Masajda & Dubik, 2001; Vyas & Senthilkumaran, 2007). To enhance more security and to meet requirements of latest applications, DRPE with Fast Walsh hadamard transform (FWHT) has been introduced (Zheng & Huang; Fino & Algazi, 1976). FWHT has been used in the cryptosystem as it protects from the quantization error and image can be perfectly reconstructed. This scheme also includes a strong key as according to the Kerckhoﬀ’s principle, security is based on the strong key i.e. assuming that encryption algorithm is public and is known to the attacker but the resistance of the algorithm should be based on secrecy of the key. Finding out the key should be very diﬃcult so therefore new spiral phase mask has been used here for encryption process which increases the key space and makes it robust to many standard attacks.

In this paper, a new spiral-phase masked symmetric image encryption technique based on Fast Walsh Hadamard Transform (FWHT) is proposed. In this technique two masks have been used one is random phase mask (RPM) other is spiral phase mask (SPM). One is used in input domain and other is used in frequency domain. To generate the spiral phase mask, two masks have been combined one is Radial Hilbert Mask (RHM) (Jeffrey et al., 2000; Lohmann et al.1997; Joshi et al. 2008) and other is Toroidal Zone Plate (TZP) (Barrera et al. 2005; Barrera et al., 2005; Singh, 2016). Mask aimed with not only improving the security but also increasing the key space. In this encryption process, we have an input plain-image that is multiplied by a random phase mask in input domain and then with spiral phase mask in frequency domain to get final encrypted image. This is based on FWHT which has low quantization error with which the quality brain scan image and Lena image can be recovered as compared to other orthogonal transforms. This scheme also enhances the security by increasing the number of parameters as SPM used is hybrid of two keys Radial Hilbert Mask and toroidal zone plate mask that increases the key space and makes it difficult for an attacker to find the actual key and image.

2. PRINCIPLE

2.1. Fast Walsh Hadamard Transform

New communications systems are dependent on the techniques which recover the quality information even in the presence of noise and interference. One of the technique used to achieve this goal is called Hadamard matrices which can be used many applications. This paper concentrates on the fast Walsh Hadamard transform where Hadamard matrices are used. Walsh Hadamard Transform (WHT) is known as generalized class of Fourier Transforms (FT). It performs linear, symmetric, orthogonal
Related Content

A Classification Analysis of the Success of Open Source Health Information Technology Projects
www.igi-global.com/chapter/classification-analysis-success-open-source/49868?camid=4v1a

A Healing Journey with a Thousand Echoes
www.igi-global.com/chapter/healing-journey-thousand-echoes/49240?camid=4v1a
Appointment Order Outpatient Scheduling System with Consideration of Ancillary Services and Overbooking Policy to Improve Outpatient Experience
[www.igi-global.com/chapter/appointment-order-outpatient-scheduling-system/56259?camid=4v1a](www.igi-global.com/chapter/appointment-order-outpatient-scheduling-system/56259?camid=4v1a)

Volumetric Analysis and Modeling of the Heart Using Active Appearance Model
[www.igi-global.com/chapter/volumetric-analysis-modeling-heart-using/13086?camid=4v1a](www.igi-global.com/chapter/volumetric-analysis-modeling-heart-using/13086?camid=4v1a)