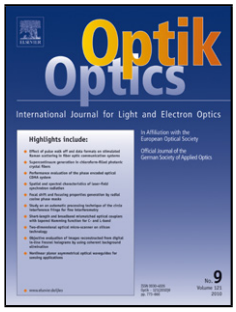

Title: Medical image encryption based on improved ElGamal encryption technique

Author: Laiphrakpam Dolendro Singh Khumanthem Manglem Singh

PII: S0030-4026(17)30920-8
DOI: http://dx.doi.org/doi:10.1016/j.ijleo.2017.08.028
Reference: IJLEO 59491

To appear in:

Received date: 20-4-2017
Accepted date: 2-8-2017

Please cite this article as: Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh, Medical image encryption based on improved ElGamal encryption technique, *<![CDATA[Optik - International Journal for Light and Electron Optics]]>* (2017), http://dx.doi.org/10.1016/j.ijleo.2017.08.028

Medical image encryption based on improved ElGamal encryption technique

Laiphrakpam Dolendro Singh[a,*], Khumanthem Manglem Singh[a]

[a]*Department of Computer Science and Engineering, National Institute of Technology, Manipur, 795001*

Abstract

Elliptic curve analogue ElGamal encryption scheme requires encoding of the plain message onto elliptic curve coordinate using Koblitz encoding technique before encryption operation. The paper proposes a medical image encryption scheme using improved ElGamal encryption technique. A new finding has been made in the proposed method where separate calculations for encoding plain message to elliptic curve coordinate is removed. The algorithm in the improved version of ElGamal encryption scheme is designed to encrypt medical image where data expansion issue is resolved and execution speed is enhanced. The strength of the proposed method is insured through various statistical and security analyses and comparison with other existing encryption schemes.

Keywords: Elliptic curve cryptography, image encryption, ElGamal cryptosystem, Koblitz encoding technique

1. Introduction

Advancement in technology has helped the medical community to capture images from various part of a living being. Like other sensitive data, medical images require security while transferring through the insecure channel of communication for various purposes such as segmentation, denoising etc. The cryptographic operation can help in providing the necessary security by ciphering the medical image to some unintelligible format using a symmetric or asymmetric key encryption scheme. Hongjun *et al.* [1] proposed an asymmetric encryption scheme for encryption of color pathological image based on the Dadras complex hyperchaotic system. The initial conditions for the chaotic system is generated by taking 512-bits secure hash algorithm (SHA) value of the plain image. The scheme has got key size large enough to resist brute-force attack and got good sensitivity to the key used. Dai *et al.* [2] proposed a medical image encryption algorithm based on confusion and diffusion operation performed using Arnold's transformation and two chaotic systems, Logistic map and Henon map. The Logistic map is used to generate the initial conditions for Henon map and Arnold's transformation is used for generating a scrambled medical image. The Henon map is used to generate the chaotic sequence which is XOR with the scrambled medical image, generating the cipher image. Though chaos system has got various

*Corresponding author
Email address: ldsingh.cse@gmail.com (Laiphrakpam Dolendro Singh)