International Journal of Rough Sets and Data Analysis
Volume 7 • Issue 1

A Novel Approach to Enhance Image Security using Hyperchaos with Elliptic Curve Cryptography

Ganavi M, Jawaharlal Nehru New College of Engineering, India
Prabhudeva S, Jawaharlal Nehru New College of Engineering, India

ABSTRACT

Information securities dominate the world. All the time we connect to the internet for social media, banking, and online shopping through various applications our priceless data may be hacked by attackers. There is a necessity for a better encryption method to enhance information security. The distinctive features of elliptic curve cryptography (ECC) include key atomity, speedy ciphering, and preserving bandwidth captivating its use in multimedia encipher. An encryption method is proposed by incorporating ECC, Secure Hash Algorithm – 256 (SHA-256), Arnold transform, and hyperchaos. Randomly generated salt values are concatenated with each pixel of an image. SHA-256 hash is imposed which produces a hash value of 32-bit, later used to generate the key in ECC. Stronger ciphering is done by applying Arnold's transformation and hyperchaos thereby achieved more randomness in image. Simulation outcomes and analysis show that the proposed approach provides more confidentiality for color images.

KEYWORDS

Arnold Transform, Decryption, Elliptic Curve Cryptography, Encryption, Hyperchaos, MSE, PSNR, Salting, SHA-256

INTRODUCTION

Secured digital image communication is possible by one of the means like Image encryption. Securing the characteristics of image data is predominant in medical, military, and commercial domains. Safeguarding interactive media intelligence against prohibited access became a critical issue in our routine. Minutiae of images are also surveyed & deployed by third-party which leads to immeasurable damage for the image proprietor. To overcome such difficulties, digital image techniques are mandatory to be applied to images to encrypt before transmitting them. Information security is required to reduce the risk level that is tolerable to the business. Security challenges for sensitive data exchange through online networks are confidentiality, authenticity, integrity, non-repudiation, and availability. The conventional encryption standards are not able to fulfill the demands of image scrambling. The chaotic nature of hypersensitive to inceptive state and system framework, no recurrence, and generating unpredictable codes. The resultant chaotic sequence is accurate (Huang et al., 2018) and it is of great significance in encryption algorithms.

Hash functions are tremendously beneficial in cryptography. These functions emerge as a prominent role in the applications of data security. They can accomplish preservation, perfection,

DOI: 10.4018/IJRSDA.288520

and regularity of data, authenticate a message and guarantee the authenticity by a digital signature (Seyedzade, 2010; Wang, 2018). It should obtain different security properties like collision resistance, pre-image resistance, and pseudo-randomness. The most commonly used hash algorithm, SHA-256 results in a unique 32-byte hash value for input data. This value may be used as a key to encrypt data. The generated key value is different for different input data. Image scrambling can be carried out by applying Arnold transformation (Min et al., 2013). The significant feature of this transformation is that it uses periodicity. The number of iterations to recover back original input is calculated based on the image size. Arnold transformation is enforced pixels as well as continued to image chunks which enhances the robustness and security level (Sathish, 2019). A cryptographic hash is required in securing the passwords or secret images when stored in memory to protect them from birthday and dictionary attacks. So always it is recommended to apply hash on a combination of salt and passwords or important pictures (Gauravaram, 2012).

ECC (Koblitz, 1987; Miller, 1985) uses smaller key sizes compared to Rivest, Shamir & Adleman (RSA) thereby providing more security (Bakr et al., 2018). It is the next level to asymmetric cryptosystem on the numerical design of structures over finite fields (Gutub et al., 2007; Laiphrakpam and Khumanthem, 2018; Koblitz, 1987; Ziad et al., 2018).

ECC has been a recent analysis topic within the space of information security (Kamalakannan and Tamilselvan, 2015; Vigila and Muneswaran, 2009; Roy et al., 2014). The proposed method uses ECC for generating the key required to encrypt/decrypt process for secure transfer of input image. A salt is randomly generated to the size of an image. An obtained random number is concatenated with each pixel value of an input image. Applying SHA-256 hashing on this image will generate a 32-byte hash value. The key to the elliptic curve point is communal in the middle of the sender and receiver. The number of times Arnold's transformation (Min et al., 2013) was carried is based on the value of the elliptic curve point. This point value is also applied to achieve the initial framework of the hyperchaos system. The resultant hyperchaos output is XOR with Arnold's transformed image (Sathish, 2019; Kaur and Talwar, 2017) to generate the cipher image. This proposed method prevents the necessity of communication of the look-up table information.

LITERATURE SURVEY

Avoiding intermediate knowledge from unofficial usage has become a critical and sensitive issue in this internet era. A novel approach has been suggested by adopting chaos and SHA-1(Slimane et al., 2017). Confusion and diffusion processes are applied to images to encrypt. An approach with a two-diffusion process and SHA-1 to obtain a private key based on nested chaotic encryption has been proposed (Slimane et al., 2016). Various security analyses, tests, and attacks are also explained. A hash function is suggested based on a chaotic system (Wadhwa et al., 2016). Input data is divided into pieces and passed through chaos separately. This approach uses the block ciphering technique which uses a plain image. High-dimensional chaotic systems have been proposed (Qi et al., 2016). Lorenz mapping is used to generate the Hyperhenon to improve the keyspace.

A comprehensive survey on chaotic image secret writing schemes is presented (Singh et al., 2018). Chaotic secret writing is extraordinary compared to other approaches to accomplish security. An image secret writing scheme using chaotic maps has been applied. A hybrid approach has been proposed by applying the permutation of input data using hyperchaos (Hassene and Eddine, 2016). Scrambling text and pictures is recommended in this approach resulting in the reduction of computational cost and better permutation. The SHA-2 algorithm is presented (Ibrahim et al., 2015). Scrambling and diffusion stages are presented (Salagundi et al., 2016). Circular operation in row and column scrambling is considered. A chaotic map is applied to each row and column to scramble. Parity is used in modifying picture elements for the diffusion stage.

A structure has been proposed (Abdoun et al., 2016) that blends the chaotic generator into neurons. Pixel shuffling and chaotic map methods are presented (Chaitanaya et al., 2015). This algorithm uses