# Image Based Data Encryption Algorithm with Dynamic Rounds (IBDEA-DR)

Mohd Iqbal Bhat
*Department of Computer Science*
*Islamic University of Science & Technology Awantipora, Pulwama, Jammu & Kashmir, India*

Kaiser J. Giri
*Department of Computer Science*
*Islamic University of Science & Technology Awantipora, Pulwama, Jammu & Kashmir, India*

**Abstract- The purpose of this paper is to introduce a new simple, secure and efficient symmetric key cryptographic method named Image Based Data Encryption Algorithm with Dynamic Rounds (IBDEA-DR) with some unique features first time introduced to the world of cryptology. It is the first cryptosystem where a monochrome digital image is used as key for both encryption and decryption of digital data. The Dynamic Round Capability (DRC) i.e., number of rounds applied on a particular plain text block vary with its block number adds to the security of the cryptosystem and guards against various kinds of cryptanalyst attacks. The number of rounds applied range from 8 to 18 and in each round S-Boxes generated using RC4 Algorithm, P-Boxes and two important operations named Left Static Bitmap Operation and Right Static Bitmap Operation are applied. The algorithm is designed to encipher and decipher blocks of data consisting of n-bits under the control of two n-bit master keys named Row Master Key ($K_r$) and Column Master Key ($K_c$) which are generated from a monochrome digital image of size nxn pixels where $n = 2^k$.**

**Keywords – Confusion, Data encryption, Diffusion, Dynamic Round Capability (DRC), Image Based Data Encryption Algorithm (IBDEA-DR), P-Box, S-Box, Symmetric Key Cryptosystems.**

## I. INTRODUCTION

The rapid advancement in communication technology and the mass utilization of communicating devices over the last decade has exponentially increased the number of communication users and also compelled many people to share their information over the Internet. As the security breaching has become a common issue in different forms of networks, the demand for adequate security to electronic data transmitted over open channels has exponentially increased and consequently received a lot of attention from researchers around the world. Cryptography plays a vital role in the security of data transmission and protects data against active and passive fraud. Cryptography provides solution for secure networks and communication.

The whole point of cryptography is to solve problems involving secrecy, authentication, integrity and dishonest people [1]. Cryptographic techniques are among the best known ways to protect both the confidentiality and integrity of data. Cryptography is the science of disguising messages so that only the intended recipient can decipher the received message. Cryptography is the lynchpin of data security. Besides providing for message confidentiality, it also helps in providing message integrity, authentication and digital signatures. Without it, e-banking, e-trading, and e-commerce would simply not be a reality [2].

The original message or document to be transferred is called plain text and its disguised version is called cipher text. The process of disguising the original plain text is called encryption and the process of receiving the original plain text from the cipher text is called decryption.

Encryption involves the use of an encryption function or algorithm, denoted by E, and an encryption key e. Likewise, decryption involves the use of a decryption function denoted by D, and a decryption key d. These operations are summarized below:

$$C = E_e (P) \text{ and}$$
$$P = D_d (C)$$

Here, P denotes a block of plain text and C denotes the encrypted cipher text.

According to Kerckhoff's Principle [3]: 'The secrecy should be in the key used for decryption, not in the decryption or encryption algorithm'. Modern ciphers are based on this principle.