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.

In a symmetric or secret key cryptography, a single key is used for encryption as well as decryption. So e=d in the above equation. The symmetric key cryptography schemes can either be stream ciphers or block ciphers. Stream ciphers operate on a single bit at a time and implement some form of feedback mechanism so that the key is constantly changing. On the other hand, a block cipher encrypts one block of data at a time using same key in each block.

According to Shannon two general principles of block ciphers are diffusion ad confusion [4]. Diffusion is spreading of influence of one plain text bit to many cipher text bits with intension to hide the statistical structure of the plain text. Confusion is transformations that change dependence of the statistics of cipher text on the statistics of plain text. In most cipher systems the diffusion and confusion is achieved by means of round repetition. Repeating single round contributes to ciphers simplicity. Modern block ciphers consist of four transformations: substitution, permutation, mixing and key adding.

There are several cryptographic algorithms widely used today. The best known secret key cryptosystems are the Data Encryption Standard (DES), Advanced Encryption System (AES), Blowfish, RC4, etc. Each cryptosystem has its strengths and weaknesses. Choosing a particular cryptosystem depends upon a variety of factors. These include ease of implementation (in hardware and/or software), hardware requirement (no. of gates, memory, etc.), performance characteristics, and security.

Designing a secure and efficient symmetric key cryptosystem continues to be a challenging area of research in recent years. In this paper we present a new method for designing an efficient, secure yet simple secret key cryptosystem. We are using a bit map matrix generated from a monochrome digital image to generate the keys used for both encryption as well as decryption of data. This bit map is also utilized during the intermediate steps of each round. Another uniqueness of this cryptosystem is its Dynamic Round Capability (DRC) i.e., the number of rounds applied on a particular plain text block vary from 8 to 16 rounds depending on its block number in the original plain text. One more peculiarity of this cryptosystem is its capability to work on any key and block sizes and is determined by the size of the digital image used.

The outline of this paper is as follows. Section II defines some notations used in this paper. Section III presents the details of encryption and decryption procedures of IBDEA-DR. Security analysis of the proposed cryptosystem is discussed in section IV. Finally the section V presents the conclusion.

II. NOTATIONS

The following notations are used throughout this paper:

1. $n = 2^k$ is the block and key size in bits.
2. Block_no = It denotes the block number of the plain text block and starts from 0.
3. Image_bit_map[n] [n] = An nxn binary square matrix containing the binary pixel values generated from a monochrome digital image.
4. K_r = The Row Master Key.
5. K_c= The Column Master.
6. L_k = Denotes the leftmost k bits.
7. L_{n-k} = Denotes the leftmost n-k bits
8. R_k = Denotes the rightmost k bits
9. R_{n-k} = Denotes the rightmost n-k bits.
10. val (L_k), val (R_k) = Denotes the decimal value of leftmost k bits and rightmost k bits respectively.
11. R_{n-k} (image_bit_map[val (L_k)] [ ]) = Denotes the rightmost n-k bits of the row of image_bit_map[ ] [ ] matrix selected by the value of the leftmost k bits of the intermediate cipher block.
12. L_{n-k} (image_bit_map[val (R_k)] [ ]) = Denotes the leftmost n-k bits of the row of image_bit_map[ ] [ ] matrix selected by the value of the rightmost k bits of the intermediate cipher block.

III. PROPOSED ALGORITHM

In this section we present our secret key cryptosystem named Image Based Data Encryption System with Dynamic Rounds (IBDEA-DR). IBDEA-DR is a symmetric key block cipher with dynamic rounds and having Cipher Block Chaining (CBC) mode of operation. IBDEA-DR supports block and key sizes of equal lengths which is determined by the size of the monochrome digital image used. The algorithm is designed to encipher and decipher blocks of plain text data consisting of n-bits under the control of n-bit keys generated from an nxn pixel monochrome digital image. The n can be any power of 2 ranging from 64 to 512 bits. The output of IBDEA-DR is an n-bit block of cipher text. Decryption takes n-bit input of cipher text analogue with n-bit keys generated from an nxn pixel monochrome digital image and produces an n-bit output of plain text. The encryption process takes varying rounds ranging from 8 to 18 rounds. In each round n/8 number of 8→8 S-Boxes are applied followed by a straight

permutation and two important image bit map matrix (image_bit_map [ ] [ ]) dependent operations named left static bit map operation and right static bit map operation.

The diagram in Figure 1 shows the general outline of IBDEA-DR.

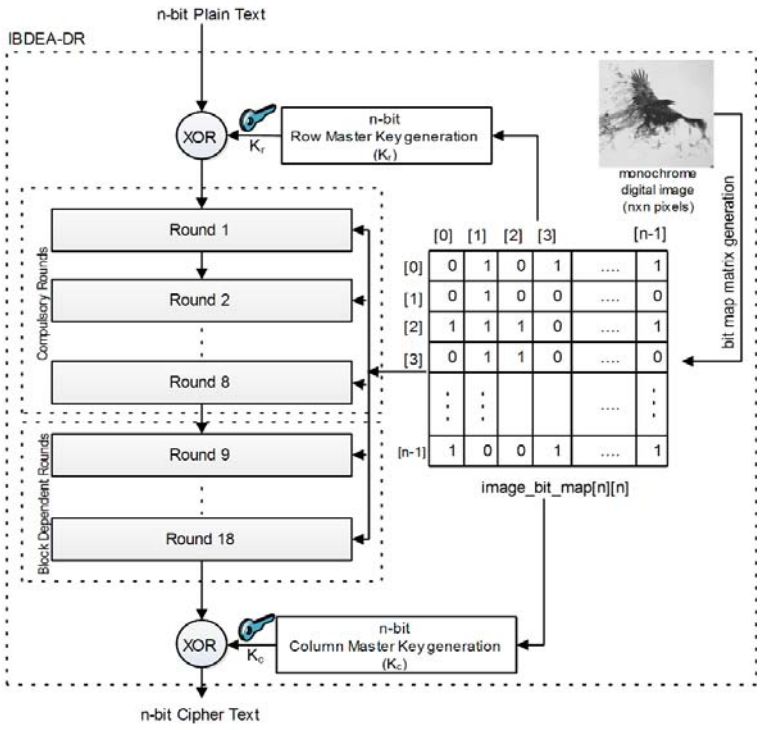

Figure 1. General Outline of IBDEA-DR

We explain the algorithm in the following stesp-

3.1 Image Bitmap matrix Generation –

The first step in this algorithm is to generate the bit map matrix from the nxn pixel monochrome digital image and is denoted by image_bit_map[n] [n] matrix i.e., an nxn square matrix containing the binary pixel values of the image. This matrix is the heart of this algorithm. The actual procedure for generation of such matrix is not discussed in this paper as it is more language dependent. The actual implementation will depend on the language used for implementation of the cryptosystem.

3.2 Row Master Key (K_r) Generation –

Next we generate the n-bit Row Master Key (K_r). The procedure to generate Row Master Key (Kr) is as follows:

1. Get the n-bit 0^{th} row of the image_bit_map [ ] [ ] matrix and denote it by R_0
   $R_0 \leftarrow$image_bit_map [0] [ ]
2. Get the decimal values of each Byte of R_0 starting from left to right and denote by $B_0,B_1,B_2,\ldots\ldots B_k$.
3. Extract the B_0^{th}, B_1^{th}, B_2^{th}, ……, B_k^{th} rows from image_bit_map [ ] [ ] matrix and denote by R_{B0}, R_{B1}, R_{B2},…. R_{Bk}.
4. Finally perform the XOR of these rows to generate the Row Master Key (K_r) as follows:
   $K_r = (R_{B0} \oplus R_{B1}) \oplus (R_{B2} \oplus R_{B3}) \oplus \ldots.. \oplus (R_{Bk-1} \oplus R_{Bk})$ if no. of rows is even
   $K_r = (R_{B0} \oplus R_{B1}) \oplus (R_{B2} \oplus R_{B3}) \oplus \ldots.. \oplus R_{Bk}$ if no. of rows is odd

3.3 Column Master Key (K_c) Generation –

The procedure for generation of Column Master Key (K_c) is same as that of Row Master Key (K_r) with the only difference that instead of rows, columns of image_bit_map [ ] [ ] matrix are used. Since matrix operations on rows are easier than columns, so while generating Column Master Key (K_c) we first perform a matrix transpose on the image_bit_map [ ] [ ] matrix and then use the same procedure of Row Master Key (K_r) generation to generate the Column Master Key (K_c).

3.4 Row Master Key (K_r) Mixing –

After Row Master Key (K_r) generation, the first operation performed on the n-bit plain text block is Row Master Key (K_r) mixing. Here the n-bit plain text is XORed with the Row Master Key (K_r). This is the only step where the Row Master Key (K_r) is applied.

3.5 Round Operations –

After the Row Master Key (K_r) mixing, the operation of a round starts. Unlike other data encryption algorithms where a fixed number of rounds are applied for a particular key size, this algorithm has the unique feature of Dynamic Round Capability (DRC). The number of rounds applied on a particular block varies from 8 to 18 depending on the block number of the particular plain text block. Each of these rounds is functionally identical. The only difference arises due to the different part of a row of image_bit_map [ ] [ ] matrix that is applied in a particular round. The general structure of a round in IBDEA-DR is shown in Figure 2.

Each round employs following four steps:

1. Byte Substitution.
2. Straight Permutation.
3. Left static bitmap operation.
4. Right static bitmap operation.

3.5.1 Byte Substitution –

This is an important step in this algorithm to achieve the property of confusion. It involves replacing each Byte with another Byte using an S-Box. Since the S-Box layer is considered to be most hardware resource consuming construct, the S-Boxes as proposed in [5] are suggested for this cryptosystem which are based on the RC4 algorithm [6]. Such generated S-Boxes are more dynamic and key dependent which increase their complexity and also make the differential and linear cryptanalysis more difficult. Each S-Box has eight input bits and eight output bits.

S-Boxes are keystone of modern symmetric cryptosystems. They bring non-linearity to the cryptosystems and strengthen their cryptographic security. This non-linearity provides protection against the attacks where an attacker could express the input and output with a system of linear equations where the key bits are unknown. Such systems can easily be solved.

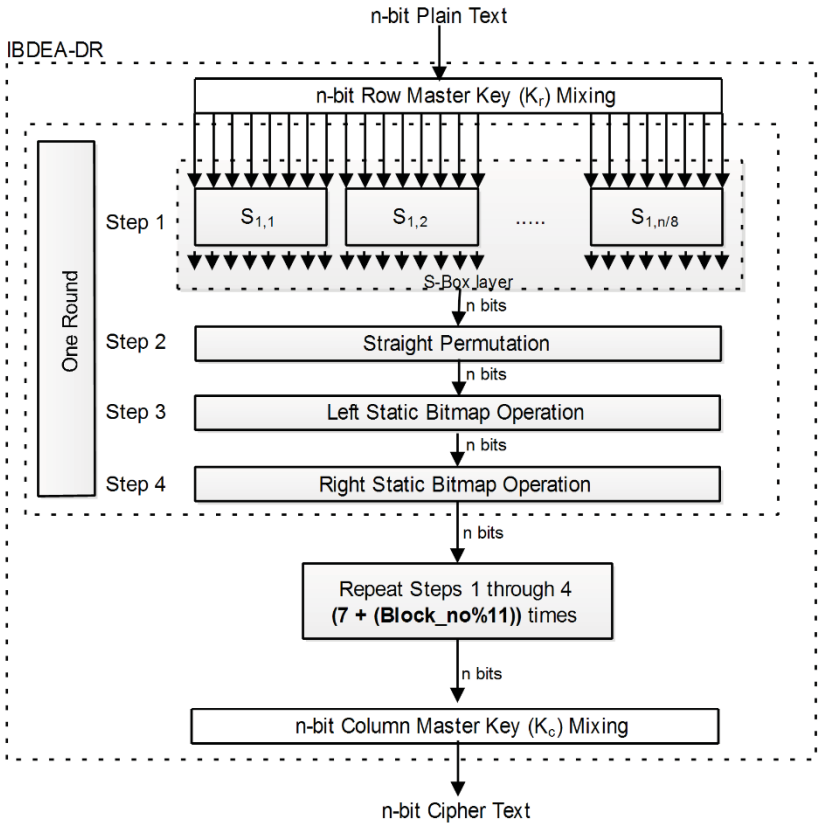

Figure 2. Image showing various operations involved in a round of IBDEA-DR

3.5.2 Straight Permutation –

The n-bit output of the S-Box Substitution is permuted according to a P-Box in order to achieve the property of diffusion. This permutation maps each input bit to an output position; no bits are used twice and no bits are ignored.

3.5.3 Left Static Bitmap Operation –

This is an image_bit_map [ ] [ ] matrix dependent operation. The general outline of this step is show in Figure 3. Below we explain the steps of the left static bitmap operation:

1. The n-bit output from the previous step is split into two parts: the leftmost k bits denoted by L_k and rightmost n-k bits denoted by R_{n-k}.
2. Next the row of the image_bit_map [ ] [ ] matrix pointed by the value of the leftmost k bits (L_k) is selected.
3. From the row selected in step 2 above, we extract the rightmost n-k bits and XOR these bits with the rightmost n-k bits denoted by R_{n-k}.
4. The L_k bits and the n-k bit output of the step 3 above are concatenated to produce the n-bit output as shown in Figure 3.

With these steps the rightmost n-k bits (R_{n-k}) get mixed with the n-k bits from the image_bit_map [ ] [ ] matrix. Since the leftmost k bits (L_k) remain unchanged hence the name Left Static.

3.5.4 Right Static Bitmap Operation –

This step is similar in operation with the Left Static Bitmap Operation with the only difference that instead of rightmost n-k bits (R_{n-k}) the leftmost n-k bits (L_{n-k}) are operated with the n-k bits from the image_bit_map [ ] [ ] matrix as shown in Figure 3. Since in this step the rightmost k bits (R_k) remain unchanged hence the name Right Static.

This completes one round of the IBDEA-DR. The same round is applied 18 more times. Among those rounds the first 8 rounds are compulsory and are applied to every block while the remaining 10 rounds are block dependent. The number of rounds applied are determined by the following formula:

$$(7 + (\text{block\_no} \% 11))$$

3.5.5 Right Static Bitmap Operation –

This is the final step of this algorithm. In this step an n-bit Column Key (K_c) mixing is performed by XORing the n-bit output from the last round with the n-bit Column Master Key (K_c) generating an n-bit cipher text as output.

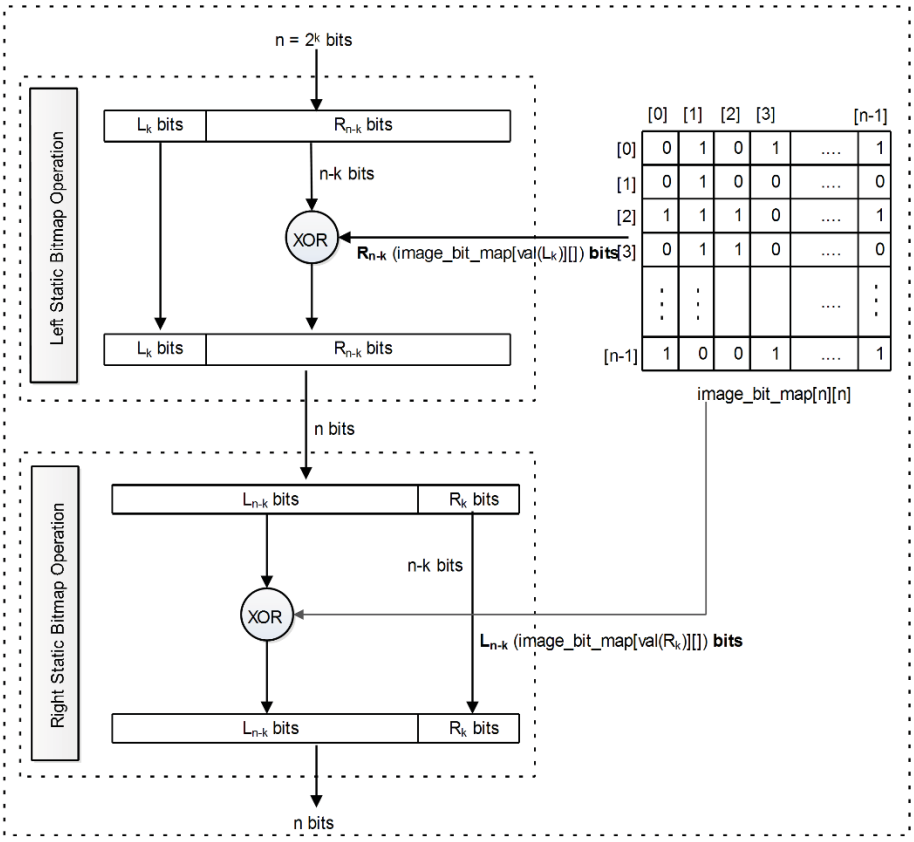

Figure 3. Image showing steps involved in left static and right static bitmap operations

3.6 Decryption –

In IBDEA-DR, decryption of cipher text is achieved by applying the steps of encryption algorithm in reverse order as shown in the Figure 4.

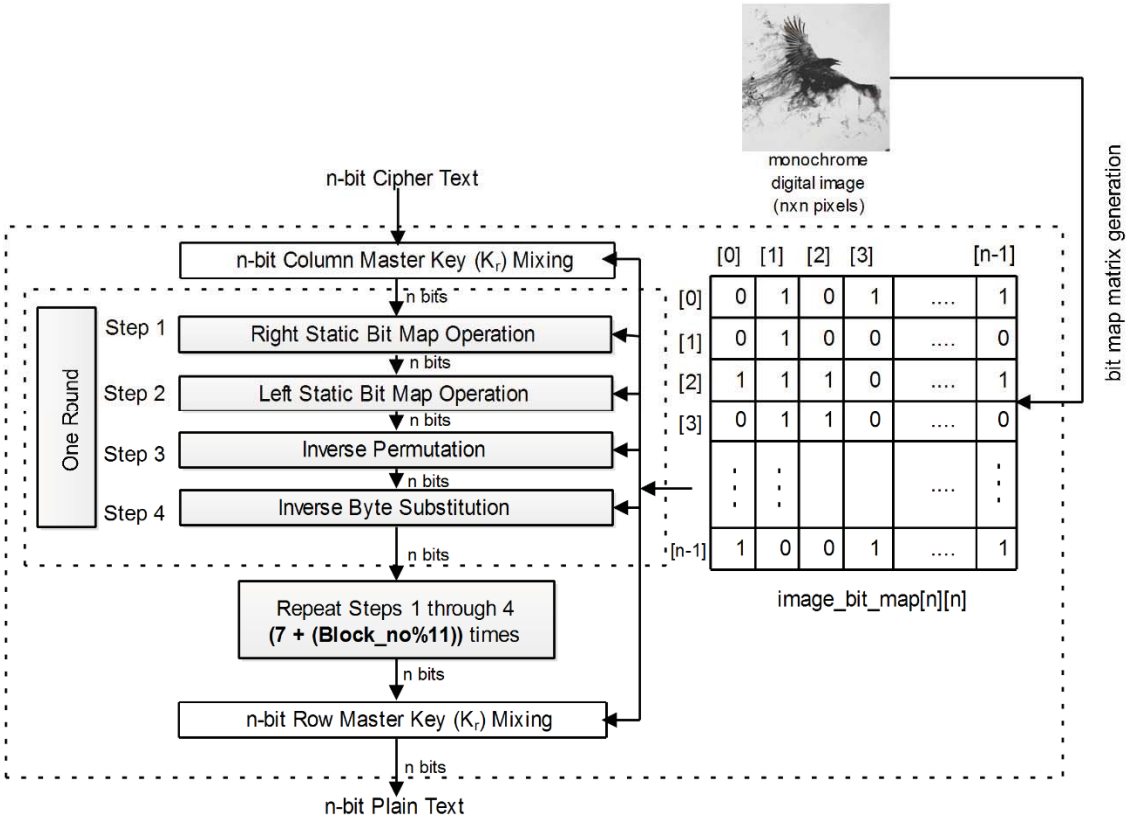

Figure 4. Image showing steps involved decryption process of IBDEA-DR

IV. SECURITY ANALYSIS

The level of security provided by IBDEA-DR can be analyzed based on the following parameters-

4.1 Key Size –

Key size is one of the important parameters in analyzing security of an encryption algorithm. The higher key sizes provide more security against the cryptanalyst attacks. Though the two main keys used in IBDEA-DR are the n-bit Row Master Keys (K_r) and Column Master Key (K_c) generated from the nxn pixel monochrome digital image but on analyzing the algorithm closely the whole image bit map matrix acts as the key. Each round intermingles the rows of the image bit map matrix in such a way that it is not possible to break this cryptosystem by just knowing the Row and Column Master keys. To break this system using brute force attack, the whole image bit map matrix needs to be generated and has the probability of $1/2^{n*n}$. If a digital image of 128x128 pixel size is used, this probability reduces to $1/2^{128*128} = 1/2^{16384}$ which is almost an impossible event. If we assume the brute force attack to be the most efficient, it would require $2^{128*128}$ (10^{4932}) encryptions to recover the image bitmap matrix. If we design a chip that can generate a trillion matrices per second and throw a trillion of them at the problem, it will still take 2.7×10^{4914} years. For higher values of n such as 192, 256 generation of such matrix is un-decidable.

4.2 Key Space –

For a digital image of 128x128 pixel size, we have an almost infinite Key Space of $2^{128*128} = 2^{16384}$ keys which are approximately 1.18×10^{4932} keys. Here each key represents a different image that acts as key for the algorithm.

4.3 Key Management –

Key management involves management of cryptographic keys in a cryptosystem including generation, exchange, storage, use and replacement of keys and has a profound impact on the overall security provided by the cryptosystem. The use of digital image as the key for encryption and decryption of data in IBDEA-DR makes the key management process simpler and secure. Moreover, no additional procedure is required for generation of the images as any image of requisite size can be used as the key for this cryptosystem. The use of image as key also makes the key exchange process simple and effective.

4.4 Dynamic Round Capability (DRC) –

Another important and unique feature of IBDEA-DR is its Dynamic Round Capability (DRC). Since the number of rounds applied on a particular plain text block is determined by its block number, it is not possible to decipher a cipher text block unless we know its block number in the original plain text block. This feature provides further protection against the "Known Cipher Text Attack", "Know Plain Text Attack" and "Chosen Plain Text Attack".

4.5 S-Boxes –

The IBDEA-DR depends on the key dependent S-Boxes generated using RC4 Algorithm as proposed in [6] where it has been proved that such S-Boxes pass the Avalanche Test, Bit Independence Test and Randomness Test which are important features for strong S-Boxes to produce more confusion to the encryption process.

V.CONCLUSION

In this paper we have successfully shown how a monochrome digital image can be used to design an efficient, secure yet simple secret key cryptosystem which can encipher and decipher blocks of data consisting of n-bits under the control of two n-bit master keys generated from a monochrome digital image of size nxn pixels where $n = 2^k$. It has been shown how to generate these two master keys from the image bit map matrix and how to apply the image bit map matrix in each round to achieve the encryption of data. It is evident from the security analysis that the proposed cryptosystem is very robust against different types of cryptanalyst attacks. It has also been shown how the Dynamic Round Capability (DRC) can provide additional protection against the different type of cryptanalyst attacks. Since it is a new cryptosystem, so the real immunity against different types of cryptanalyst attacks can only be judged once exposed to the cryptanalyst community.

REFERENCES

[1] Schneier, Bruce, "Applied cryptography: protocols, algorithms, and source code in C.", John Wiley & Sons, 2007.

[2] Menezes, Bernard L, "Network Security and Cryptography". Cengage Learning India Pvt. Ltd, pp. 45-46, 2010.

[3] D. Kahn, "The Codebreakers: The Story of Secret Writing," New York: Macmillan Publishing Co., 1967.

[4] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, v. 28, n. 4, 1949, pp. 656-715.

[5] Abd-ElGhafar, A. Rohiem, A. Diaa, and F. Mohammed. "Generation of AES Key Dependent S-Boxes using RC4 Algorithm." *in 13th International Conference on Aerospace Sciences & Aviation Technology, pp. 26-28.*

[6] Stallings, William, "The RC4 Stream Encryption Algorithm." (2005).