J. Korea Soc. Math. Educ. Ser. B: Pure Appl. Math. ISSN 1226-0657
Volume 11, Number 1 (February 2004), Pages 1–14

IMAGE ENCRYPTION THROUGH THE BIT PLANE DECOMPOSITION

TAE SIK KIM

ABSTRACT. Due to the development of computer network and mobile communications, the security in image data and other related source are very important as in saving or transferring the commercial documents, medical data, and every private picture. Nonetheless, the conventional encryption algorithms are usually focusing on the word message. These methods are too complicated or complex in the respect of image data because they have much more amounts of information to represent. In this sense, we proposed an efficient secret symmetric stream type encryption algorithm which is based on Boolean matrix operation and the characteristic of image data.

1. INTRODUCTION

The aim of cryptography is to enable two man, say Alice as a sender and Bob as a receiver, to communicate over an insecure channel such as a telephone line or computer network in such a way that Oscar, as an opponent, cannot understand what is being said. For this, Alice first encrypts the plaintext which to send message by using a predetermined secret key and some encryption algorithm, and then send the resulting ciphertext over the channel.

Oscar must cannot determined what the plaintext was even though he sees the ciphertext in the channel by eavesdroping, while Bob, who knows the encryption key, can decrypt the ciphertext to reconstruct the plaintext. This sort of cryptography was exclusive domain of the military for the last many years. So the United States' National Security Agency (NSA) and its counterparts in the former Soviet Union, England, France, Israel, and other countries, have spent billions of dollars in securing their own communications systems while trying to break other's ones. However,

Received by the editors March 15, 2003 and, in revised form, December 1, 2003.
2000 *Mathematics Subject Classification.* 15A33, 94A08, 94A60.
Key words and phrases. cryptosystem, elementary operation, Boolean matrix, bit plane.
This work was supported by the Brain Korea 21 Project.

private individuals, with far less expertise and budget, have been powerless to protect their own privacy against these governments. Nowadays, due to the availability of computer and internet network, state-of-the-art computer cryptography is practiced outside the secured walls of the military agencies.

Encryption algorithms usually can be divided into two basic classes-secret key and public key encryption algorithms. These are used, in their characteristics, in different ways to provide security services. Secret key encryption algorithm has been used in commerce networks since early 1970s. The U. S. Data Encryption Standard (DES) National Breau of Standards (NBS) [7], which was developed at IBM in 1976, has its full specification as a public standard. Recently, the U. S. National Institute of Standards and Technology (NIST) is organizing the international competition to develop an Advanced Encryption Standard (AES) to protect sensitive information in federal compute systems and finally NIST announces that Rijndael proposed one has been selected as the proposed AES on October 2, 2000 Daenen & Rijmen [2].

While secret key algorithm used only one key in symmetric, public key encryption algorithm is asymmetric in a sense that Alice and Bob use each different key which usually used for the purpose of confidentiality, key distribution and authentication Okamoto & Tanaka [10] and Rivest, Shamir & Adleman [11]. As the first one, RSA was developed by Ron Rivest, Adi Shamir and Len Adleman at MIT in 1978 Rivest, Shamir & Adleman [11]. However, this algorithm needs high processing resources when applied to high bit-rates. Though the symmetric secret encryption algorithms such as DES is much faster than public key algorithms, they are very complicate and involve large computation Kocarev & Jakimoski [6]. There are another attempts to use non-linear chaotic dynamical systems for the cipher systems Kocarev & Jakimoski [6] and Murali [9].

Nowadays, according to the development of computer related internet network or mobile communication, it is essential to transfer or to save in secrecy the image such as pictures or fax documents as fast as possible. However, the image has very large amount of data in contrast to the text source so there can be much need of appropriate image encryption algorithm. In this paper, we proposed a new stream type of symmetric image encryption algorithm based on the image characteristics and the properties of the Boolen matrix.

2. Preliminaries and definitions

Usually, secret key algorithm uses the substitutions and permutations to have sufficient diffusion and confusion. Diffusion spreads out the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. As an extension of this idea, we make a single key influence over many digits of ciphertext. Confusion complicates the dependence of the statistics of ciphertext on the statistics of plaintext. On the other hand, public key algorithms is defined through another mathematical concepts. The major respect of our paper is to define an algorithm related the symmetric secret key algorithm based on stream cipher only. For this we first inspect the concept of cryptosystem and some properties of Boolean algebra.

Definition 2.1. A system $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is called *cryptosystem* if it satisfies the followings.

(1) $\mathcal{P}$ is a finite set of possible plaintexts.
(2) $\mathcal{C}$ is a finite set of possible ciphertexts.
(3) $\mathcal{K}$, called keyspace, is a finite set of possible keys
(4) $\mathcal{E} = \{E_K : \mathcal{P} \to \mathcal{C} | K \in \mathcal{K}\}$ and $\mathcal{D} = \{D_K : \mathcal{C} \to \mathcal{P} | K \in \mathcal{K}\}$ are the function spaces.
(5) For each $K \in \mathcal{K}$, there exists an encryption rule $E_K \in \mathcal{E}$ and a corresponding decryption rule $D_K \in \mathcal{D}$ such that $D_K(E_K(p)) = p$ for any $p \in \mathcal{P}$.

Definition 2.2. Let $\mathcal{P} = \mathcal{C} = Z_\ell^m$ for a given integer $\ell > 1$. If the keyspace $\mathcal{K}$ is defined by $\mathcal{K} = \{K = (k_{i,j}) \mid k_{i,j} \in Z_\ell^m$ and K is irreducible$\}$ such that $E_K(p) = pK$ and $D_K(c) = cK^{-1}$ for each $K \in \mathcal{K}$, then the cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is called the *Hill cipher.*

Definition 2.3. Let $\mathcal{P} = \mathcal{C} = Z_\ell^m$ for a given integer $\ell > 1$. If the key space $\mathcal{K}$ is defined by $\mathcal{K} = \{\pi : \{1, 2, \ldots, m\} \to \{1, 2, \ldots, m\} \mid \pi$ is permutation$\}$ such that

$$E_\pi(p_1 p_2 \cdots p_m) = p_{\pi(1)} p_{\pi(2)} \cdots p_{\pi(m)}$$

and

$$D_\pi(c_1 c_2 \cdots c_m) = c_{\pi(1)} c_{\pi(2)} \cdots c_{\pi(m)},$$

then the cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is called the permutation cipher.

Recall that $GF(2) = \{0, 1\}$ is a field with the two operations $\oplus$ and $\wedge$ defined by

$$a \oplus b = \begin{cases} 1 & \text{if } a \neq b \\ 0 & \text{otherwise} \end{cases}, \quad a \wedge b = \begin{cases} 1 & \text{if } a = 1 = b \\ 0 & \text{otherwise} \end{cases}$$

For two $m \times m$ Boolean matrix $A = (a_{i,j})$ and $B = (b_{i,j})$, where $a_{i,j}, b_{i,j} \in GF(2)$, their addition and multiplication are in natural defined as

$$A \oplus B = (a_{i,j} \oplus b_{i,j}) \text{ and } \quad AB = (\bigoplus_{k=1}^{m} a_{i,k} \wedge b_{k,j}).$$

In elementary matrix theory, we have three types of elementary row (*resp.* column) operations.

(1) Interchange i-th row (*resp.* column) and j-th row (*resp.* column): $R_{i \leftrightarrow j}$, $(C_{i \leftrightarrow j})$.
(2) Replace i-th row (*resp.* column) with their k times one, $k \neq 0 : kR_i$, (kC_i).
(3) Replace j-th row (*resp.* column) by adding k times i-th row (*resp.* column) to that one: $kR_i + R_j$, $(resp.\ kC_i + C_j)$.

Definition 2.4. (1) If a matrix E is achieved from the identity matrix I by taking only one elementary operation, then the matrix E is called a elementary matrix.
(2) If a matrix B is achieved from A by consecutive finite number of elementary row (*resp.* column) operations, B is row (*resp.* column) equivalent to A and denoted by $A \sim_R B$ $(resp.\ A \sim_C B)$.

Since the only non-zero element is 1 in $GF(2)$, we only consider two types of row (*resp.* column) elementary operations $R_{i \leftrightarrow j}$, $(resp.\ C_{i \leftrightarrow j})$ and R_{i+j}, $(resp.\ C_{i+j})$ in this paper.

Lemma 2.5. *Let A be any Boolean matrix and E be an elementary matrix. Then from the properties of Boolean addition and multiplication, we have following idempotent laws:*

(1) $A \oplus A = O$.
(2) $EE = I$.

Several cryptosystems may be combined by forming their product so that they frequently incorporate a sequence of permutation and substitution operations. Such systems are of fundamental importance in the design of most present-day cryptosystems such as Advanced Encryption Standard (AES). For given two cryptosystems $\mathcal{S}_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ and $\mathcal{S}_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$ their product cryptosystem

$(\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$ can be defined such that for each key $K = (k_1, K2) \in \mathcal{K}$, E_K and D_K satisfy

$$E_K(p) = E_{K_1,K_2}(p) = E_{K_2}(E_{K_1}(p))$$

and

$$D_K(p) = D_{K_1,K_2}(p) = D_{K_1}(D_{K_2}(p)).$$

In cryptosystems, the probability distributions are associated with their key spaces. Therefore as in usual way we can define the probability distribution for key space $\mathcal{K}$ of above product cryptosystem by

$$\mathrm{P_r(K)} = \mathrm{P_r}\big[(\mathrm{K_1}, \mathrm{K_2})\big] = \mathrm{P_r(K_1)P_r(K_2)}.$$

Definition 2.6. Let $\mathbf{K} =< K_i >$ be a key stream in a key space $\mathcal{K}$. For this key stream, when every plaintext string $\mathbf{p} = p_1 p_2 \cdots$ is encrypted by

$$\mathbf{c} = c_1 c_2 \cdots = E_{K_1}(p_1) E_{K_2}(p_2) \cdots$$

the cryptosystem is called the stream cipher. In particular, if the key stream $\mathbf{K}$ is consist of only one key K such that

$$\mathbf{c} = c_1 c_2 \cdots = E_K(p_1) E_K(p_2) \cdots$$

this is called the block ciphers.

Usually we generate a key stream $< K_i >$ from a given initial key which is independent of the plaintext string, by some specialized algorithms. This type of stream cipher is called *synchronous* and defined formally as follows:

Definition 2.7. A system $(\mathcal{P}, \mathcal{C}, (\mathcal{K}_s, \mathcal{G}, \mathcal{K}), \mathcal{E}, \mathcal{D})$ is called a *synchronous stream cipher* if

(1) $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is cryptosystem.

(2) $\mathcal{K}_s$ and $\mathcal{K}$, respectively, are finite sets which are called a *initial key space* and a *key stream alphabet*, respectively.

(3) $\mathcal{G} : \mathcal{K}_s \to \sum_{j=1}^{\infty} \mathcal{K}^j$, called a *key stream generator*, generate a key stream in $\mathcal{K}$.

3. Main Results

Most recent block ciphers have the cryptosystems based on the product cipher and synchronous stream cipher with a key schedule and a specified round function. From a random binary key, Ks, of some specified length the N-round key schedule

$(K_1, K_2, \ldots, K_N)$ is generated by a fixed public algorithm. The round function $\mathcal{G}_E : K \times \mathcal{P} \times I \to \mathcal{P}$ defined by

$$\mathcal{G}_E(K_i, t_{i-1}) = t_i$$

where $i = 1, 2, \ldots, N$, $t_0 = p$ as an input plaintext, and $t_N = c$ as a final encrypted text is assumed to be the symmetric inverse of it such that

$$\mathcal{G}_E(K_i, t_i) = t_{i-1}.$$

As an example, let us recall that the Data Encryption Standard (DES) algorithm, which is published in 1977 by the US National Bureau of Standard and designed to work with the binary data. DES can encrypt 64-bit data blocks with a 56-bit secret key. Basic operations of this algorithm are transposition and substitution operations by predefined eight S-box tables. First DES algorithm performs initial permutation as a transposition operation such that it rearranges bits to produce inputs of next step. Next it performs the product transformation based on number of XOR operation, substitutions and permutation operations. This process is continued to the 16 rounds on 64-bit data using 56-bit key. In this course, every 64-bit input block is divided into two 32-bit blocks, which are denoted by L_{i-1} and R_{i-1} in Figure 1.

The rightmost 32-bits R_{i-1} of input blocks becomes leftmost 32-bits of output blocks, that is, $R_{i-1} = L_i$. The rightmost 32-bits R_{i-1} is expand to a 48-bit data block. In each round, a 48-bit subkey is generated by the 56-bit key and added modulo-2 to the 48-bit data block. The result is divided into eight 6-bit groups, and is sent through eight S-box to produce eight 4-bit groups. They are concatenated together and form 32-bit output, which is again permuted to generate new 32-bit block. This is added modulo-2 to the leftmost 32-bits L_{i-1} so that the rightmost 32-bit, R_i is made. The descryption is proceeded reversely to the encryption process.

Image file is usually represented by eight bits in gray-level and twenty four bits in color level at each pixel, so we need more time and memory in image file encryption. Every pixel of image I with N bit resolution takes one of 2^N possible values, that is,

$$I(i,j) = \sum_{k=0}^{N-1} 2^{N-k-1} b_k(i,j)$$

where $b_k(i,j) \in GF(2)$ for each (i,j)-th pixel $I(i,j)$ of an Image I. Thus each image can be decomposed into N binary image from MSB to LSB. As an example, Lenna

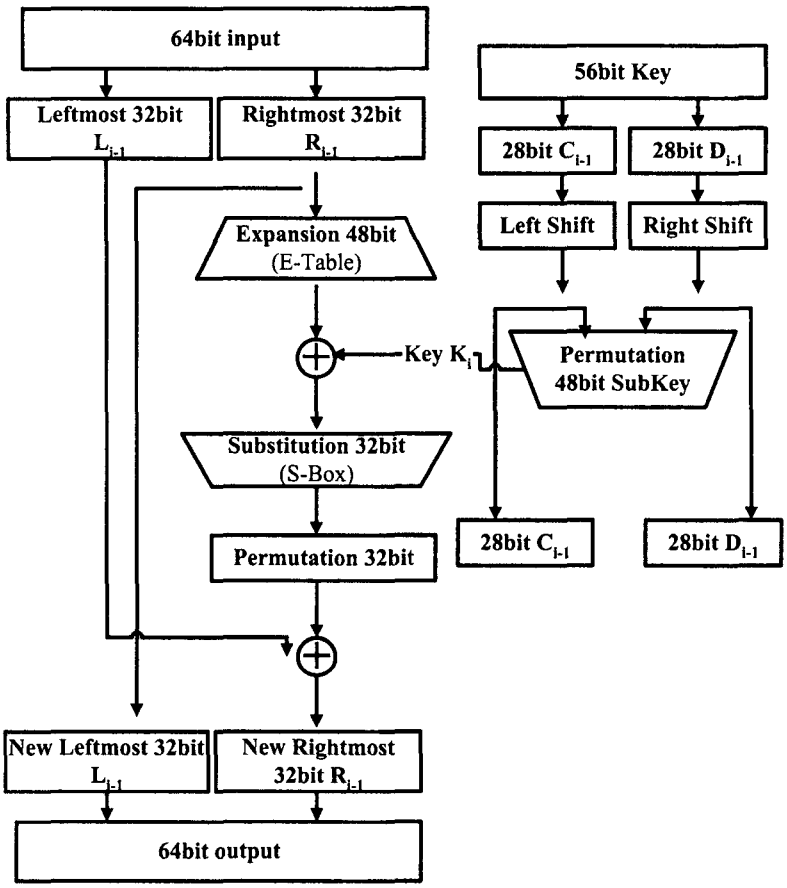

Figure 1. Single Round of DES Algorithm

image of size 256 × 256 pixels and its 8-level bit plane images are shown in Figures 2–4.

Figure 2. (a) original, (b) bitP(7), (c) bitP(6) images of Lenna

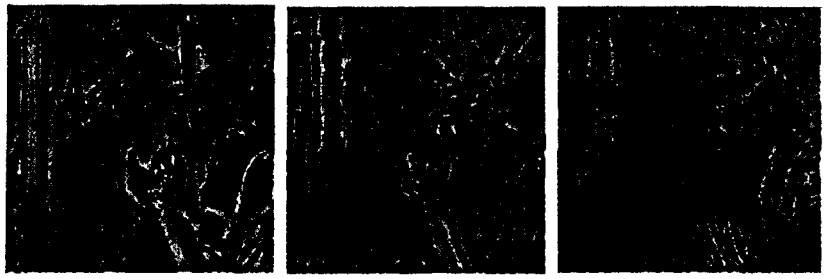

Figure 3. (a) bitP(5), (b) bitP(4), (c) bitP(3) images of Lenna

Figure 4. (a) bitP(2), (b) bitP(1), (c) bitP(0) images of Lenna

For the fast image encryption as in video image as well as still image to cope with real time process, we proposed a variant DES algorithm where we use the initial key K_0 without subkey generation and initial matrix V_0 chosen in $GF(2)$ randomly or LSB bit plane of given image. To protect this key K_0 and initial matrix V_0, Alice defines the master key K and V from the public key K by

$$\mathsf{K} = K^{-1}K_0K^{-1}, \quad \mathsf{V} = K^{-1}V_0K^{-1}$$

and sends to Bob. The receiver can recover the key K_0 and initial matrix V_0 by

$$K_0^{-1} = K^{-1}\mathsf{K}K^{-1}, \quad V_0 = K^{-1}\mathsf{V}K^{-1}.$$

Confusion and diffusion are two basic design criteria of secret key encryption algorithms. By the confusion property, the ciphertext depends on the key as well as plaintext in a complicated and involved way. Through the diffusion, each plaintext bit and each key bit must influence every cipher text bit. For this, we usually employ substitution and permutation.

In DES algorithm, predefined eight S-box is used and sixteen rounds are iterated for this purpose. However, in image encryption, to apply these processes by taking a small block of image is costly. Instead, we take total image decomposed by bit planes

where we apply the elementary row and column operations with XOR operation by the following properties.

Lemma 3.1. *If B is achieved from A by one row (*resp. *column) elementary operation and E is the element matrix from the same elementary operation on the identity matrix, then $B = EA$* (resp. $B = AE$).

Proof. We only prove the lemma in case of an elementary operation $R_i + R_j$ since the other cases are also proved in similar ways. Let $A_{i.}$ be the i-th row vector and $A_{j.}$ be the j-th column vector of matrix A.

For i-th row,

$$B_{i.} = A_{i.} = I_{i.}A = E_{i.}A = (EA)_{i.}$$

For j-th row,

$$B_{j.} = A_{i.} \oplus A_{j.} = I_{i.}A \oplus I_{j.}A = (R_i \oplus R_j)_{j.}A = E_{j.}A = (EA)_{j.}$$

For $k \neq i, j$

$$B_{k.} = A_{k.} = I_{k.}A = E_{k.}A = (EA)_{k.}$$

Therefore $B = EA$. □

For two $m \times m$ matrix A and B, let $(A|B)$ be the $m \times 2m$ matrix by concatenating A and B in row-wise and let $\left(\frac{A}{B}\right)$ be the $2m \times m$ matrix by concatenating in column-wise.

Lemma 3.2. *Let A and B are $m \times m$ matrix.*

(1) *If $(A|I) \sim_R (I|B)$, then $B = A^{-1}$.*
(2) *If $\left(\frac{A}{I}\right) \sim_C \left(\frac{I}{B}\right)$, then $B = A^{-1}$.*

Proof. From the lemma 3.1, there exists a sequence $E_1, E_2, \ldots, Er$ such that

$$E_r \cdots E_2 E_1 A = I \text{ and } E_r \cdots E_2 E_1 I = B.$$

Therefore $BA = E_r \cdots E_2 E_1 A = I$ or $B = A^{-1}$.

For the column relation, the result is similarly proved. □

The following modified lemma is used in this paper.

Lemma 3.3. *If $A \sim I$, then its inverse A^{-1} exists such that $I \sim_C A^{-1}$ under the same sequence of elementary matrix.*

Proof. For $A = E_r \cdots E_2 E_1 I$, claim its inverse $B = I E_1 E_2 \cdots E_r$.

From the Lemma 3.2, $AB = E_r \cdots E_2 E_1 I I E_1 E_2 \cdots E_r = E_r \cdots E_2 E_1 E_1 E_2 \cdots E_r$ $= E_r \cdots E_2 E_2 \cdots E_r = \cdots = E_r E_r = I$. □

As bit plane images shown in Figures 2–4, LSB plane corresponds to subband image with the highest spatial frequencies while MSB plane corresponds to one with lowest spatial frequencies. In particular, analyzing the bit plane images under level 3, we can see that those images act like the uniform random noise. In this sense, to execute the fast encryption of image, we can use the lowest level bit plane image, say $bitP(0)$, instead of a random initial substitution image or vise versa. From the randomness of lower bit plane images, for a faster encryption algorithm with a few quality loss, we can treat some higher level images with casting out lower level image information which is randomly filled in receiver.

$\mathbf{P} = (P_7, P_6, \ldots, P_0)$
For $i = 7$ to N_r
  $P_i' = P_i \oplus C_{i-1}$, $(C_{-1} = K_w)$
  For $j = 1$ to $j = N/2$
    $P_i'' = P'_{\pi_S^2(j,j')}$ .... EP process
    $P_i''' = P''_{(j,\pi_P(j))}$
  $C_i = P_i''' \oplus P_{i-1}$, $(P_{-1} = K_w)$
$\mathbf{C} = (C_7, \ldots, C_{Nr}, 0, \ldots, P_0)$

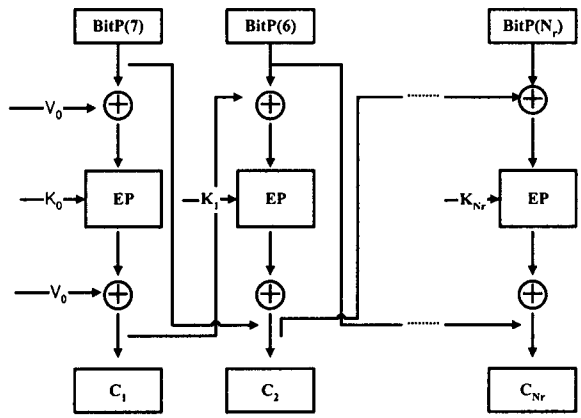

Figure 5. Algorithm and block-diagram of the proposed image encryption

In this algorithm, we decomposed the given image into the eight level bit plane images as plaintexts, say, $\mathbf{P}$ and after the encryption algorithm have been proceeded, we have its encoded image as similar form, say, $\mathbf{C}$. Usually, the secret key schedules are used in starting and ending whitening course. However, in our algorithm we use then the previous ciphertext bit plane image and previous plaintext bit plane image, respectively. Instead, we use the key schedules in the second loop algorithm to substitute efficiently. In this loop, substitution products are executed iteratively sufficiently. For the high randomness, we substitute each j-th row with new row by adding every random taken $N/2$ row, and each j-th column with new column

by adding every random taken $N/2$ column and denoted by π_S^2. Therefore, considering the matrix properties aforementioned, these encryption processes as well as decryption processed faster as an elementary row and column operation.

Accordingly, the key schedules are predefined by the elementary row transformations taken randomly. For this, Alice first taken $N/2 \times N$ random matrix Rm in which every j-th row consists of the number in $\{1, 2, \ldots, N\}$ except j. Then Boolean key matrix $K_R \sim_R I$ is made through every elementary row operations $(R_{j,j_k},\ j_k \in Rm_{j.})$ for all j. Similarly through the all elementary column operations according to R_m, we have $K_C \sim_C I$ which is the inverse of K_R. After one elementary row and column operations $R_{j,j'}$, $C_{j,j'}$ to each K_R and K_C, respectively.

Therefore by defining key schedules $\mathbf{K} = (\bar{K}_0, \bar{K}_1, \ldots, \bar{K_{N_r}})$ in which $\bar{K}_i = (K, K^i)$ for the $K = K_R$ in encryption and $K = K_C$ in decryption algorithm, the iterative substitutions and permutation can be simply formalized by encryption rule

$$E_K(P_i') = K_R P_i' K_R^i = K_R(P_i \oplus C_{i-1})K_R^i \oplus P_{i-1}.$$

Finally Alice has encrypted her image with her secret key K_R, and should send corresponding key K_C with the lowest level bit plane image to Bob with encrypted ones by the public key algorithm. The description algorithm is defined symmetrically by transposing P_i and K_R into C_i andK_C, respectively as in following equation:

$$\begin{aligned} D_K(C_i) &= K_C(C_i \oplus P_{i-1})K_C^i \oplus C_{i-1} \\ &= K_C(K_R(P_i \oplus C_{i-1})K_R^i \oplus P_{i-1} \oplus P_{i-1})K_C^i \oplus C_{i-1} \\ &= (P_i \oplus C_{i-1})K_R^i K_C^i \oplus C_{i-1} \\ &= P_i \oplus C_{i-1} \oplus C_{i-1} \\ &= P_i \end{aligned}$$

Figure 6. bitP(7), encrybitP(7), decrybitP(7) of Lenna image

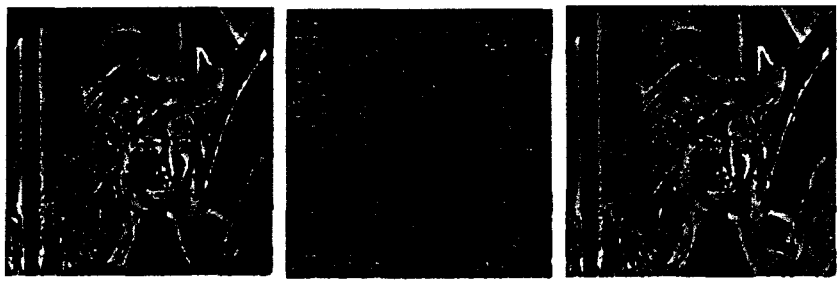

Figure 7. bitP(6), encryptbitP(6), decryptbitP(6) of Lenna image

In Figures 6–7 show each encrypted and decrypted images of bit plane level 7 and 6 of Lenna image, respectively. In encryption process, Alice can determine the key round number $N_r > 0$ to determine bit plane level according to the image data's importance and compactness.

In Figure 8, encrypted and decrypted images over the level 4 and 5 by using the initial random matrix are shown, while in in Figure 9, those images which use $bitP(0)$ in stead of random initial matrix are shown. We can observe that there is no serious difference of image quality in visual under the level 3. In case of continuous encryption for the video images, P_{-1} and C_{-1} can be replaced with the previous image's lowest bit plane.

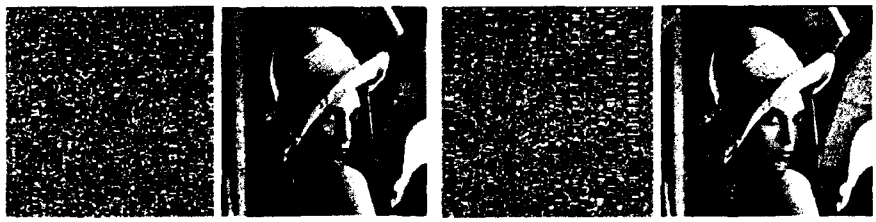

Figure 8. encrypt and decrypt images to the level 4, and level 3 with randdom initial

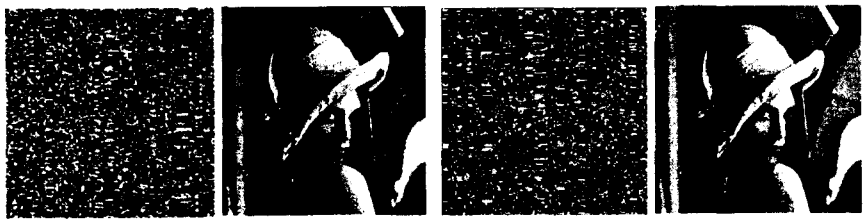

Figure 9. encrypt and decrypt images to the level 4, and level 3 with bitP(0)

4. Similarity and complexity of encryption and decryption

Let the u-th bit plane image $P_u = (p_{i,j}(u))_{n\times n}$ be encrypted to the u-th encrypted image $C_u = (c_{i,j}(u))_{n\times n}$ through the key matrix $K = (k_{i,j})_{n\times n}$ and $K^u = (k_{i,j}(u))_{n\times n}$. Then from the proposed encryption algorithm,

$$c_{i,j}(u) = \Big[\bigoplus_{1\le m\le n} k_{i,m} \wedge \bigoplus_{1\le s\le n} \Big(\big(p_{m,s}(u) \oplus c_{m,s}(u-1)\big) \wedge k_{s,j}(u) \Big) \Big] \oplus p_{i,j}(u-1)$$

where $p_{i,j}(0)$ is the (i,j)-element of random initial matrix V_0. So we can see that each (i,j)-element of u-th encrypted image depends on all elements of u-th bit plane images and previous encrypted image C_{u-1}. Since all elements of C_{u-1} are related with the all elements of key matrix K, the element $C_{i,j}(u)$ also depends on all elements of key matrix.

Therefore our proposed algorithm satisfies confusion property well, in a sense that the encrypted image depends on the original image and key matrix in a complicated and involved way. It also satisfies diffusion property since every element of bit plane image and key matrix influence every element of encrypted image. In the structure of the proposed cipher systems, we can see that decryption is essentially the same process as the encryption except using a different key matrix. Thus this algorithm may facilitate computer execution in software as well as hardware, and save the physical space in structure implement.

References

1. F. Andres: Multimedia and security. *IEEE Multimedia* **8(3)** (2001), 20–21.
2. J. Daenen & V. Rijmen: *AES Proposal: Rijndael.* June, AES submission, 1998.
3. W. Diffie & M. E. Hellman: New directions in cryptography. *IEEE Trans. Information Theory* IT-22 (1976), no. 6, 644–654. MR **55**#10141
4. G. Jakimoski & L. Kocarev: Differential and linear probabilities of a block-encryption cipher. *IEEE Trans. Circuits Systems I Fund. Theory Appl.* **50** (2003), no. 1, 121–123. CMP 1965727
5. L. Kocarev: Chaos-based cryptography: a brief overview. *IEEE Circuits Systems Magazine* **1** (2001) 6–21.
6. L. Kocarev & G. Jakimoski: Pseudorandom bits generated by chaotic maps. *IEEE Trans. Circuits Systems I Fund. Theory Appl.* **50** (2003), no. 1, 123–126. CMP 1965728
7. National Breau of Standards (NBS): *Data encryption standard.* FIPS PUB 46, National Breau of Standards, Washington, D.C., 1997.

8. X. Lai: *On the design and security of block cipher.* Konstanz, Germany: Jartung-Gorre, 1992.
9. K. Murali: Heterogeneous chaotic systems based cryptography. *Phys. Lett. A* **272** (2000), no. 3, 184–192. MR **2001d:**94018
10. E. Okamoto & K. Tanaka: Key distribution system based in identification information. *IEEE Selected Areas in Communications* **7** (1989), 482–485.
11. R. L. Rivest, A. Shamir & L. Adleman: *A method for obtaining digital signatures and public key cryptosystem.* Communication of ACM, 1978.

SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, KYUNGPOOK NATIONAL UNIVERSITY, 1370 SANGYEOK-DONG, BUK-GU, DAEGU 702-701, KOREA
Email address: tskim@ee.knu.ac.kr