Volume 1, No. 3, Sept-Oct 2010
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info
ISSN No. 0976-5697

Cryptography of a Gray Level Image using a Modified Feistel Cipher

Dr. V. Umakanta Sastry*
Department of Computer Science and Engineering
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
vuksastry@rediffmail.com

D. S. R. Murthy
Department of Information Technology
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
dsrmurthy@sreenidhi.edu.in

Dr. S. Durga Bhavani
School of Information technology
Jawaharlal Nehru Technological University Hyderabad (JNTUH)
Hyderabad – 500 085, Andhra Pradesh, India
sdurga.bhavani@gmail.com

Abstract: In this paper, we have made use of a modified Feistel cipher for encrypting a Gray level image. This image is represented in the form of a square matrix of size 256. The encryption is carried out by considering, at each instance, a matrix of size 32 x 64. Here, as the cipher is an elegant one, we notice that the time required for computation is much less.

Keywords: Feistel Cipher, Gray level Image, Encryption, Decryption and Encrypted Image.

I. INTRODUCTION

The advent of Internet in the last decade of the previous century brought in a revolution in the transmission of information. The study of cryptography of plain texts [1] and images has gained considerable impetus in the last two decennia. Several papers [2–5] of image cryptography have appeared in the literature in the recent past.

In a recent investigation [6], we have modified the Feistel cipher by introducing several new concepts. In the classical Feistel cipher, the plain text is a binary string of 2w binary bits and the cipher is governed by the relations [1]

$P_0 = w$, $Q_0 = w$,

$P_i = Q_{i-1}$,

$Q_i = P_{i-1} \oplus F(Q_{i-1}, K_i)$, $\quad i = 1$ to n, (1.1)

for encryption, and

$Q_{i-1} = P_i$,

$P_{i-1} = Q_i \oplus F(P_i, K_i)$, $\quad i = n$ to 1, (1.2)

for decryption.

Here, P and Q stand for the left and right halves of the plain text; K_i is the key in the i^{th} round of the iterative process occurring in the analysis, and $\oplus$ denotes the XOR operation. The initial conditions in the decryption are taken from the cipher text obtained at the end of the encryption.

In the cipher developed by us, we have taken the plain text as a matrix contains $2m^2$ decimal numbers, and the key K as a square matrix of size m^2. In this, we have multiplied the first half of the plain text matrix by the key K on both the sides and used modular arithmetic. For the detailed description of this analysis, we refer to [6].

In the present paper, our objective is to utilise the block cipher developed in [6] for the cryptography of an image. We represent the gray level values of the pixels of the image in terms of a square matrix of size 256. We consider, each time, an image matrix of size 32 x 64 and perform the encryption. We adopt this process till we exhaust the entire image. The process of decryption is done just in the reverse manner to the process of encryption.

In Section 2, we have discussed the development of the procedure for the cryptography of a gray level image. In Section 3, we have given an example and illustrated the process. Finally, in Section 4, we have indicated the computations carried out in this analysis and drawn conclusions.

II. DEVELOPMENT OF A PROCEDURE FOR THE CRYPTOGRAPHY OF A GRAY LEVEL IMAGE

Consider an image whose gray level values can be represented in the form of a matrix given by

$\mathbf{P} = [\mathbf{P_{ij}}]$, $i = 1$ to m, $j = 1$ to $2m$. (2.1)

Here, each P_{ij} lies in [0, 255].

Let K be the key matrix given by

$\mathbf{K} = [\mathbf{K_{ij}}]$, $i = 1$ to m, $j = 1$ to m, (2.2)

where each K_{ij} is also in the interval [0, 255].

Let $\mathbf{C} = [\mathbf{C_{ij}}]$, $i = 1$ to m, $j = 1$ to $2m$ (2.3)

be a matrix, obtained on encryption.

In this analysis, the matrix P is represented in the form of a pair of square matrices P_0 and Q_0, where each one is of size m. P_0 contains the elements in the left half of P and Q_0 contains the elements in the right half of P.

The process of encryption is described by the relations

$P_i = Q_{i-1}$,

$Q_i = (P_{i-1} \oplus (F(Q_{i-1}, K)) \bmod N$, for $i = 1$ to n,

$F(Q_{i-1}, K) = (KQ_{i-1}K) \bmod N$, (2.4)

and the process of decryption is given by

$Q_{i-1} = P_i$,

$P_{i-1} = (Q_i \oplus (F(P_i, K)) \bmod N$, for $i = n$ to 1,

$F(P_i, K) = (KP_iK) \bmod N$. (2.5)

In the present analysis, we have used mod N appropriately, and n denotes the number of rounds in the iteration process.

The flowcharts for the process of encryption and the process of decryption are given in Fig. 1.

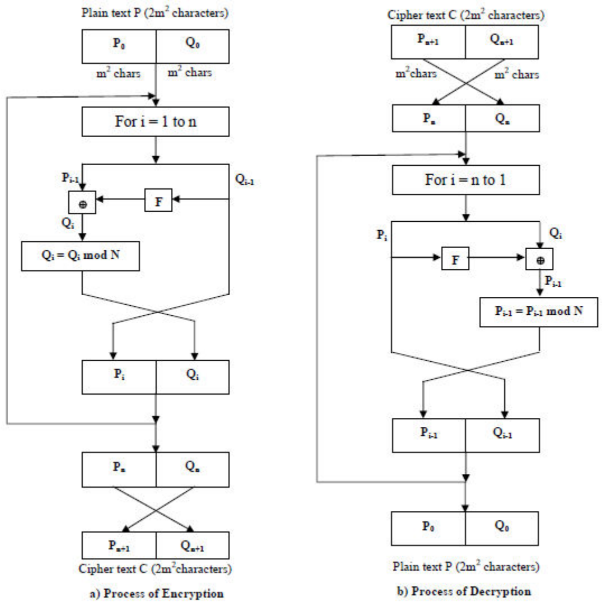

Fig. 1 Schematic Diagram of the Cipher

In what follows, we present the algorithms for encryption, and decryption.

Algorithm for Encryption

1. Read P, m, n, N
2. P_0 = Left half of P
   Q_0 = Right half of P
3. for i = 1 to n
   {
   $P_i = Q_{i-1}$
   $F = (KQ_{i-1}K) \bmod N$
   $Q_i = (P_{i-1} \oplus F) \bmod N$
   }
4. $P_{n+1} = Q_n$
   $Q_{n+1} = P_n$
5. $C = P_{n+1} \parallel Q_{n+1}$ /* || stands for concatenation
6. Write (C)

Algorithm for Decryption

1. Read C, m, n, N
2. P_{n+1} = Left half of C
   Q_{n+1} = Right half of C
3. for i = n to 1
   {
   $Q_{i-1} = P_i$
   $F = (KP_iK) \bmod N$
   $P_{i-1} = (Q_i \oplus F) \bmod N$
   }
4. $P_0 = Q_1$
   $Q_0 = P_1$
5. $P = P_0 \parallel Q_0$ /* || stands for concatenation
6. Write (P)

III. ILLUSTRATION OF THE CRYPTOGRAPHY OF AN IMAGE

Let us consider a typical sample gray level image which can be represented in the form of a matrix containing 8 rows and 16 columns. This is given by

$$P = \begin{bmatrix} 166 & 176 & 165 & 154 & 154 & 144 & 150 & 134 & 129 & 127 & 134 & 132 & 129 & 130 & 132 & 144 \\ 176 & 165 & 160 & 150 & 145 & 142 & 135 & 147 & 140 & 135 & 126 & 122 & 136 & 134 & 128 & 127 \\ 164 & 163 & 157 & 162 & 161 & 142 & 136 & 126 & 131 & 127 & 116 & 119 & 133 & 135 & 139 & 123 \\ 167 & 161 & 162 & 163 & 143 & 132 & 128 & 126 & 119 & 122 & 135 & 130 & 116 & 121 & 139 & 122 \\ 169 & 170 & 163 & 163 & 143 & 134 & 134 & 139 & 134 & 127 & 134 & 140 & 109 & 125 & 155 & 133 \\ 173 & 183 & 157 & 159 & 150 & 139 & 140 & 135 & 135 & 123 & 123 & 134 & 123 & 130 & 127 & 141 \\ 168 & 167 & 161 & 146 & 150 & 144 & 136 & 123 & 125 & 113 & 119 & 139 & 128 & 136 & 124 & 133 \\ 166 & 158 & 164 & 147 & 150 & 145 & 132 & 130 & 109 & 117 & 122 & 117 & 112 & 124 & 156 & 142 \end{bmatrix} \quad (3.1)$$

Let us take a key matrix K of size 8 x 8 in the form

$$K = \begin{bmatrix} 175 & 173 & 027 & 065 & 032 & 065 & 017 & 076 \\ 232 & 084 & 072 & 069 & 032 & 185 & 069 & 082 \\ 027 & 179 & 102 & 033 & 083 & 097 & 073 & 032 \\ 065 & 084 & 143 & 069 & 105 & 153 & 213 & 163 \\ 184 & 028 & 049 & 005 & 069 & 031 & 166 & 109 \\ 208 & 185 & 077 & 234 & 207 & 171 & 071 & 080 \\ 237 & 249 & 101 & 057 & 095 & 191 & 037 & 132 \\ 127 & 107 & 032 & 085 & 117 & 254 & 165 & 087 \end{bmatrix} \quad (3.2)$$

On applying the encryption algorithm given in section 2, we get

$$C = \begin{bmatrix} 192 & 122 & 376 & 277 & 192 & 289 & 119 & 172 & 275 & 035 & 301 & 289 & 268 & 234 & 304 & 398 \\ 145 & 168 & 182 & 355 & 156 & 229 & 381 & 463 & 327 & 260 & 382 & 347 & 320 & 364 & 282 & 351 \\ 207 & 287 & 292 & 248 & 243 & 134 & 406 & 212 & 276 & 131 & 126 & 193 & 463 & 303 & 231 & 138 \\ 082 & 244 & 191 & 120 & 499 & 161 & 334 & 161 & 309 & 135 & 303 & 264 & 359 & 390 & 328 & 077 \\ 196 & 396 & 395 & 089 & 253 & 455 & 245 & 235 & 141 & 460 & 260 & 125 & 398 & 155 & 84 & 087 \\ 332 & 240 & 264 & 362 & 315 & 350 & 140 & 396 & 347 & 453 & 415 & 172 & 196 & 231 & 392 & 353 \\ 271 & 370 & 316 & 259 & 309 & 108 & 346 & 159 & 326 & 251 & 375 & 373 & 457 & 295 & 078 & 394 \\ 142 & 313 & 260 & 053 & 325 & 264 & 494 & 177 & 339 & 303 & 262 & 442 & 271 & 129 & 317 & 138 \end{bmatrix} (3.3)$$

This can be represented in the form of an image (Encrypted image) given in Fig. 2.

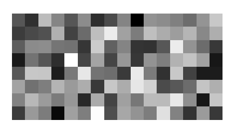

Fig. 2 Encrypted form of the sample Image

On applying the decryption algorithm (See Section 2) on the cipher text in (3.3), we get back the original plain text P.

The aforementioned process can be applied to any gray level image of any size by taking an appropriate key and dividing the image into a number of parts. In what follows, we discuss the encryption and decryption of an image in general.

IV. COMPUTATIONS AND CONCLUSIONS

Consider the image of a person (Einstein) given in Fig. 3.

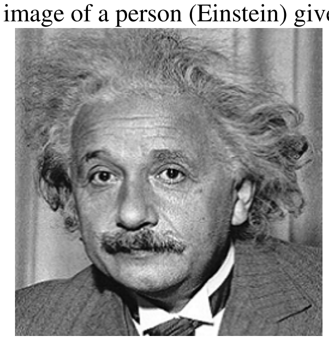

Fig. 3 Image of Einstein

This gray level image is represented in the form of a square matrix of size 256. This is divided into 32 parts, wherein each part is a matrix of size 32 x 64.

Here, we consider a square key matrix of size 32. This is generated from the key matrix K given in (3.2) by applying the procedure discussed in Appendix.

On using the key K of size 32 x 32 given in Appendix, and the procedure discussed in section 3, we have encrypted all the 32 parts of the image. Thus, we have obtained the cipher text corresponding to the entire image. This is displayed in Fig. 4.

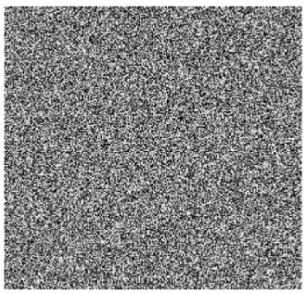

Fig. 4 Encrypted form of the Entire image

Here, it may be noted that the sender has to transmit the square key matrix of size 8 and the receiver has to transform it into a square matrix of size 32 as described in Appendix.

On applying the decryption algorithm on all the 32 parts separately, we get back the plain text, which can be readily brought to the form of the original image (Fig. 3).

All the computations in this analysis are carried out by writing C programs corresponding to the encryption and the decryption algorithms. The development of the encrypted image is done by using MATLAB.

Finally, we conclude that, this cipher is a strong one, and it is impossible to find the original image (even when the encrypted image is available and the algorithms are known) by any means without having the knowledge of the key.

V. REFERENCES

[1] William Stallings, *Cryptography and Network Security, Principles and Practice*, Third Edition, Pearson, 2003.

[2] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, "*An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption*", Informatica, 31, pp. 121 – 129, 2007.

[3] Mohammed A. F. Al-Husainy, "*Image Encryption Using Genetic Algorithm*", Information Technology Journal, Vol. 5, No. 3, pp. 516 – 519, 2006.

[4] Nawal El-Fishawy, and Osama M. Abu Zaid, "*Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms*", International Journal of Network Security, Vol. 5, No. 3, pp. 241 – 251, Nov 2007.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "*A Modified AES Based Algorithm for Image Encryption*", World Academy of Science, Engineering and Technology, Vol. 27, pp. 206 – 211, 2007.

[6] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "*A Modified Feistel Cipher involving Modular Arithmetic and a Key on both the sides of a Plain Text Matrix*", International Journal of Computational Intelligence and Information Security (IJCIIS), ISSN: 1837-7823, Special Issue, Vol. 1, No. 4, pp. 10 – 16, Jun 2010.

AUTHORS

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 40 research papers in various international journals. He is a Member, Editorial Board and Reviewer of International Journal of Computational Intelligence and Information Security (IJCIIS), Senior Member of International Association of Computer Science and Information Technology (IACSIT) and Reviewer of International Journal of Computer and Network Security (IJCNS). His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE) and International Journal of Computational Intelligence and Information Security (IJCIIS).

Dr. S. Durga Bhavani is presently working as Professor in School of Information Technology (SIT), JNTUH, Hyderabad, India. She has more than 18 years of teaching experience. Her research area includes Evidential Reasoning, Cryptography and Image Processing. She has no. of research publications to her credit.

Prof. D. S. R. Murthy obtained B. E. (Electronics) from Bangalore University in 1982, M. Tech. (CSE) from Osmania University in 1985 and presently pursuing Ph.D. from JNTUH, Hyderabad since 2007. He is presently working as Professor in the Dept. of Information Technology (IT), SNIST since Oct. 2004. He earlier worked as Lecturer in CSE, NIT (formerly REC), Warangal, India during Sep. 1985 – Feb. 1993, as Assistant Professor in CSE, JNTUCE, Anantapur, India during Feb. 1993 – May 1998, as Academic Coordinator, ISM, Icfaian Foundation, Hyderabad, India during May 1998 – May 2001 and as Associate Professor in CSE, SNIST during May 2001 - Sept. 2004. He worked as Head of the Dept. of CSE, JNTUCE, Anantapur during Jan. 1996 – Jan 1998, Dept. of IT, SNIST during Apr. 2005 – May 2006, and Oct. 2007 – Feb. 2009. He is a Fellow of IE(I), Fellow of IETE, Senior Life Member of CSI, Life Member of ISTE, Life Member of SSI, DOEACC Expert member, and Chartered Engineer (IE(I) & IETE). He is a Reviewer of International Journal of Advanced Research in Computer Science (IJARCS), International Journal of Computational Intelligence and Information Security (IJCIIS) and International Journal of Computational Intelligence and Information Security (IJCIIS). He is a member of International Association of Computer Science and Information Technology (IACSIT). He published a text book on C Programming & Data Structures. His research interests are Image Processing and Image Cryptography and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE), International Journal of Computational Intelligence and Information Security (IJCIIS) and in International Journal of Advanced Research in Computer Science (IJARCS).

