ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cryptography of a Gray Level Image using a Novel Block Cipher Involving Feistel Structure and Modular Arithmetic

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 novel block cipher involving Feistel structure and modular arithmetic for encrypting a Gray level image. The image is represented in the form of a matrix of size 256 x 256, and this is divided into 32 parts, wherein each part is of size 32 x 64. A key of size 8 x 8 is taken and it is transformed into a key of size 32 x 32. This key is utilised in carrying out the computations required for encryption and decryption. As the cipher is a strong one, we find that no one can identify the original image by any means.

Keywords: Block Cipher, Gray level image, Feistel structure, Modular arithmetic, Encryption, Decryption and Encrypted image.

I. INTRODUCTION

The study of cryptography of images has been an interesting area of research in recent years. Most of the symmetric block ciphers [1–4] and the public key ciphers [5–7] are utilised in the development of the image cryptography. In all these investigations, security of images is achieved in a significant manner.

In a recent paper [8], we have developed a novel block cipher by using Feistel structure and modular arithmetic. In this analysis, we have made use of '+' operation instead of XOR operation, which was used in the classical Feistel cipher [9]. Here, we have shown that the cipher is a strong one as the length of the key is quite considerable and it leads to nonlinearities as we have included the key on both the sides of a portion of the plain text.

In the present paper, our objective is to study the encryption and decryption of a gray level image. To this end, we have followed the procedure which is the same as that utilised in [10].

In Section 2, we have presented 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 mentioned the computations carried out in this analysis and drawn conclusions.

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

Let us consider a plain text P having $2m^2$ characters. This can be written in the form of a pair of square matrices denoted as P_0 and Q_0, in which each is having m^2 characters. Let K be a key (square) matrix of size m.

Now, the process of encryption and the process of decryption are governed by the relations

$P_i = Q_{i-1}$,

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

$$F(Q_{i-1}, K) = (KQ_{i-1}K) \bmod N, \quad (2.1)$$

and

$Q_{i-1} = P_i$,

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

$$F(P_i, K) = (KP_iK) \bmod N. \quad (2.2)$$

In the present analysis, N will be chosen appropriately. Here, n stands for the number of rounds of the iteration process.

The flow charts describing encryption and decryption are shown in Fig. 1.

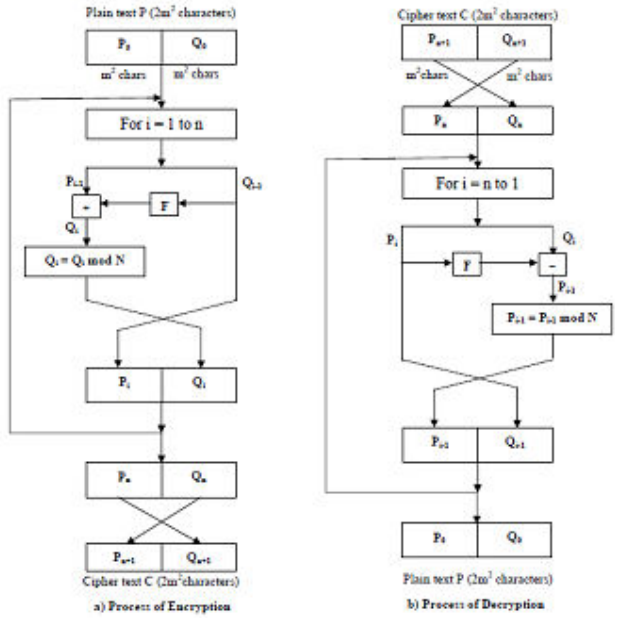

Figure 1. Schematic diagram of cipher

Here, 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
   {
   $P_i = Q_{i-1}$
   $F = (KQ_{i-1}K) \bmod N$
   $Q_i = (P_{i-1} + F) \bmod N$
   }
4. $P_{n+1} = Q_n$
   $Q_{n+1} = P_n$
5. $C = P_{n+1} \| Q_{n+1}$ /* || 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
   {
   $Q_{i-1} = P_i$
   $F = (KP_iK) \bmod N$
   $P_{i-1} = (Q_i - F) \bmod N$
   }
4. $P_0 = Q_1$
   $Q_0 = P_1$
5. $P = P_0 \| Q_0$ /* || stands for concatenation
6. Write (P)

III. ILLUSTRATION OF THE CRYPTOGRAPHY OF AN IMAGE

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

$$P = \begin{bmatrix} 001 & 001 & 004 & 008 & 000 & 006 & 011 & 002 & 007 & 004 & 002 & 003 & 003 & 003 & 005 & 009 \\ 001 & 002 & 001 & 003 & 012 & 000 & 001 & 011 & 003 & 003 & 010 & 004 & 002 & 006 & 012 & 010 \\ 001 & 010 & 004 & 001 & 001 & 001 & 001 & 006 & 000 & 000 & 011 & 000 & 012 & 117 & 163 & 147 \\ 001 & 003 & 005 & 005 & 001 & 011 & 019 & 001 & 001 & 012 & 001 & 104 & 214 & 211 & 205 & 239 \\ 001 & 010 & 001 & 014 & 016 & 001 & 001 & 001 & 007 & 081 & 197 & 252 & 250 & 226 & 236 & 240 \\ 001 & 001 & 015 & 001 & 001 & 014 & 002 & 010 & 153 & 253 & 251 & 248 & 245 & 239 & 238 & 241 \\ 017 & 001 & 001 & 022 & 001 & 067 & 230 & 253 & 249 & 251 & 240 & 223 & 248 & 239 & 214 & 233 \\ 001 & 026 & 000 & 000 & 005 & 107 & 253 & 242 & 250 & 229 & 240 & 248 & 234 & 241 & 248 & 229 \end{bmatrix} \quad (3.1)$$

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 have

$$C = \begin{bmatrix} 176 & 322 & 268 & 258 & 278 & 346 & 134 & 278 & 172 & 302 & 280 & 138 & 222 & 134 & 254 & 182 \\ 264 & 238 & 210 & 180 & 150 & 116 & 400 & 304 & 398 & 398 & 212 & 234 & 292 & 160 & 286 & 090 \\ 240 & 122 & 318 & 092 & 446 & 112 & 132 & 068 & 334 & 418 & 312 & 290 & 340 & 140 & 106 & 342 \\ 348 & 462 & 344 & 134 & 138 & 450 & 210 & 366 & 204 & 218 & 320 & 402 & 174 & 270 & 486 & 402 \\ 140 & 096 & 282 & 112 & 100 & 370 & 210 & 056 & 034 & 172 & 252 & 254 & 238 & 106 & 156 & 034 \\ 024 & 164 & 420 & 226 & 212 & 168 & 180 & 278 & 208 & 180 & 436 & 446 & 468 & 216 & 340 & 370 \\ 460 & 276 & 366 & 206 & 048 & 474 & 286 & 218 & 356 & 076 & 270 & 394 & 296 & 274 & 102 & 118 \\ 044 & 330 & 160 & 362 & 242 & 338 & 170 & 326 & 368 & 102 & 356 & 458 & 370 & 254 & 234 & 254 \end{bmatrix} \quad (3.3)$$

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

Figure 2. Encrypted form of the sample Image

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

The procedure described above can be adapted to any gray level image of any size by taking a suitable key and dividing the image into a set of subimages appropriately. In the next section, we describe the encryption and decryption processes of a real image.

IV. COMPUTATIONS AND CONCLUSIONS

Let us consider the image of Dr. S. Radhakrishnan, given in Fig. 3.

Figure 3 Image of Dr. S. Radhakrishnan

This gray level image is represented in the form of a matrix of size 256 x 256. In order to carryout the process of encryption in a convenient manner, this image is divided into 32 parts, in which each part is of size 32 x 64.

We consider a key matrix of size 32 x 32, which is generated from the key matrix K of size 8 x 8 given in (3.2), by applying the procedure described in [10].

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

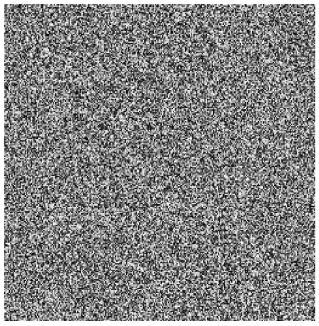

Figure 4. Encrypted form of the Entire image

On carrying out the process of decryption on all the 32 parts separately, we have got the original plain text and the corresponding image (Fig. 3).

All the computations in this analysis are carried out by writing C programs for the encryption and the decryption algorithms (given in section 2). We have used MATLAB in the development of encrypted image.

As the image corresponding to the cipher text is totally in a peculiar form, we conclude that no one can recognize it in the process of transmission. This is all due to the strength of the cipher.

V. REFERENCES

[1] José J. Amador, Robert W. Green, *"Symmetric-key block cipher for image and text cryptography",* International Journal of Imaging Systems and Technology (IJIST), Vol. 15, No. 3, pp.178–188, Oct 2005.

[2] Kamlesh Gupta & Sanjay Silakari, "*Efficient Image Encryption using MRF and ECC*", International Journal of Information Technology and Knowledge Management (IJITKM), Vol. 2, No. 2, pp. 245-248, Jul – Dec 2009.

[3] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah, A. Hegazy, "*An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems*", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No. 2, pp. 226 – 232, Feb 2010.

[4] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "*Image Encryption Using Advanced Hill Cipher Algorithm*", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[5] Han Shui-hua Han and Yang Shuang-Yuan Yang, "*An Asymmetric Image Encryption Based on Matrix Transformation*", ECTI Transactions on Computer and Information Technology, Vol.1, No.2, pp. 126–133, Nov 2005.

[6] Ganesan, K. Singh, I. Narain, M., "*Public Key Encryption of Images and Videos in Real Time Using Chebyshev Maps*", Fifth International Conference on Computer Graphics, Imaging and Visualisation (CGIV '08), pp. 211 – 216, Aug. 2008.

[7] K. Prasadh, R. Gnanajeyaraman, "*Analysis of Chaotic-Chebyshev Polynomials using on Public Key Cryptosystems*", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No. 6 (23), 2009.

[8] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "*A Novel Block Cipher involving Feistel Structure and Modular Arithmetic*", International Journal of Computational Intelligence and Information Security (IJCIIS), ISSN: 1837-7823, Special Issue, Vol. 1, No. 4, pp. 48 - 54, Jun 2010.

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

[10] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "*Cryptography of a Gray Level Image Using a Modified Feistel Cipher*", International Journal of Advanced Research in Computer Science (IJARCS), Sent for publication.

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, Ananta-

pur, 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).