Enhancement of Security in Data Mining using FEAL(Fast Encryption Algorithm)

Amarpreet Singh, Vinay Bhardwaj
Research Scholar(Department of Computer Science),Sri Guru Granth Sahib World University, Fatehgarh Sahib
Asst.Professor(Department of Computer Science), Sri Guru Granth Sahib World University, Fatehgarh Sahib

Abstract
Fast Encryption Algorithm (FEAL) is an encryption/decryption technique used for the encryption/decryption of the grey scale images only. In this paper, FEAL is used for the encryption/decryption of colour images and text. In this, the key generation system for FEAL algorithm is updated using the XAND gate. By using the XAND gate, data cannot be deciphered using partial knowledge of key. This proposed system can also work upon the text data, which is firstly converted into bit sequence before making it an encrypted text. The comparison of the existing FEAL and proposed FEAL shows that the time taken by the proposed FEAL for the encryption /decryption of the grey scale image is less than that of the existing FEAL. To perform this research a simulation study is done using MATLAB. Along with this, JAVA is also used for obtaining the GUI as the applied for the results. The comparison of existing FEAL is done with the proposed FEAL on the basis of taken by the image to encrypt/decrypt. All the results are generated above defined simulator and are satisfactory.

Keywords:
FEAL, Encryption, XAND, MATLAB, JAVA.

1. Introduction

Cryptology is process of converting plain text to cipher text and vice versa. Cryptology deals with usage different varieties of cryptosystems to encrypt and decrypt the data with the use of a key. The party who is having a key is only able to encrypt or decrypt so that data is securely shared among the trusted parties. The cryptographic systems can be classified as private and public key cryptosystems. In public key cryptosystem there are mainly two keys. One key is public and is shared by all the parties. Other key is private and is secret. One key encrypts and other key is meant for decrypting the cipher text. Private key cryptographic method is one in which the same key is used to encrypt and decrypt the message. Cryptography and key exchange techniques are well described in [3-6]. Cryptosystem can be applied to any field where security is essential. Major interest of this paper is regarding cryptographic techniques associated with digital images. Given an image in any available formats such tiff, jpg, bmp, etc. the encrypted image results in unreadable (or cipher) image with same image format as that of the original image. Decryption of an encrypted image with proper key should result in retrieval of original image. Over the years many image cryptographic algorithms have been proposed by the researchers [11-13]. Still a lot of scope for research is available to design and develop the stronger cryptic techniques for images. The Fast Encryption Algorithm (FEAL) is a symmetric encryption algorithm, also called as Japanese Encryption algorithm. FEAL works almost similar to Data Encryption Standard algorithm (DES), but it is faster than DES. FEAL works in different standards like FEAL-4, FEAL-6 and so on up to FEAL-n. Here, „n" indicates the number of Feistel permutation rounds. To apply FEAL algorithm for image encryption, the input gray scale test image of size 256 X 256 matrix is divided into sixteen square matrices of size 16 X 16. These subdivided image matrices are treated as plain text for encryption. The key generation procedure uses fk(a ,b) function and generates 12 keys of size 16-bit each (K0 to KB). In which 6 keys are used for encryption of a message and rest of the 6 keys are used for the decryption of the cipher. XOR gate is applied in FEAL [13]. In this paper the encryption of colour images and text is discussed.

2. Problem Statement:

The Fast Encryption Algorithm (FEAL) is a symmetric encryption algorithm. The algorithm mainly uses 12 keys of size 16-bit each to perform encryption and decryption. It works in the frequency domain so it is less vulner with respect to the noise and other factors. The main problem in encryption with FEAL is that if the 80% of the data is decrypted by anyone, the whole of the secret message will be known. The other problem is that FEAL is used for the encryption of gray scale images only. In this defined problem we are improving the security of the data mining using the FEAL which falls in the category of frequency domain so it is less prone to other factors like noise, distortion or any kind of other unstructured or corrupted data. In spite of this, we will now modify FEAL for the encryption of colour images also. The image size was fixed, i.e. 256*256 pixels. Now we will make the size of

Manuscript received August 5, 2015
Manuscript revised August 20, 2015

image dynamic, so that the size of the image can be changed.

3. Related Study

• Nikolaos G. Bourbakis [8] presented an image data compression-encryption scheme by using the words (patterns, or orders) produced by an image processing language called SCAN.
• S.S. Maniccam and N.G. Bourbakis [9] have presented a new methodology which performs both
lossless compression and encryption of binary and gray-scale images. The compression and encryption
schemes are based on SCAN patterns generated by the SCAN methodology.
• Howard Cheng, Xiaobo li [10] performed compression using Quadtree compression Algorithm. But partial encryption is applied.
• Younggap You, Hanbyeori Kim [11] performed compression using DWT (Discrete Wavelet Transform). For encryption Standard Encryption algorithm AES or ARIA is used.
• Abdul Razzaque [12] gives an account of simultaneous image compression and encryption scheme is discussed. The order of the two processes viz. compression and encryption is EC i.e. image encryption is performed first then the image compression is applied. For image encryption a symmetric key cryptography multiplicative cipher is used. Similarly for compression Discrete Cosine Transform is used. In the proposed approach a private key cryptography is used for encryption without sharing the secret key. But image transmission is required two times. Therefore to save the bandwidth partial encryption is carried out. Image compression is concerned with minimizing the number of bit required to represent an image.
Image Encryption is hiding image from unauthorized access with the help of secret key that key can be private or public.
• D. Maheswari, V. Radha [13] employed lossless compression using a novel layer based compound
image compression technique that uses XML compression and JPEG to compress data. The encryption scheme, called, Shuffle Encryption Algorithm (SEA), proposed by Yahya and Abdalla (2008), is used.

4. Proposed FEAL:

In the proposed FEAL, the FEAL algorithm is extended to the encryption of colour images and text. Above all, the security in the FEAL is increased. The drawbacks of FEAL are improved in this. The drawbacks of FEAL were that it was used for the gray scale images of limited resolution only. Secondly if the 80% of the image is decrypted it is fully known that what the image really is. In the proposed scheme the text is encrypted using XAND gate key encryption. The proposed FEAL encryption technique is implemented using MATLAB simulation environment. MATLAB is installed on Intel i3 processor with 3 GB RAM computer with 32-bit Windows Operating System with. Using XAND gate the drawback of FEAL, that the encryption can get compromised if the key decryption is 80% similar to that of original key, is updated. The decrypted image to some extent reveals the information of original image. The images considered are only gray scale images of size 256x256 pixel resolution only. The above defined drawback of the FEAL is reduced in the proposed scheme as defined in the following flowchart.

5. Description of Flowchart

As defined in the below flowchart a text file is feeded to the FEAL encryption, and the key is generated using XAND gate to encrypt data. In case of binary data image is normalized into block of equal size and then it is encrypted using proposed scheme. In this work, a comparative study is also done with existing FEAL algorithm using a text as shown in figure 2 and 3. The encryption and decryption of images is shown in figure 4 and figure 5.

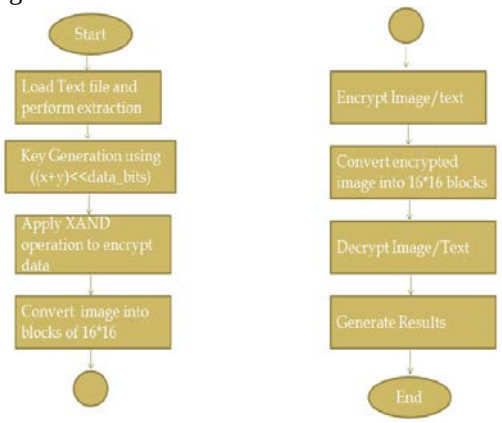

Figure 1: Flowchart for FEAL

6. Results and Discussion

In the results and discussion part the figure 2 and figure 3 described about the encrypted and decrypted image by using the proposed FEAL algorithm. Figure 2 shown below described about the encrypted data and figure 3 described about the Decrypted data. It shows about the browsing the text file, then it is encrypted. After this, the encrypted text is shown in new window. In the next step,

the encrypted data is decrypted. The decrypted data is then shown in the new window. The same is done for the encryption and decryption of images.
The encrypted image and decrypted image are shown in the figure 4 and figure 5.

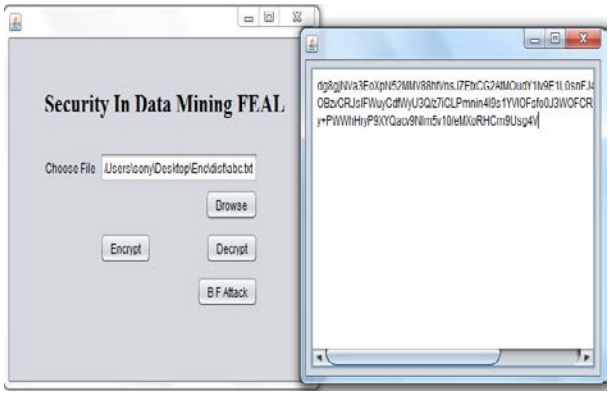

Fig 2: Encrypted Data

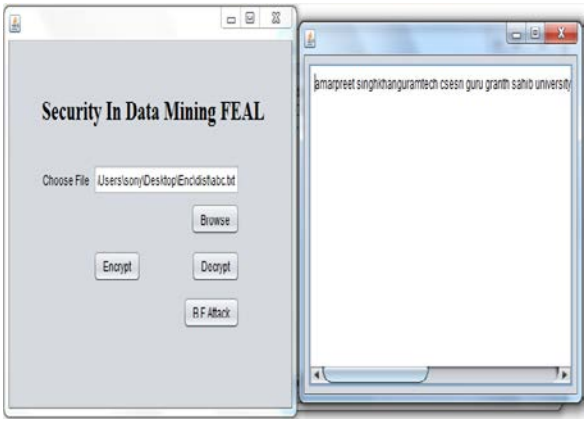

Fig 3: Decrypted Data

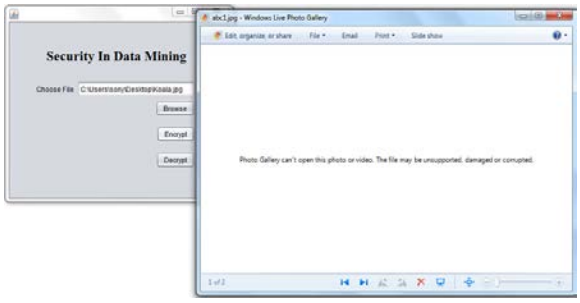

Fig 4: Encrypted Image

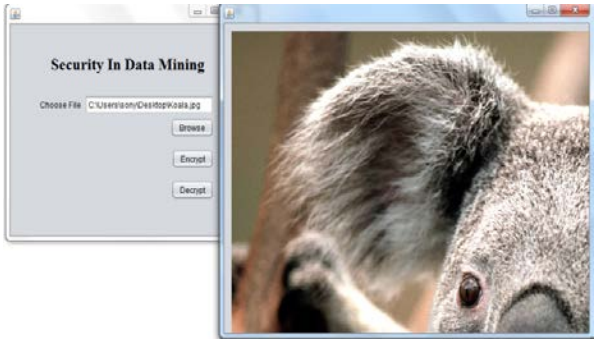

Fig 5: Decrypted Image

Conclusion:

In this research paper Fast Encryption Algorithm is modified to make it work on text and binary data. In the modification logic gate is modified to make key generation more secure. Also in this research FEAL is able to encrypt any type text of data where as previously it can-not work on text type of data, it was implemented only on gray scale images. Despite this, the FEAL can now be used for the encryption of colour images. The time comparison of the existing and the proposed FEAL is also done. It shows that the proposed FEAL takes less time than the existing FEAL. In the future, any video type of data can be encrypted using FEAL algorithm. Along with this, the data of large size takes more time to encrypt and decrypt, which can be minimized in the future.

References

[1] D. Luciano and Gordon Prichett. Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. The College Mathematics Journal, vol. 18, No. 1, pp. 2-17, January 1987.
[2] S. T. F. Al-Janabi and M. A. Rasheed. Public-Key Cryptography Enabled Kerberos Authentication. In Proc. Of IEEE conference on Developments in E-systems Engineering, pp. 209-214, Dec. 6-8, 2011
[3] G.P. Biswas. Diffie–Hellman technique: extended to multiple two-party keys and one multi-party key.Published in IET Information Security, vol. 2, No. 1, pp. 12– 18, 2008.
[4] R. Sharma. A Novel Approach to combine Public-key encryption with Symmetric-key encryption. The International Journal of Computer Science & Applications, Vol. 1, No. 4, pp. 8-15, June 2012
[5] Jithin VM,K K gupta (2013)"Robust invisible QR code image watermarking in DWT domain",2013.
[6] Nan Lin; Jianjing Shen; Xiaofeng Guo; Jun Zhou, "A robust image watermarking based on DWT-QR decomposition," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on , vol., no., pp.684,688, 27-29 May 2011.
[7] Nithin N. Anupkumar M Bongale, G. P. Hegde. "Image Encryption based on FEAL algorithm",International Journal of Advances in Computer Science and Technology , 2(2), March 2013, 14-20

[8] N.G. Bourbakis" Image and video encryption using SCAN patterns " Volume 37, Issue 4, April 2004, Pages 725–737
[9] S.S. Maniccam, N.G. Bourbakis" Lossless image compression and encryption using SCAN" Volume 34, Issue 6, June 2001, Pages 1229–1245
[10] Cheng, H. ; Xiaobo Li "Partial encryption of compressed images and videos" Volume 48, issue 8, Aug 2000
[11] Younggap You, Hanbyeori Kim" An Approach to Image Compression with Partial Encryption without sharing the Secret Key" IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012
[12] Abdul Razzaque 1 and Dr. Nileshsingh V.Thakur" An Approach to Image Compression with Partial Encryption without sharing the Secret Key" IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012
[13] D. Maheswari, V. Radha "Secure layer based compound image compression using XML compression" Dec 2010