ISSN 2320 - 2602

Volume 2, No.3, March 2013
International Journal of Advances in Computer Science and Technology
Available Online at http://warse.org/pdfs/2013/ijacst01232013.pdf

Image Encryption based on FEAL algorithm

Nithin N[1], Anupkumar M Bongale[2], G. P. Hegde[3]
[1]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, Karnataka, India
nisarga7777@gmail.com
[2]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal, Karnataka, India
ambongale@gmail.com
[3]Department of Computer Science and Engineering,
Shree Dhramasthala Manjunatheswara Institute of Technology, Ujire, Karnataka, India
gphegde123@gmail.com

ABSTRACT

Multimedia security is an important field of research in the area of information sharing. In this paper, Fast Encryption Algorithm (FEAL), an encryption/decryption strategy for gray scale images is proposed. The FEAL is a block cipher, also called as Japanese Encryption algorithm. FEAL works almost similar to Data Encryption Standard (DES) algorithm, but it is faster than DES. To encrypt the images, the input image is split into 16x16 blocks of information. Encryption/Decryption is carried out using 12 keys, each of length 16-bits. The proposed image encryption algorithm is evaluated based on histogram analysis and key sensitivity analysis and results obtained are satisfactory.

Key words: Image Encryption, Block Cipher, FEAL, Information Security, Multimedia Security.

1. INTRODUCTION

Over the computer network images, videos and other multimedia data are shared among connected users almost every day. As the days are passing, the usage of internet and sharing the images over social networks increasing exponentially. Provision of security to multimedia content is a major concern. Image security and encryption has become important area of research in the field of information security. Image encryption can be broadly classified into two types – encryption with compression and encryption without compression [1-6].

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 [7-10].

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. In this paper a recent set of cryptographic algorithms for images is discussed.

The rest of the paper is organized as follows. In section II, the recent algorithms proposed for image security and image encryption are discussed in detail. In section III, working of FEAL algorithm is described with necessary block diagrams. In section IV, experimental results are shown. Elaborated experimental results obtained by applying FEAL algorithm on standard image dataset are described. Section V consists of a brief conclusion and future work to be carried out.

2. RELATED WORK

Wide varieties of symmetric and asymmetric key algorithms are proposed for image encryption. Zhang et al. in [14] have proposed a new image encryption techniques based on chaos and improved Data Encryption Standard (DES) algorithm. Recently Chaos based image encryption technique has gained wide level of popularity. The basic principle of chaotic encryption technique is to encrypt the image using arbitrary random sequences and to deal with inflexibility associated with fast and secure image encryption. The authors have identified that chaos technique is having limitation as it may not produce the accurate encryption results. In this context, chaotic algorithm is modified with incorporation of improved DES encryption algorithm. Through theoretical analysis and the simulation, it is found that the technique is producing high

starting value sensitivity, and enjoys high security and the encryption speed.

Naveed et al. in [15] have exploited multiplicative homomorphic properties of RSA, may result in false data blocks during the extraction of message. A controlled solution by analyzing their probability distribution is suggested in the paper. The analysis concludes that "larger n, and hence p and q, not only provide high level of security but also reduces the error probability in extraction process, when used to exploit the multiplicative homomorphism of RSA". It is also observed, theoretically and practically that if the size of n and the gap between the primes p and q is small then the probability of false data can be reduced.

Modified Advanced Encryption Standard (MAES) is proposed in [16] for providing a high level security and better image encryption. Seyed et al. have specified that multimedia information is highly redundant in nature. By applying the encryption algorithm pixel by pixel may not lead to complete secure encrypted image. For example, the image shown in Figure 1 is encrypted by Advanced Encryption Standard (AES) algorithm directly. From Figure 1, still some information can be inferred from the cipher imge so as draw a conclusion on about the appearance of the original image. To overcome the problem of security issues associated with AES algorithm a modification is done by adjusting the Shift Row Transformation. Through experimentation, the authors have investigated the significance of the security of the MAES algorithm.

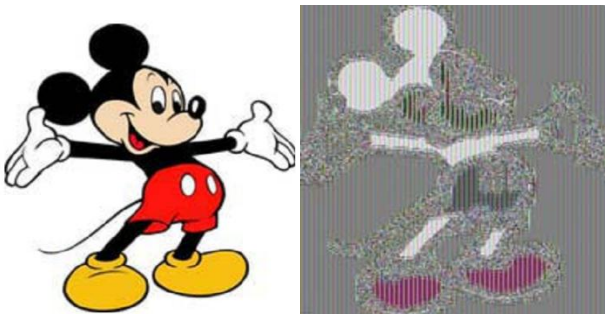


Figure 1: Application of the AES cipher to Mickey plain image\cipher image

Abirand Ali in [17] have proposed a novel chaos-based algorithm for image encryption. Initially image pixel points are shuffled using 2D chaotic map. The novelty of the image encryption lies in the incorporation of chaotic substitution method based on DNA coding and the complementary rule. To evaluate the security of the proposed method authors have conducted correlation test, information entropy analysis, histogram analysis, key sensitivity test and difference analysis between original and encrypted images. Paper concludes with result that "chaotic DNA substitution method enhances the statistical properties of the encrypted images".

Subramanyan et al. in [18] have proposed an algorithm based on AES Key Expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the a 128 bit key which changes for every set of pixels. The keys to be used are generated independently at the sender and receiver side based on AES Key Expansion process hence the initial key is alone shared rather than sharing the whole set of keys. Contribution of the proposed work lies in the modification of the AES Key Expansion. The major modifications introduced are (1) The initial key is expanded based on the number of pixels in the image (2) To improve the avalanche effect Rcon value formed from the initial key itself (3) Key Expansion is done using both the s-box and Inverse s-box (4) Circular shift is introduced in S-box and Inverse S-box to improve the key sensitivity. The encryption algorithm resulted in high encryption quality with minimal memory requirement and computational time. The key sensitivity and key space of the algorithm is very high which makes it resistant towards Brute force attack and statistical cryptanalysis of original and encrypted images.

Based on brief recent survey specified above it is observed that image encryption has been an active research area. Many researchers have proposed extensive encryption/decryption techniques suitable for color as well as gray scale images. Each of the techniques involves use of encryption algorithms by modifying them to suit the digital images. In this research article, FEAL based encryption algorithm is proposed for image encryption/decryption.

3. FAST ENCRYPTION ALGORITHM (FEAL)

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. The function in FEAL-4 uses two S-box functions S0 and S1 represented as follows:

$$S_0(x,y) = \big((x + y \ mod\ 256) \ll 2\big)$$

And

$$S_1(x,y) = ((x + y + 1 \ mod\ 256) \ll 2)$$

Function *f(a, b)* is meant for performing the linear functionality in FEAL encryption algorithm according to the Figure 2. Key generation function f_k uses both the S-boxes. The 64-bit key is divided into two equal parts of 32-bit each represented by *a* and*b* respectively. The keys *a* and*b* are further divided into 8-bits of the form *a1, a2, a3, a4, b1, b2, b3* and *b4*. The key generation function $f_k$is shown in Figure. 3.

The iterations of linear encryption functions in basic FEAL algorithm use 64-bit plain text and 64-bit key to encrypt and

decrypt the given plain text. 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 $f_k(a, b)$ function and generates 12 keys of size 16-bit each (K_0 to K_B). 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.

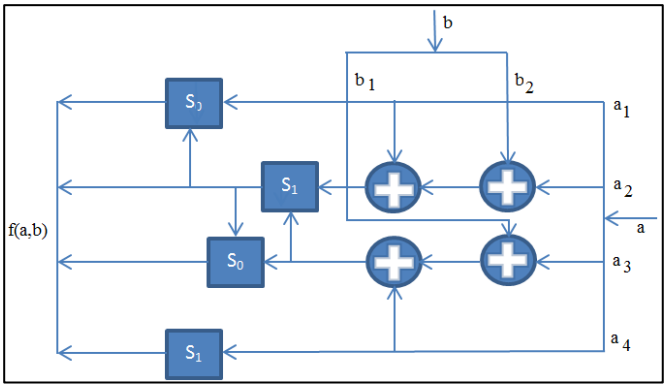


Figure 2: Function *f(a, b)*

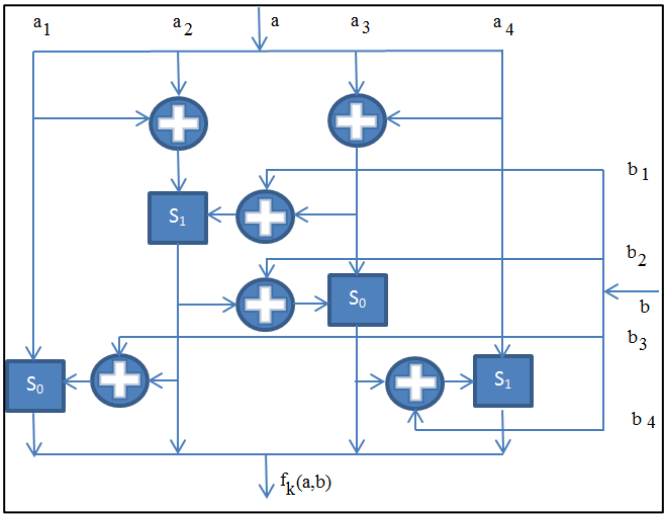


Figure 3: Key generation function f_k

The encryption and decryption process of FEAL algorithm, using these key sets which are generated by the key generation function $f_k(a,b)$. An encryption uses (k_4, k_5, k_6 and k_7) keys to perform concatenation operation before encryption. The keys k_0, k_1, k_2 and k_3 are used for cipher operation in each rounds. Set of keys (k_8, k_9, $k_A$and k_B) are used to generate the cipher text after the rounds with concatenation. The decryption is performed reverse order. The key pairs are (k_4, k_5, $k_6$and k_7) are used for concatenation operation with cipher text. The *keys* k_0, k_1, $k_2$and k_3 are used for decipher operation in each rounds. After the completion of rounds the text is contaminated with keys (k_8, k_9, $k_A$and k_B) to get the plain text. The key sets are same for encryption as well as decryption process. Only the order of keys used for encryption and decryption is different. FEAL is a simple encryption algorithm. In this paper FEAL-4 is used for encryption and the Figure 4 describe the key generation using key generation function with XOR operation is specified. In Figure 5 data encryption and decryption process is shown, which uses the keys generated by key generation function. These keys are used for concatenationoperation with plain text and cipher text. The four keys are used in rounds r_0 to r_3, which will produce the cipher text [19].

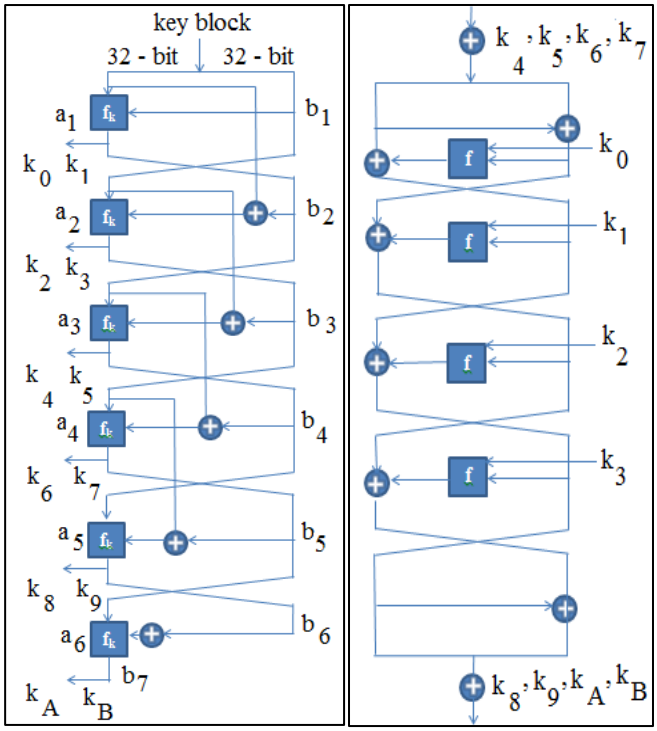


Figure 4: Key generation, Encryption and Decryption process using FEAL

4. Experimental Results

The FEAL image encryption technique is implemented using MATLAB simulation environment.MATLAB is installed on Intel Core 2 Duo CPU with 2 GB RAM computer with 32-bit Windows 7 Operating System. To validate the encryption strategy of FEAL, image database maintained in [20] is used. The image database contains standard test images of Lena, peppers, cameraman, lake, etc., all in uncompressed *.tif* format and of the same 512 x 512 size. For our experimentation purpose only three of the images are considered. All the images are pre-processed to convert them to 256x256 pixel resolution gray scale images of JPEG image compression format. For encryption, the input image is split into 16 sub-images of size 16x16 pixel resolution each. The sub images are encrypted separately and combined to get the actual encrypted image. Same process is used for decryption also. During decryption procedure, cipher image are converted into 16x16 pixel sub-images and the performed decryption key substitution. Thorough experimental evaluation is performed and discussed about the same in the next sub sections.

4.1 FEAL Encryption/Decryption-

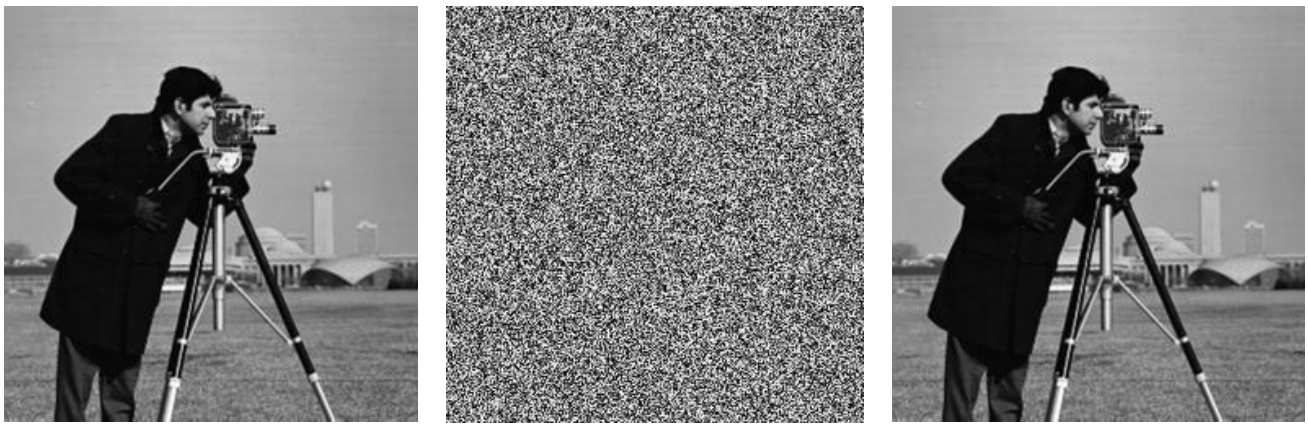
FEAL has been validated using series of experiments. Figure 5-7 show result of application of FEAL algorithm on standard image dataset to obtain encrypted and decrypted images. Encrypted images visually appear secure enough and decryption leads to successful retrieval of original image.

4.2 Histogram analysis-

In an image, neighboring pixels will be having statistical similarity with respect to color and intensity levels. A good encryption strategy should lead to secure encrypted image. Image histograms help in understanding the similarity measure among the pixels. If there is no or negligible similarity among the pixels then cipher image is secure from adversary attacks. Figure 8 shows the histogram of Cameraman image. Figure 8(b) represents the histogram plot of original plain image shown in Figure 8(a). It can observe that statistical relation among the pixels has resulted in variation in the histogram plot. Figure 8(d) represents the histogram plot of encrypted image shown in Figure 8(c). It is clear from the histogram plot shown in figure 8(d) that adversary may infer least information from the ciphered image as neighboring images are least related one another. Thus our proposed encryption strategy avoids any statistical attacks that can be performed on encrypted image.

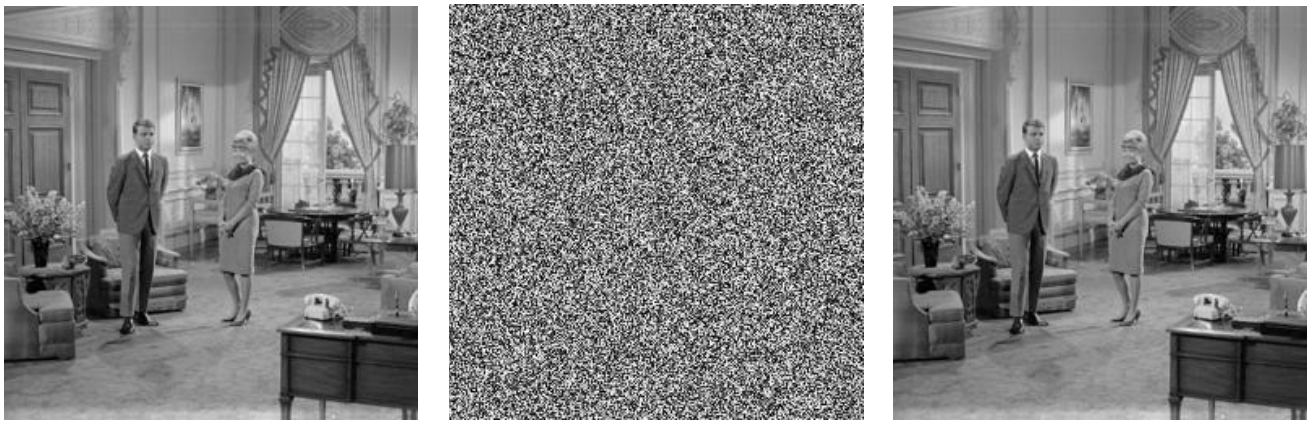
4.3 Key Sensitivity Analysis-

Encryption technique should be secure enough even if there is little modification in key. If the adversaries somehow guess the partial correct key then also the encryption should not be compromised. In this direction, key sensitivity analysis is performed by modifying the two byte information of the valid key. Figure 9 shows the decryption of encrypted image with the valid key: 4b444b2933. Figure 10 shows decryption of ciphered image with the key: 4b3E4243AD. Here except first two hexadecimal digits rest of the key is completely different. Under such a circumstance the encryption strategy is secure. But in figure 11, decryption is carried out using the key: 4b444b29AD (except last two digits rest of thekey is same as valid key). The encryption strategy compromises by revealing the information of the original image as shown in figure 11(c). Proposed algorithm is not very well secure if the key is 80% similar to the valid key.



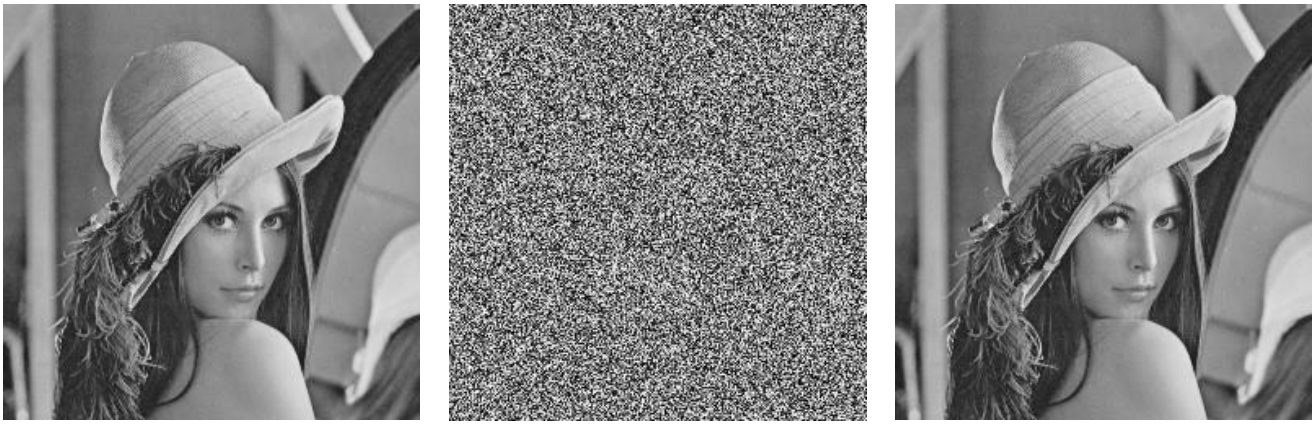
(a) Original Image (b) Cipher Image (c) Deciphered Image

Figure 5: Application of FEAL encryption on Cameraman.jpg



(a) Original Image (b) Cipher Image (c) Deciphered Image

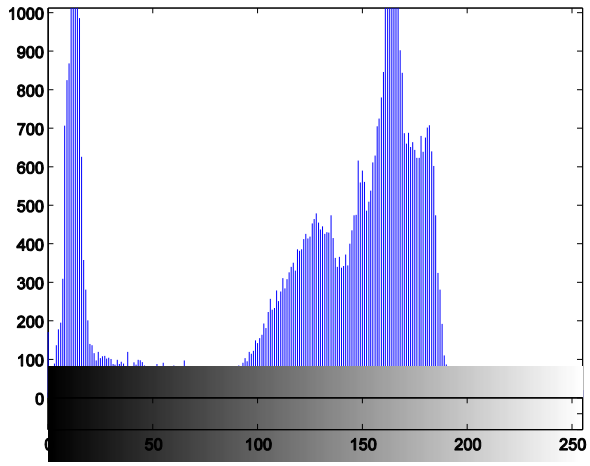
Figure 6: Application of FEAL encryption on Livingroom.jpg



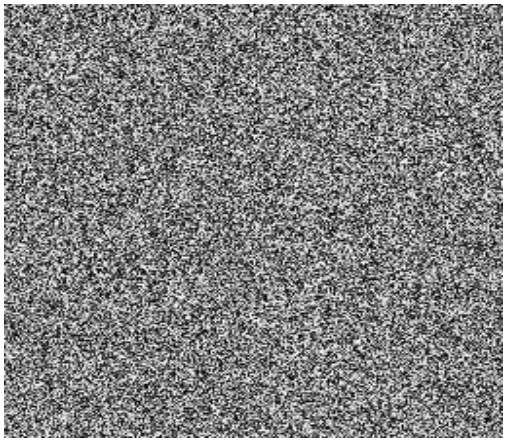
(a) Original Image (b) Cipher Image (c) Deciphered Image

Figure 7: Application of FEAL encryption on Lena.jpg

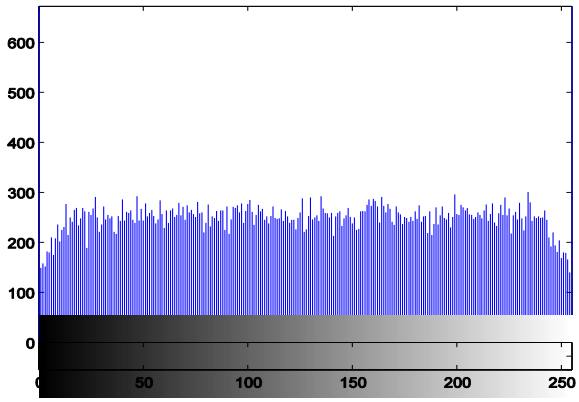
(a) Original Image



(b) Histogram of Original Image

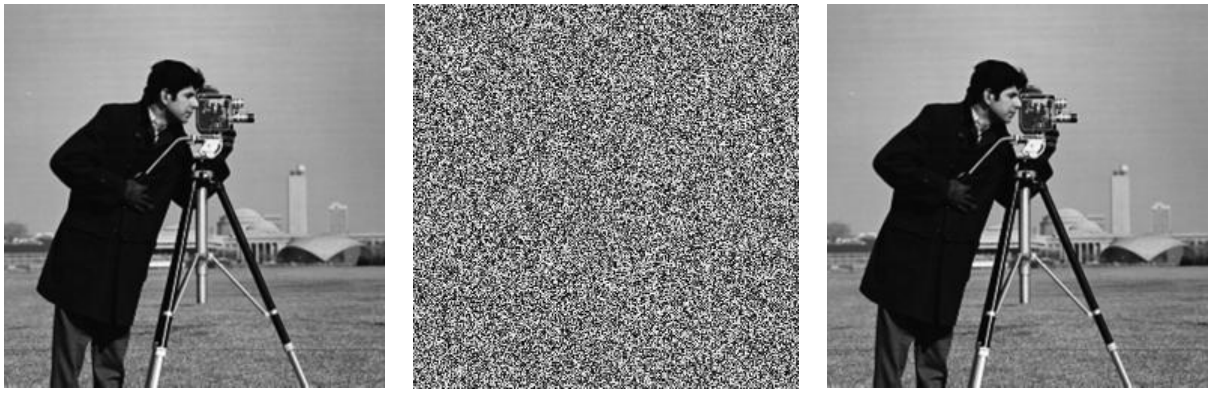


(c) Cipher Image



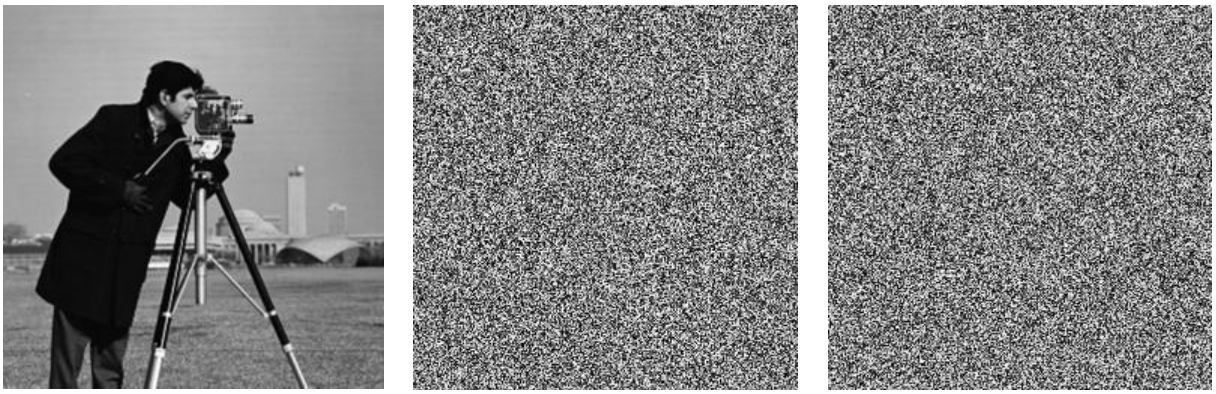
(d) Histogram of Cipher Image

Figure 8: Histogram of Plain Ciphered Cameraman Image



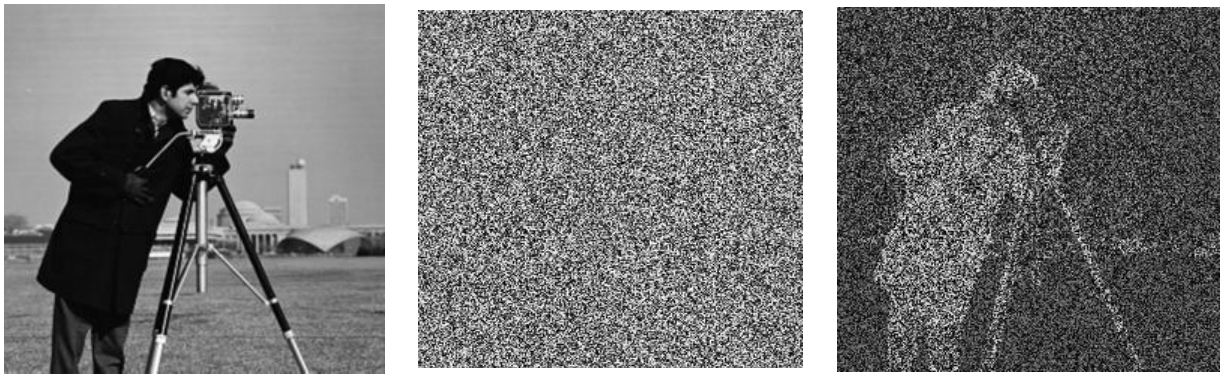
(a) Original Image (b) Cipher Image Key: 4b444b2933 (Correct) (c) Deciphered Image

Figure 9: Decryption using Correct Key (Key: 4b444b2933)



(a) Original Image (b) Cipher Image Key: 4b3E4243AD (Incorrect) (c) Deciphered Image

Figure 10: Decryption using Wrong Key (Key: 4b3E4243AD)



(a) Original Image (b) Cipher Image Key: 4b444b29AD (Incorrect) (c) Deciphered Image

Figure 11: Decryption using Wrong Key (Key: 4b444b29AD)

5. CONCLUSION

In this paper image encryption and decryption strategy based on FEAL algorithm is proposed. The algorithm mainly uses 12 keys of size 16-bit each to perform encryption and decryption. Standard dataset is used to carry out the experiments to validate the FEAL encryption strategy for images. Encryption is found to be satisfactory visually and through histograms analysis. But the proposed algorithm is having some drawbacks with respect to key sensitivity. It is observed that the encryption can get compromised if the key decryption is 80% similar to that of original key. 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. In future, an attempt to improve for the proposed algorithm to address the

mentioned drawback will be made. Encryption algorithm will be extended for color and higher resolution images as well.

REFERENCES

1. G. M. Priya and P. V. Kumari. **Compression of Quasi-Group Encrypted Grayscale Images**. *International Journal of Scientific and Research Publications*, vol. 2, No. 7, pp. 1-4, July 2012.
2. S. S. Kumar and H. Mangalam. **Wavelet-based Image Compression of Quasi Encrypted Grayscale Images**.*International Journal of Computer Applications (0975 – 8887)*, vol. 45, No.12, pp. 35-39, May 2012.
3. R. Ye. **A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism**.*In Proc. Of Optics Communications*, vol. 284, No. 22, pp. 5290-5298, Oct. 2011.
4. S. Tedmori and N. Al-Najdawi. **Lossless image cryptography algorithm based on discrete cosinee transform.***The International Arab Journal of Information Technology*, vol. 9, No. 5, pp. 471-478, September 2012.
5. S. Al-Maadeed, A. Al-Ali and T. Abdalla. **A New Chaos-Based Image-Encryption and Compression Algorithm.** *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1-11, 2012.
6. F. Ahmed,M. Y. Siyal and V. U. Abbas. **A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme.** *In Proc. Of IEEE conference on Fourth Pacific-Rim Symposium on Image and Video Technology (PSIVT)*, pp. 232-238, Nov. 14-17, 2010.
7. 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.
8. 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.
9. 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.
10. 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.
11. V. Bhatt and G. S. Chandel. **Implementation of new advance image encryption algorithm to enhance security of multimedia component**. *International Journal of Advanced Technology & Engineering Research*, vol. 2, Issue 4, pp. 17-20, July 2012.
12. S. Dey. **SD-EI: A Cryptographic Technique To Encrypt Images**. *In Proc. Of IEEE international conference in Cyber Security, Cyber Warfare and Digital Forensic*, pp. 28-32, Jun 26-28, 2012.
13. I. Landge, B. Contractor, A. Patel and R. Choudhary. **Image encryption and decryption using blowfish algorithm**. *World Journal of Science and Technology*, vol. 2, No. 5, pp. 151-156, 2012.
14. Z. Yun-peng, Z. Zheng-jun, L. Wei, N. Xuan, C. Shui-ping and D. Wei-di. **Digital Image Encryption Algorithm Based on Chaos and Improved DES**.*In Proc. of the IEEE International Conference on Systems*, Man, and Cybernetics, San Antonio, TX, USA, pp. 474-479, October 2009.
15. N. Islam, W. Puech, K. Hayat and R. Brouzet. **Analysis of homomorphic properties of RSA based cryptosystem for image sharing**. *In Proc. Of IEEE conference on Signal Processing*, pp. 1825-1828, 2010.
16. S. H. Kamali, M. Hedayati, R. Shakerian and M. Rahmani. **A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption**. *In Proc. of International Conference on Electronics and Information Engineering*, vol 1, pp. 141-145, 2010.
17. A. Awad and A. Miri. **A New Image Encryption Algorithm Based on a Chaotic DNA Substitution Method**. *In Proc. Of IEEE international conference on communication*, pp. 1011-1015, 2012.
18. B. Subramanyan, V. M. Chhabria and T. G. S. babu. **Image Encryption Based On AES Key Expansion**. *In Proc. Of IEEE Second International Conference on Emerging Applications of Information Technology*, pp. 217-220, 2011.
19. J. Pieprzyk, T. Hardjono and J. Seberry. **Fundamentals of Computer Security**. *Published by Srpinger-Verlag Berlin HeidelBerg*, Newyork, pp.106-108, 2003.
20. http://www.imageprocessingplace.com/root_files_V3/image_databases.htm