Journal of Computer Science 4 (2): 125-128, 2008
ISSN 1549-3636

Testing Image Encryption by Output Feedback (OFB)

Yas A. Alsultanny
College of Graduate Studies, Technology Management Program,
Arabian Gulf University, Manama, P.O. Box 26671, Kingdom of Bahrain

Abstract: When it is necessary to securely transmit data in open networks, the encryption must be performed. Most of the cryptographic algorithms were mainly developed for text data. Unfortunately, algorithms those are good for textual data might not suitable for image. The OFB mode of encryption implemented to test five images of different resources, by using three combinations (schemes): a combination of an 8-bit input block with an 8-bit feedback block, a combination of an 8-bit input block with a 16-bit, or a combination of a 16-bit input block with a 16-bit feedback block. Results showed that higher degree of encryption achieved when the input block and the feedback block are of the same size. The OFB mode achieved a mid range level of encryption with a mean entropy value of 7.93.

Key words: Image encryption, output feedback mode, encryption modes, image processing

INTRODUCTION

Internet and wireless network offer powerful channels to deliver and exchange images. The increased popularity of image exchange places a great demand on efficient image storage and transmission techniques. The major hurdle for allowing much broader access of digital images lies in how to make sure that an image is used for its intended purpose, by its intended recipients. Sensitive and confidential information is vulnerable to various kinds of misuse when data is transmitted to/from computer system. Many business and medical organizations worry about users finding ways to alter the contents of their image files. Such alteration might be used, for example, to change an x-ray photograph, discover a debit card number, or forget a hand-written signature on the bitmap of a check[1]. The core issue then becomes the development of secure management usage of digital images across communication networks[2].

SECURITY ISSUES OF A CRYPTOGRAPHIC ALGORITHM

One of the most important properties of a cryptographic system is a proof of its security. Different algorithms offer different degrees of security; it depends on how hard they are to break. If the cost required breaking an algorithm is greater than the value of encrypted data, or if the time required to break an algorithm is longer than the time the encrypted data must remain secret, then the algorithm is secure[3].

OUTPUT FEEDBACK MODE (OFB)

This mode prevents the same block of data from generating the ciphered block by using an internal feedback mechanism that is independent of both the original data and the ciphered data. Figure (1a) shows the mechanism of encryption. Figure (1b) shows the mechanism of decryption.

Where:
IV: The random Initial Vector
P_n : The n^{th} original block
C_n: The n^{th} ciphered block

ENTROPY VALUE MEASUREMENT

Entropy value, a concept of information theory, can be thought of as a mathematical measure of information or uncertainty of a true value of a random variable. If (X) is a random variable which takes values according to a probability distribution p (X), then the entropy value H (X) can be computed by using this quantity:

$$H(X) = -\sum_{i=0}^{(n-1)^2} p_i \log_2 p$$

i= 0,1 and (n-1)2 to an image of (n*n) dimension

Entropy is also useful for approximating the average number of bits required to encode the elements of (X). In general, the greater the entropy, then it is harder to break a cryptosystem[4].

IMPLEMENTATION OF (OFB)

For applications in which all error propagation must be avoided, OFB mode of operation may be used. Its structure is similar to that of CFB[5], but the output of encryption function is fed back to the shift register (IV) as shown in Fig. 1. If the same key is used for different images, IV value must be changed; otherwise, there is no security[3,6]. Each ciphered block is independent of both the original data and the previous ciphered blocks. This mode is implemented by using a flowchart shown in Fig. 2.

Since OFB has the same structure as that of CFB[7], then there are two main factors that may affect on encryption degree: input block size and feedback block size. To do this, the three schemes of block size (8-bit, 16-bit, and 32-bit), in addition to, the three schemes of feedback size (8-bit, 16-bit, and 32-bit) are employed. In fact, there are three combinations (schemes): a combination of an 8-bit input block with an 8-bit feedback block (scheme1), a combination of an 8-bit input block with a 16-bit (scheme2), or a combination of a 16-bit input block with a 16-bit feedback block (scheme3).

When OFB mode is implemented by using, these three schemes, then the result in the experimental results are shown in Fig. 3.

Figure 3b shows the encrypted image of the LENNA with its histogram by using scheme1 (8-bit input block with 8-bit feedback block), Fig. 3c shows the encrypted image with its histogram by using scheme2 (8-bit input block with 16-bit feedback block). Figure 3d shows the encryption by using scheme3 (16-bit input block with 16-bit feedback block), with its histogram.

In fact, there are some boundaries and edges exist to the encrypted image, but in different scales. It seems that the scheme1 and scheme3 achieved higher degree of encryption than that achieved by using scheme2 because there are less boundaries and edges. Which mean that, the OFB mode can achieve the highest degree of encryption when it's implemented with a scheme of an 8-bit input block and an 8-bit feedback block or with a scheme of a 16-bit input block and a 16-bit feedback block. In other words, the OFB mode can achieve the highest degree of encryption when it is implemented with an input block of the same size as that of the feedback block.

When applying the same procedure of OFB to SAT image, the experimental results are shown in Fig. 4. Figure 4b shows the encrypted image of SAT with its histogram by using scheme1 (8-bit input block with 8-bit feedback block). Figure 4c shows the encryption of

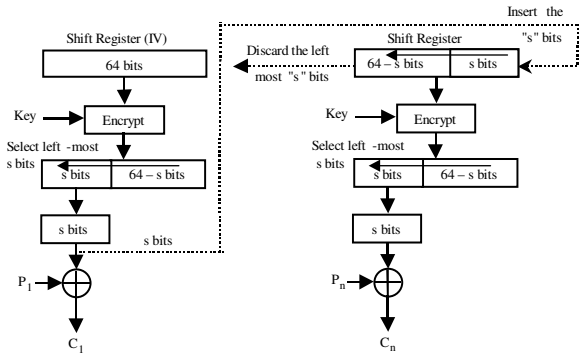


Fig. 1: The OFB mode

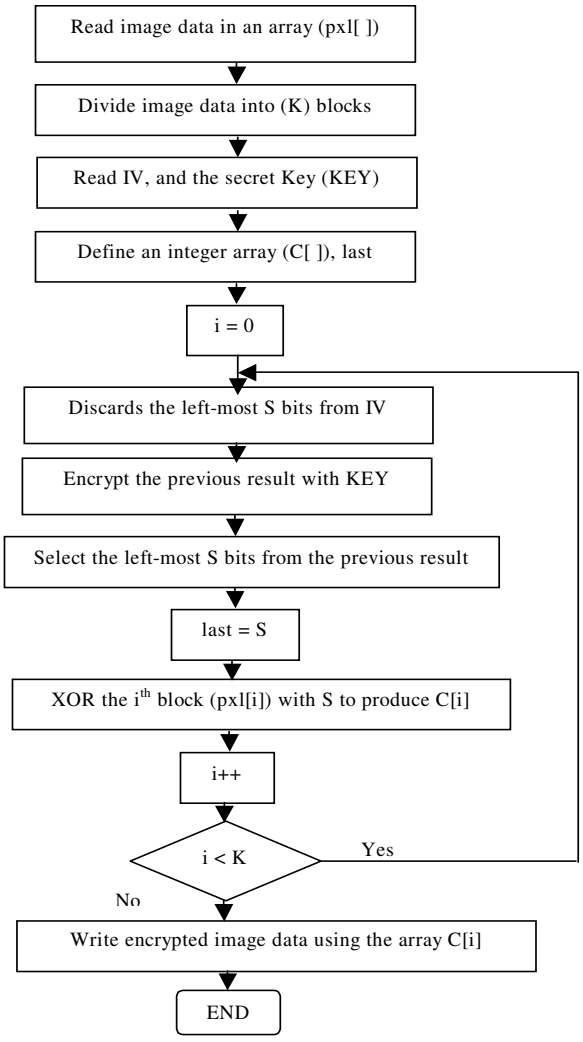
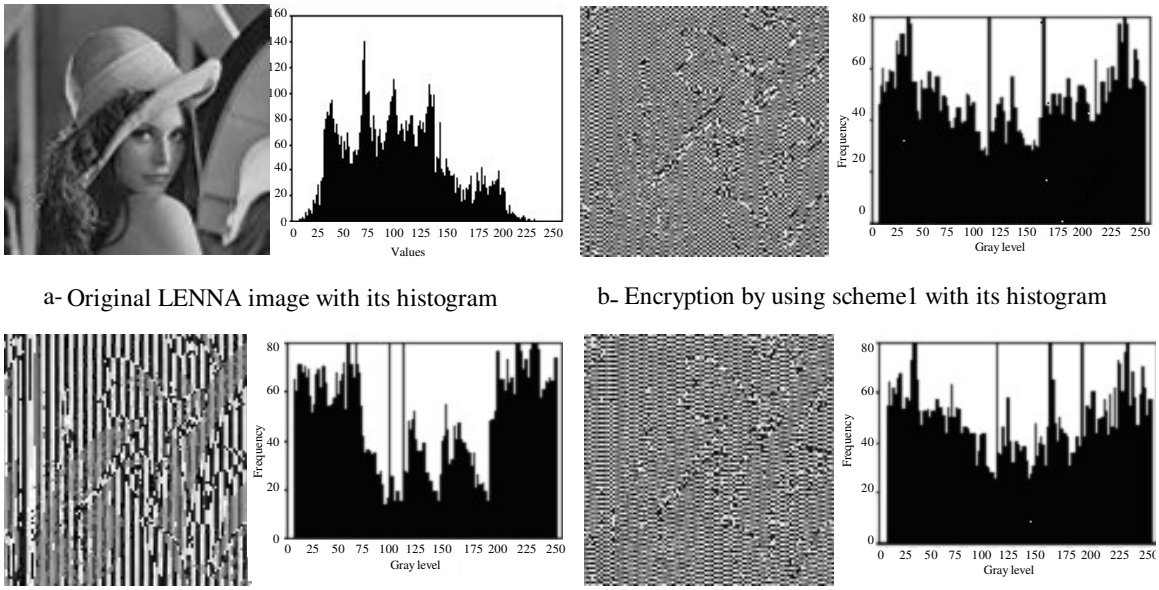


Fig. 2: Flowchart of OFB mode

the SAT image by using scheme2 (8-bit input block with 16-bit feedback block), Figure 4d shows the



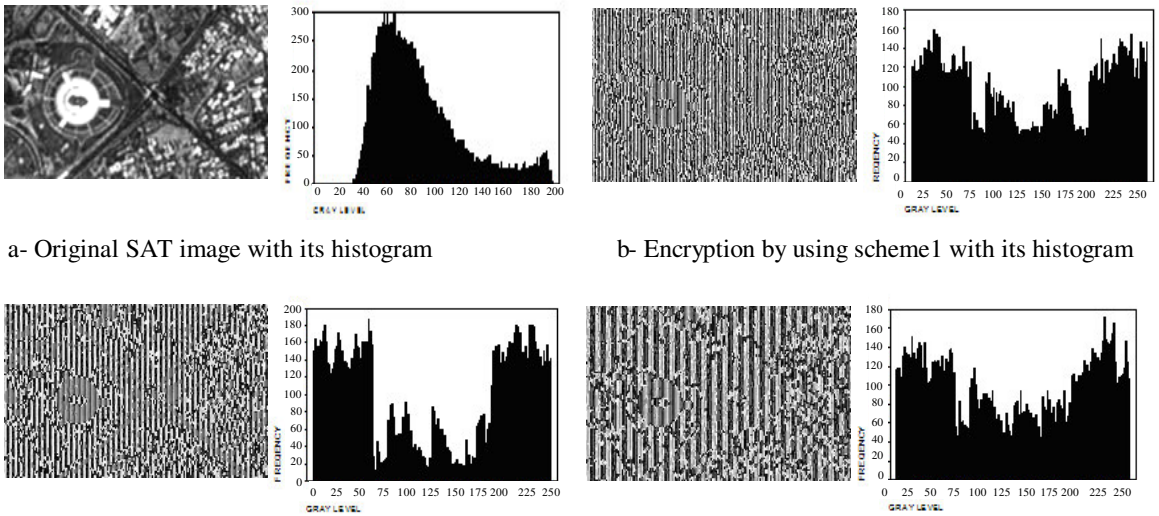
a- Original LENNA image with its histogram

b- Encryption by using scheme1 with its histogram

c- Encryption by using scheme2 with its histogram

d- Encryption by using scheme3 with its histogram

Fig. 3: Encryption of the LENNA image by using OFB with different schemes



a- Original SAT image with its histogram

b- Encryption by using scheme1 with its histogram

c- Encryption by using scheme2 with its histogram

d- Encryption by using scheme3 with its histogram

Fig. 4: Encryption of the SAT image by using OFB with the different three schemes

encryption of the SAT image by using scheme3 (16-bit input block with 16-bit feedback block).

As seen from the histograms of the encryption of the LENNA image, pixel values don't dissipate in a uniform distribution, but they dissipate in a wide range especially in the cases of scheme1 and scheme3. This may result in a mid-range degree of encryption in scheme 2. On the other hand, pixel values in the case of scheme 1 and scheme3 dissipate in a distribution that it not gave useful information to cryptanalyst. As a result, scheme1 and scheme3 achieve a good encryption degree, whereas, scheme2 achieves a low degree of encryption. Pixel values don't dissipate equally but they dissipate in a wide range especially those pixel values

Table 1: The entropy to the five images before and after encryption with the different schemes

Original Image		Scheme1	Scheme2	Scheme3
Lenna	7.49102	7.9168	7.83269	7.92834
Sat	7.28905	7.9134	7.70228	7.92216
Airplane	7.03743	7.9009	7.7719	7.8933
Cat	6.75757	7.78071	7.31998	7.78261
Greece	5.91171	7.60284	7.18036	7.61707

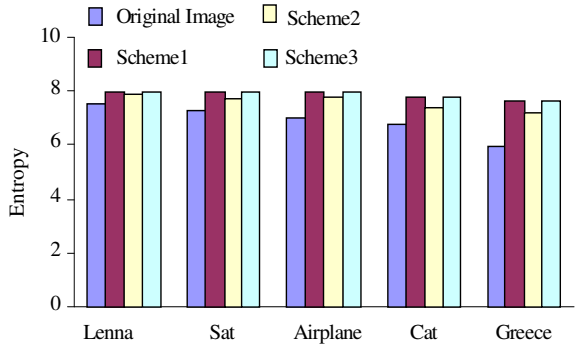


Fig. 6: The entropy to the encrypted images by using OFB mode with the different three schemes

in the cases of scheme1 and scheme3. Whereas, pixel values in scheme 2 dissipated in a way that it may gave useful information to cryptanalyst. These analyses show that OFB mode achieves its highest degree of encryption in cases of scheme1 and scheme3 in which the feedback block is the same size as that of input block.

RESULT AND DISCUSSION

The security level of this mode can be measured by computing entropy value. Entropy values are computed to the five images of different resources before and after encryption by using different schemes as shown in Table 1.

These results also can be illustrated in Fig. 6, by constructing the bar chart to the computed entropy values.

It is clear from this figure that the OFB achieves the highest degree of encryption, when it is implemented by using scheme1 or scheme3, which means that when OFB is implemented by using an input block of the same size as that of the feedback block.

CONCLUSIONS

For image encryption purposes, there are two important things that must be taken in account when we are encrypting images: the mode of encryption and the block size of the input data.

The size of the input data block and the size of the feedback block, play an important role in determining the degree of encryption. The highest degree of encryption can be obtained, when both the size of the input block and the feedback block are of the same size of 8 bits or 16 bits. We can conclude that the highest degree of encryption can be obtained when the input data block and the feedback block are of the same size.

REFERENCES

1. James D. Murray and William Vanryper, 1996. Encyclopedia of Graphics File Formats. 2nd Edn., O'Reilly and Associates, Inc.
2. Rafael C. Gonzalez and Richard E. Woods, 2002. Digital Image Processing. Prentice-Hall, Inc.
3. Bruce Schneier, 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., John Wiley and Sons, Inc.
4. Chung-Ping Wu and C.C. Jay Kuo, 2001. Efficient Multimedia Encryption via Entropy Codec Design. Proceedings of SPIE Vol. 4314.
5. Alsultanny, Y., 2004. Comparison of Image Ciphering using Different Modes of Encryption. ICIT2004, the 1st International Conference on Technology and Information Technology, pp: 49-56.
6. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 1997. Handbook of Applied Cryptography, CRC Press.
7. Alsultanny, Y., 2007. Image Encryption by Cipher Feedback Mode (CFB). Int. J. Innovat. Comput., Inform. Control, 4: 1-7.