Selective Bitplane Encryption For Secure Transmission Of Image Data In Mobile Environment

Nazneen M. G, Sufia Banu, Zahira Tabassum, Khamer Fatima, Arshiya Shariff S

Abstract: In this paper, we propose selective bitplane encryption to provide secure image transmission in low power mobile environment. We assume a 512 X 512 pixels image to be given in 8bit/pixel (bpp) precision. We consider the 8bpp data in the form of 8 bit planes, each bit plane associated with a position in the binary representation of the pixels. The Selective or partial encryption (SE) approach is to AES encrypt a subset of the bit planes only, starting with the bitplane containing the most significant bit (MSB) of the pixel. Each possible subset of bit planes may be chosen for SE the minimal percentage of data to be encrypted is 12.5 % increasing in steps of 12.5 % for each additional bitplane encrypted.

Index Terms: Advanced Encryption Standard (AES), Bitplane, Low Power, Minimal percentage, Secure Image Transmission, Selective Encryption (SE), 8 bit/pixel (bpp) precision,

1 INTRODUCTION

This paper gives an application in the area of multimedia security, the terms “selective encryption” or “soft encryption “are sometimes used as opposed to classical “hard” encryption schemes like the Advanced Encryption Standard. Such schemes do not strive for maximum security and trade off security for computational complexity. They are designed to protect multimedia content and fulfill the security requirements for a particular multimedia called application. For example, real-time encryption for an entire video stream using classical ciphers requires much computation time due to the large amounts of data involved, on the other hand many multimedia applications require security on a lower. Therefore, the search for fast encryption procedures specifically tailored to the target environment is mandatory for multimedia security applications. Selective or partial encryption (SE) of visual data is an example for such an approach. Here, application specific data structures are exploited to create more efficient encryption systems. Consequently, selective encryption only protects the visually most important parts of an image or video representation relying on a secure but slow “classical” cipher. In this work we propose and evaluate selective bit plane encryption for confidential transmission of image data in mobile environments.

2 OBJECTIVES

- Fast encryption.
- Lossless compression.
- Secure image transmission in low power mobile environments.

3 SELECTIVE BITPLANE ENCRYPTION

Intuitively, SE seems to be a good idea in any case since it is always desirable to reduce the computational demand involved in image processing applications. However, the security of such schemes is always lower as compared to full encryption. The only reasons to accept this drawback are *significant* savings in terms of processing time or power. Therefore, the environment in which SE should be applied needs to be investigated thoroughly in order to decide whether its use is sensible or not. Due to requirements of certain applications a loss of image quality may not be acceptable during transmission or storage (e.g., in medical applications because of reasons related to legal aspects and diagnosis accuracy [21]). Therefore, lossless compression schemes need to be employed for such applications. We assume a target environment, where due to the low processing power of the involved hardware not even lossless compression and decompression of visual data is reasonable or possible (e.g. mobile clients). Additionally, due to the increasing bandwidth available at mobile communication channels, compression seems not to be mandatory in any case, which is especially true for lossless applications. The reason is that the data reduction of lossless compression schemes is much lower as compared to lossy ones making the respective application less profitable. Note also that the time demand for compression is significantly higher as the time demand for encryption for almost all high quality codecs and symmetrical ciphers (which is mostly due to the efficient cache use of block-based encryption).

4 METHODOLOGY

4.1 GENERATION OF BITPLANES

We assume a 512 X 512 pixels image to be given in 8bit/pixel (bpp) precision. Each pixel has a gray value between 0 and255 For example, dark pixel may have a value of 10 and a bright pixel might have a value of 230. The entire image can be considered as a two dimensional array of pixel values. We consider the 8bpp data in the form of 8 bit planes, each bit plane associated with a position in the binary representation of the pixels.8 bit data is a set of 8 bitplanes. Each bitplane may have a value of 0 or 1 at each pixel, but together all the bitplanes makeup a byte with value between 0 to 255.Given below are the bitplanes of lena image.

Fig. 1 Lena

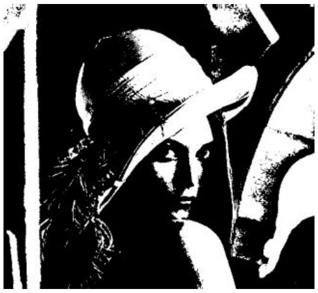


Fig 2: MSB Bitplane

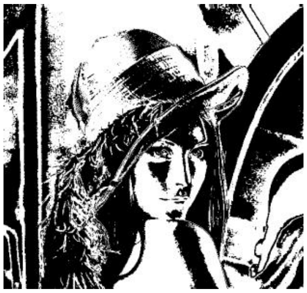


Fig 3: 7th Bitplane

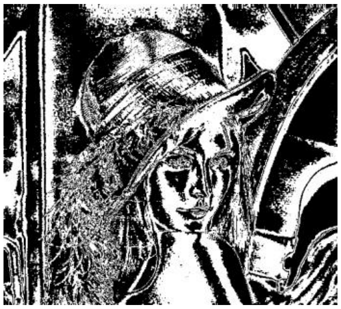


Fig 4: 6th Bitplane

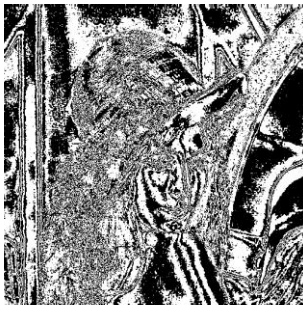


Fig 5: 5th Bitplane

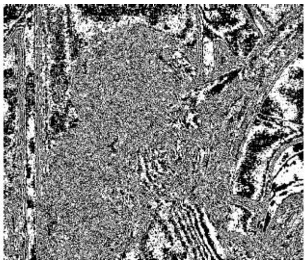


Fig 6: 4th Bitplane

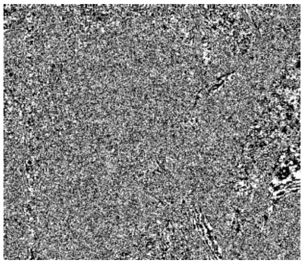


Fig 7: 3rd Bitplane

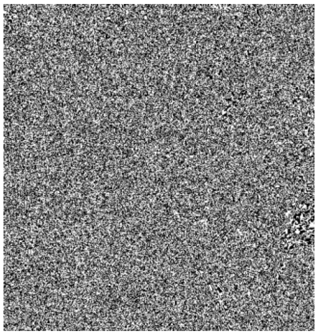


Fig 8: 2nd Bitplane

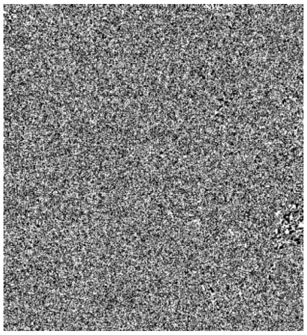


Fig 9: 1st Bitplane

4.2 Encryption Of Single Bitplane

The SE approach is to AES encrypt a subset of the bitplanes only, starting with the bitplane containing the most significant bit (MSB) of the pixels. Each possible subset of bitplanes may be chosen for SE, however, the minimal percentage of data to be encrypted is 12.5 % (when encrypting the MSB bitplane only), increasing in steps of 12.5 % for each additional bitplane encrypted. We use an AES implementation with block size 128 bit and a 128 bit key. The 128 bit block is filled with a quater of a bit plane line .The encrypted bitplanes are transmitted together with the remaining bitplanes in plain text. In the encrypted MSB of the Lena image we can see the barcode pattern. This phenomenon is due to the fact that AES encryption is used with identical key for all blocks in the image. Consequently, if there are identical plain text quater-lines directly situated above each other which also adhere to the AES block-border (i.e. starting at pixel positions 0, 128, 256, or 384), these data produce identical cipher text blocks. Identical blocks of cipher text are again arranged as identical quater-lines thereby generating the barcode effect. In the case of encrypting the MSB only structural information is still visible.

4.3 Encryption Of Selective Bitplane

Figure shows images after selectively encrypting 1 and 2 bitplane(s). Whereas in the case of encrypting the MSB only structural information is still visible, encrypting two bitplanes leaves no useful information in the reconstruction, at least when directly reconstructing the image data.

5 SECURITY ANALYSIS BY STATISTICAL APPROACH

The aim of this section is to assess the security of many SE investigations is the lack of the quantifying the quality of selective bitplane encryption by conducting two types of simple cipher text-only attacks. A shortcoming visual data that can be obtained by attacks against SE. Mostly visual examples The reason is the poor correlation of PSNR and other simple quality measures and perceived quality especially for low-quality images.

5.1 STATISTICAL ANALYSIS

5.1.1 HISTOGRAMS OF ENCRYPTED IMAGES

The histogram of an image represents the relative frequency of occurrence of the various gray levels in the image. The histogram of a digital image with gray levels in the range [0, L-1] is a discrete function.

$$P\ (r_k) = n_k /n \qquad (1)$$

Where, r_k is the k^{th} gray level, nk is the number of pixels in the image, and k=0, 1, 2,3……L-1.

P (r_k) gives an estimate of the probability of occurrence of $r_{k.}$ A plot of this function for all a values of k provides a global description of the appearance of image.

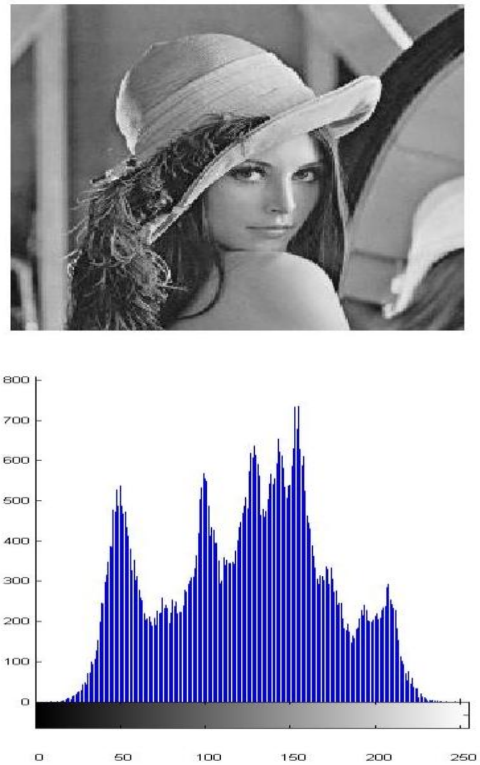


Fig 10: Lina and its Histogram

For dark images the histogram will be concentrated towards the dark end of the gray scale range. The opposite is true for low contrast images. We can see that the histogram of the ciphered image as shown in the figure 5.1 is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration. Moreover, there is no loss of image quality after performing the encryption/decryption steps.

5.1.2 ENTROPY AND CORRELATION

- **ENTROPY**: Let A be a image of size N then the entropy of A is written as,

$$H(A) = -\sum_{i=0}^{255} p(x_i) log_2(p(x_i));$$

  Where p (xi) = n/N is the correlation of the pixel xi, and n is the number of grey levels that repeat themselves.

- **CORRELATION**: We test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered image. First, we randomly select n pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient of each pair (x, y) by using the following formula.

$$r = cov(x, y) / var(x)*var(y) \qquad (3)$$

Where,

x and y are gray-scale values of two adjacent pixels in the image and r is coefficient of correlation.

6 RESULTS AND CONCLUSION

We have performed encryption on a standard grayscale image. The image used is of size 512x512.The images are first encrypted using normal AES algorithm and then decrypted. The images are first converted to plaintext using matlab code. The text file obtained is then given as the input to the AES in matlab. The Matlab code is then run to get the output file using Matlab.

6.1 ENCRYPTION AND DECRYPTION OF LENA IMAGE

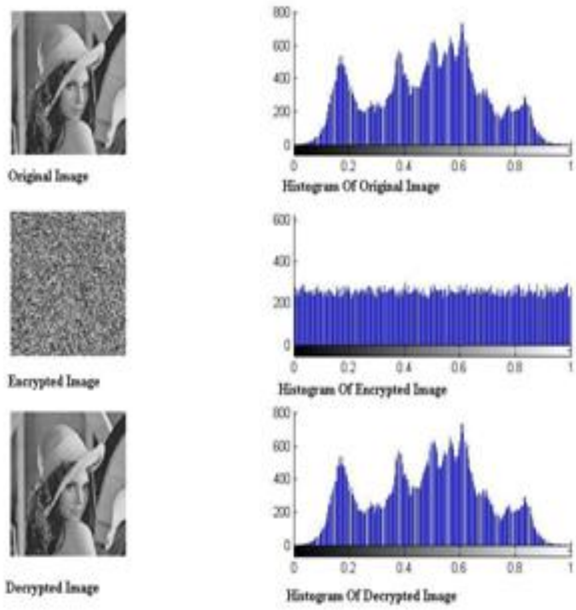


Fig 11: Encrypted & Decrypted image of single Bitplane

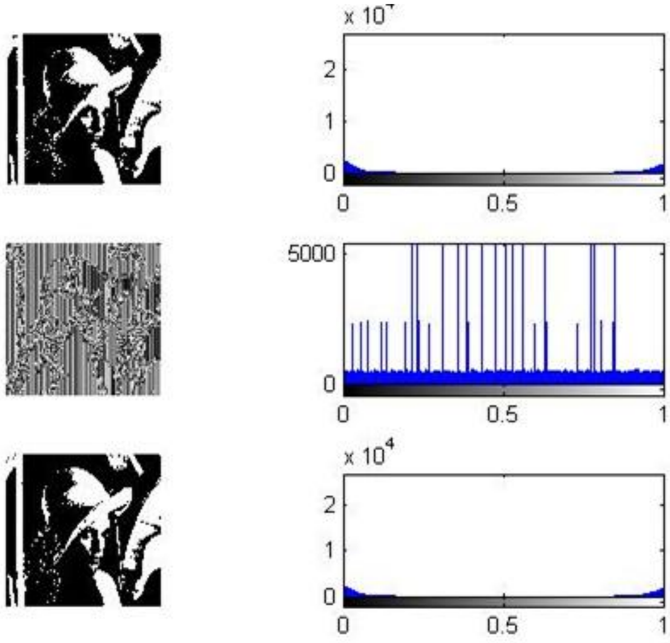


Fig 12: Encrypted & Decrypted image of MSB Bitplane

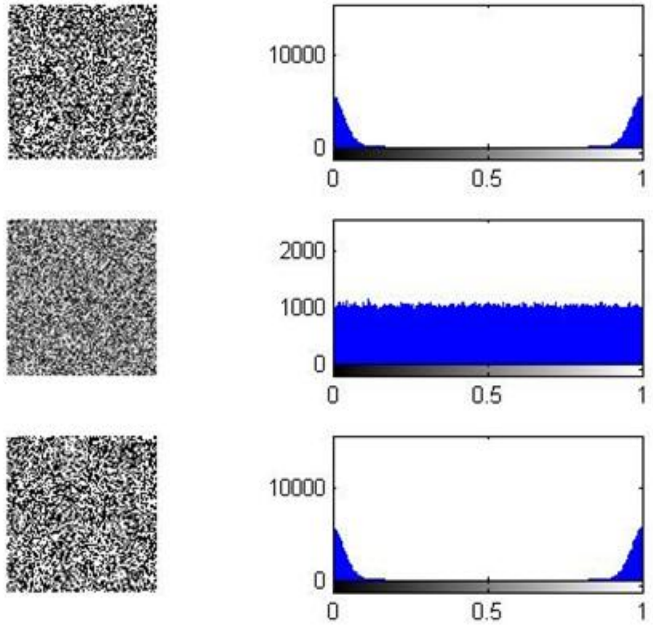


Fig 13: Encrypted & Decrypted image of LSB Bitplane

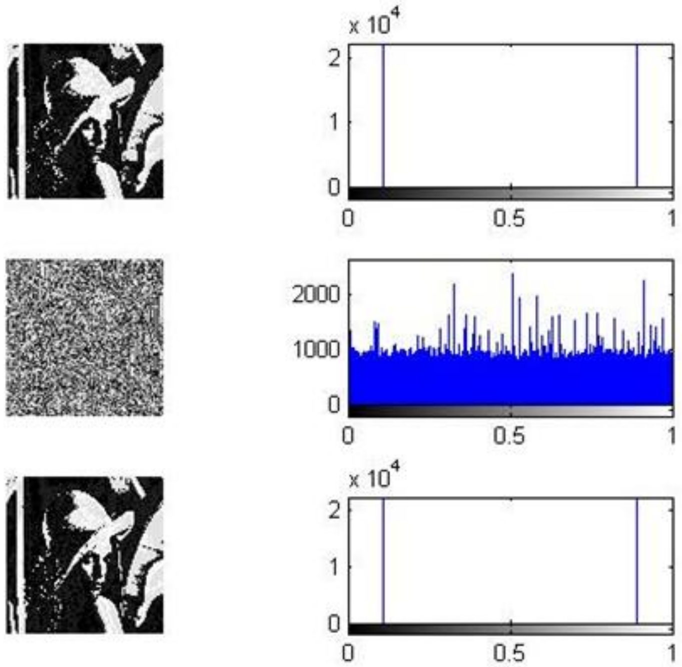
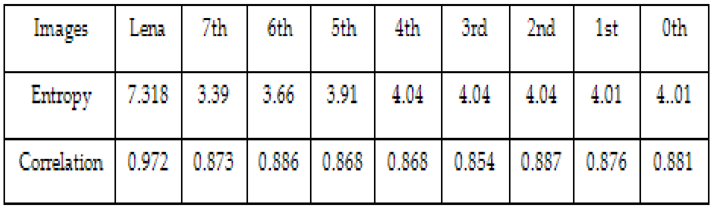


Fig 14: Encrypted & Decrypted image of combination of 5^{th} and 8^{th} Bitplane

6.2 RESULTS OF STATISCAL ANALYSIS



Images	Lena	7th	6th	5th	4th	3rd	2nd	1st	0th
Entropy	7.318	3.39	3.66	3.91	4.04	4.04	4.04	4.01	4..01
Correlation	0.972	0.873	0.886	0.868	0.868	0.854	0.887	0.876	0.881

Table 1: Statistical Analysis

The table above shows the value of entropy and correlation of lena and its bitplanes. Entropy of original is almost two times the bitplanes; correlation for lena is higher than bitplanes.

6.3 CONCLUSION

- We have proposed selective bitplane encryption to secure image transmission in mobile environments where no compression is involved.
- Two types of cipher text only attacks show clearly that encryption of the MSB bitplane only is not secure enough.

However, selectively encrypting two bit planes is sufficient if sever alienation of the image data is acceptable, whereas the encryption of four bit planes provides high confidentiality.

6.4 FUTURE SCOPE

- Used in low power mobile environments, where there is less overhead cost and there is a need for encryption.
- Extended to color images.

References

[1] Cryptography and Network security by William stallings Pearson Education.

[2] S. Thomas, D. Anthony, T. Berson and G. Gong, “The W7 Stream Cipher Algorithm”.

[3] J. Daemen and V. Rijmen, AES submission document on Rijndael, Version 2, September 1999. (http:// csrc.nist. gov/ Crypto Toolkit/ aes/ rijndael/ Rijndael.pdf)

[4] I. Agi and L. Gong. An empirical study of secure MPEG video transmissions. In ISOC Symposium on Network and Distributed Systems Security, San Diego,California, 1996.

[5] A. M. Alattar, G. I. Al-Regib, and S. A. Al-Semari. Improved selective encryption techniques for secure transmission of MPEG video bit-streams. In Proceedings of the 1999 IEEE International Conference on Image Processing (ICIP’99). IEEE Signal Processing Society, 1999.

[6] H. Cheng and X. Li. On the application of image decomposition to image compression and encryption. In P. Horster, editor, Communications and Multimedia Security II, IFIP TC6/TC11 Second Joint Working Conference on Communications and Multimedia Security, CMS ’96, pages 116–127, Essen, Germany, Sept. 1996. Chapman & Hall.

[7] H. Cheng and X. Li. Partial encryption of compressed images and videos. IEEE Transactions on Signal Processing, 48(8):2439–2451, 2000.

[8] J. Daemen and V. Rijmen. The Design of Rijndael: AES - he advanced encryption standard. Springer Verlag, 2002

	Ms. Naazneen M. G Working as a Lecturer at HKBK College of Engineering, Bangalore, India. Having 2 years of Teaching Experience. Completed M. Tech from BVBCET in "DIGITAL ELECTRONICS". Published more than 05 papers in various National conferences. Area of interest are Networking, VLSI Design, and Image Processing.
	Mrs. Sufia Banu Working as Lecturer at HKBK College of Engineering, Bangalore, India. Having 5 years of Teaching Experience. Pursuing M.Tech in "VLSI DESIGN & EMBEDDED SYSTEMS" from REVA College of Engineering and Technology, Bangalore, India. Published more than 07 papers in various National, International conferences & International Journals. Areas of research interests include VLSI, Networking, Embedded, Network security & Cloud Computing.
	Mrs. Zahira Tabassum Working as Assistant Professor at HKBK College of Engineering, Bangalore, India. Having 12 years of Teaching Experience. Completed M.Tech from UVCE in "POWER ELECTRONICS". Published more than 05 papers in various National conferences. Area of interest are Embedded Systems, VLSI Design, and Image Processing.

	Ms. Khamer Fathima Working as Lecturer at HKBK College of Engineering, Bangalore, India. Having 2 years of Teaching Experience. Completed BE in Electronics & Communication & M.Tech in "VLSI DESIGN & EMBEDDED SYSTEMS" Published more than 05 papers in various National & International conferences. Areas of research interests include. Areas of research interests include Networking, Embedded, VLSI, Network security.
	Ms. Arshiya Shariff N. Working as Lecturer at HKBK College of Engineering, Bangalore, India. Having 1 years of Teaching Experience. Completed BE in Electronics & Communication. Published more than 05 papers in various National, International conferences & International Journals. Areas of research interests include Networking, Embedded, VLSI, Network security.