Comparison between the application of DES on bitmap and JPEG images

Doaa H. Salem [a], A.Y. Bilal [a] and M. Fouad [b]
[a] *Computer Dept., International Telecommunication Institute (N.T.I)*
[b] *Communication Dept, Faculty of Eng., Zagazig University, Egypt*

The need for the encryption of the image data is becoming increasingly important as the Internet and Multimedia systems grow in size and popularity. This paper presents a comparison between the application of data encryption standard (DES) as a strong encryption algorithm that takes long time to be cracked on two different kinds of images, bitmap and JPEG (joint photographic experts group) images. It shows the results of encryption on both kinds of images, determines the best one for DES application to achieve a perfect hiding of image details, and determine the advantages and disadvantages of each case.

إن النمو السريع لتكنولوجيا الاتصالات قد جعل العديد من التطبيقات مثل تطبيقات الإنترنت و نظم الوسائط المتعددة (multimedia) والتطبيقات العسكرية تحتاج للدخول فى عالم الاتصالات المرئية ،والتي تتطلب قدر عالي من السرية. وحيث أن نقل الصور عبر شبكات الحاسب سواء المحلية أو العالمية (خاصة الإنترنت)،يجعلها عرضة للمهاجمة من اى شخص دخيل غير مصرح له بالاطلاع عليها سواء بقراءتها أو تغييرها بطريقة غير مسموح بها،فانه من المهم استخدام آلية التشفير لاخفاء كل معالم الصورة والحصول على صورة مبهمة تماما،وهذا يشمل الصور التي تمس الأمن القومي أو ألا بحاث المصنفة وغيرها. وفى هذا البحث يتم عمل مقارنة بين تطبيق نظام تشفير البيانات القياسي (DES) الذي يعتبر من أقوى أنظمة التشفير المتماثل واشهرها على نوعين معروفين من الصور، أولهما من نوع (BITMAP) والتي تعتبر الاختيار الأمثل للصور ذات التدرج الحاد في الألوان مثل الصور المرسومة (painted)، والثاني من نوع (JPEG) والذي يعتبر من اشهر الطرق المستخدمة في ضغط الصورة.و يتم عرض نتائج التشفير على كلا النوعين ،وتحديد العيوب و المميزات فى كلتا الحالتين تم تحديد أفضلهما عند تطبيق نظام التشفير (DES) وذلك لاخفاء معالم الصورة بكفاءة عالية والحصول على صورة مبهمة تماما.

Keywords: DES algorithm, Image encryption, Bitmap, JPEG

1. Introduction

As the telecommunication technologies grow rapidly, many applications such as multimedia applications and military applications needs to enter the era of visual communications, especially visual cryptography. Transferring special images through network (especially Internet) makes them vulnerable to eavesdropping, so it is important to employ encryption mechanism to hide all the details of the image.

There are many methods that were proposed for image encryption. Prashant, Rsiddharth and Rajeev kumer [1] presented an algorithm for image encryption which is delivered across the web, it depends on amalgamating two concepts-molecular genetics and image patterning.

Maniccam and Bourbakis [2] proposed a method, which performs both lossless compression and encryption of binary, and grayscale images based on SCAN patterns generated by the SCAN methodology. The drawback of this methodology is that compression-encryption takes longer time and for only gray scale images.

This paper investigates the application of Data Encryption Standard (DES)[3,4] as popular encryption scheme on two kinds of images. The Bitmap [5] image which are the best choice for representing subtle gradations of shades and color such as screen shots or simple painted images, and the JPEG [6,7] image which is the best for continuous tone images such as photographs. In each case, DES is applied to the image data bit stream (i.e. does not include the image header). DES is applied on a Bitmap image by dividing it into 8-bytes blocks and specifying a scan path along which the encryption algorithm is performed. In the case of JPEG image, the bits of the compressed image are rearranged by decompressing the file and dividing it into 8-bytes blocks and specifying a scan path along which the encryption algorithm is performed.

Also it makes comparison between both cases, investigates the encryption result for efficiency of hiding the entire voluminous data body of an image, and determines the advantages and disadvantages of each case.

This paper is organized as follows, section 2 provides a background of using DES to encrypt the image, section 3 provides the encryption of bitmap image, section 4 provides the encryption of JPEG image, section 5 tests the results, section 6 provides the conclusion of the work.

2. Image encryption by DES

As with any encryption scheme, there are two inputs to the encryption function, the plane text to be encrypted and the encryption key. In this case, the original image data bit stream (not including the image header is divided into 64-bits blocks (i.e. 8 bytes blocks).

The first 64-bits block is entered as plane text to the encryption function of DES, the second input is the 64-bit encryption key which is divided into two sub keys. Then it followed by the next 64-bit block, and so on with the scan path shown in fig. 1 (i.e. from left to right and top to the bottom) until finish the image data stream.

In the decryption process, the encrypted image is also divided into 64-bits blocks from top to bottom. The first 64-bits block is also entered to DES decryption function and the same encryption key is used to decrypt the image, but the application of sub keys is reversed. Then it followed by the next 64-bits block, and so on with the same scan path was taken to encrypt the original image as shown in fig. 2.

3. Encryption of a bitmap image

The encryption of a bitmap image is performed in similar way to the scheme mentioned in the previous section. By studying the bitmap file format shown in fig. 2 all the parts of the header file are determined to know the star of bitmap pixels or bitmap bits array, which differ in format depending on the bitmap type (4-8-16,24 bit bitmap image). The bytes of bitmap bits array may be also

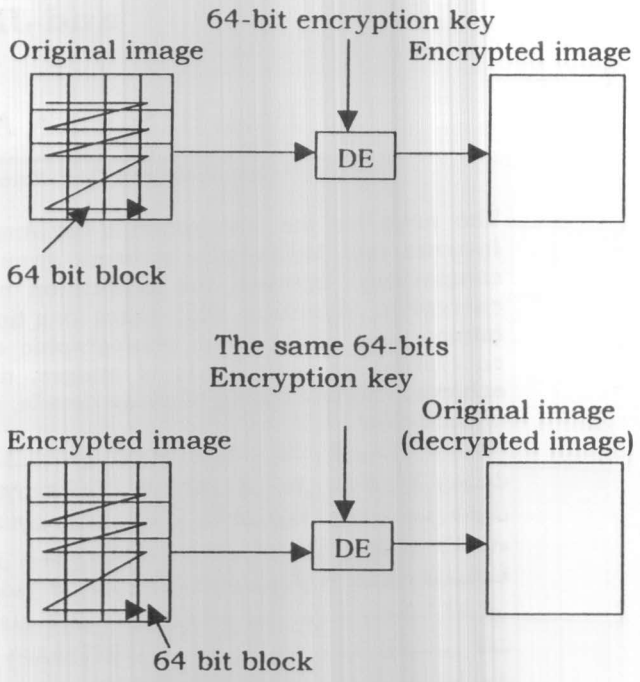

Fig.1. Image encryption by DES and the scan path used.

compressed and stored in raw order from left to right with each row representing one scan line of the image.

After then the bitmap array is entered to DES encryption function, as mentioned previously in section 2. The structure of a bitmap file format and the beginning of encryption process is determined in fig. 2.

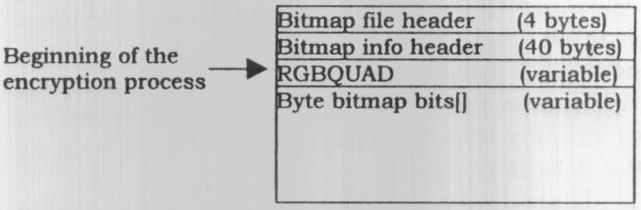

Fig. 2. Bitmap file format.

4. JPEG image encryption:

JPEG (joint photographic experts group) is compression standard for continuous tone images, grayscale and color image. It includes two basic compression methods, each with various modes of operation "lossy compression" and "losless compression", we

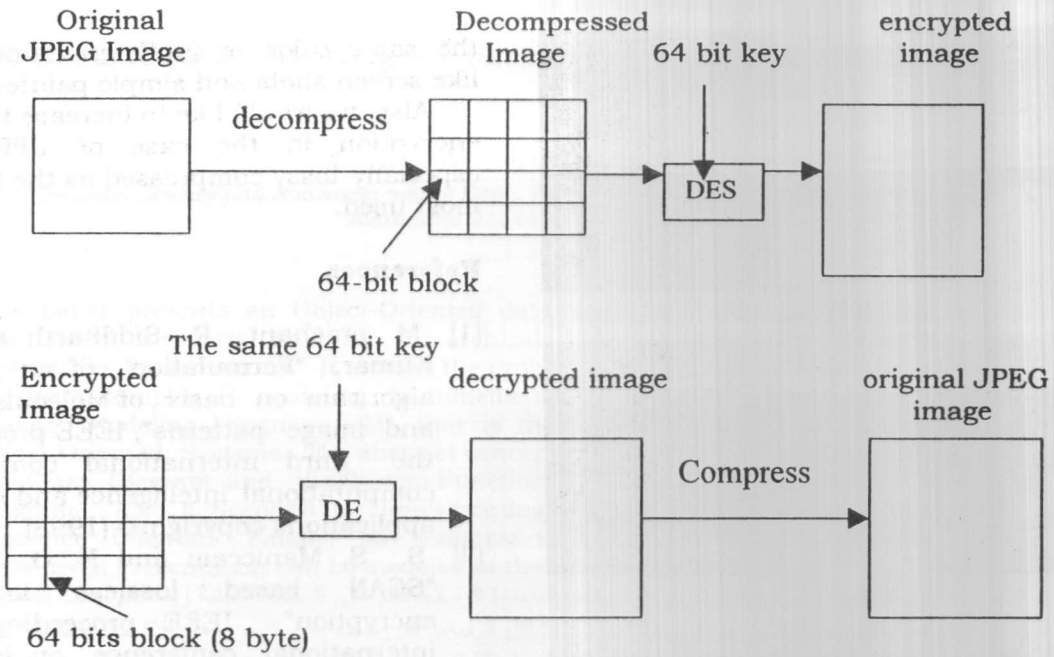

Fig. 3. Encryption of JPEG image.

are concerned with the first as it is the facility that is most used.

The DES encryption algorithm is applied on JPEG image after decompressing the image as shown in fig. 3. Then, the JPEG file format of decompressed image is studied and the header file is determined to know the star of JPEG bits array, on which the encryption is performed with the same scheme in section 2.

Then the encrypted image is compressed to get the encrypted JPEG image. In the decryption process, DES is applied to the encrypted image which is saved in a buffer (before compression) on which the decryption is performed with the same scheme in section 2 and then compress the file to get the original JPEG image as shown in fig. 3.

5. Results

The method that was used for applying DES on both Bitmap and JPEG images was implemented in software using C++. Fig. 4-a shows a continuous tone color JPEG image and its corresponding encrypted JPEG image, fig. 4-b shows a JPEG image that has large area of single color or subtle gradations in color. Fig 5-a shows a (8 bits/pixels) bitmap images with many different colors (continuous tone image) and its corresponding encrypted Bitmap image, while fig. 5-b. shows a (8 bits/pixels) bitmap images with large area of a single color and its corresponding encrypted bitmap image.

6. Conclusions

This paper is concluded by making a comparison between the application of DES on bitmap and JPEG image.

The comparison shows that joint image compression and encryption by DES is achieving very efficient results in hiding all the details of a continuous tone color image, where compression can facilitate encryption due to zero redundancy. In addition to using DES gives our work a good security due to its strength against attacking. But in the case of an image that has a large area of a single color, the results are little efficient.

For a bitmap image, the results of encryption are inefficient in the case of an image that has a large area of a single color or subtle gradations in the color, and quite efficient results in the case of a continuous tone image. However in this case, the encryption process is fast in comparing to the case of a JPEG image, where encryption needs more

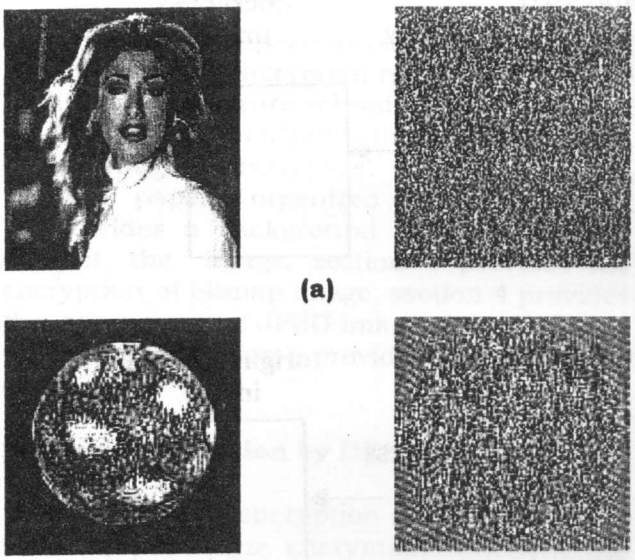

Fig. 4. JPEG color image and its corresponding encrypted JPEG image.

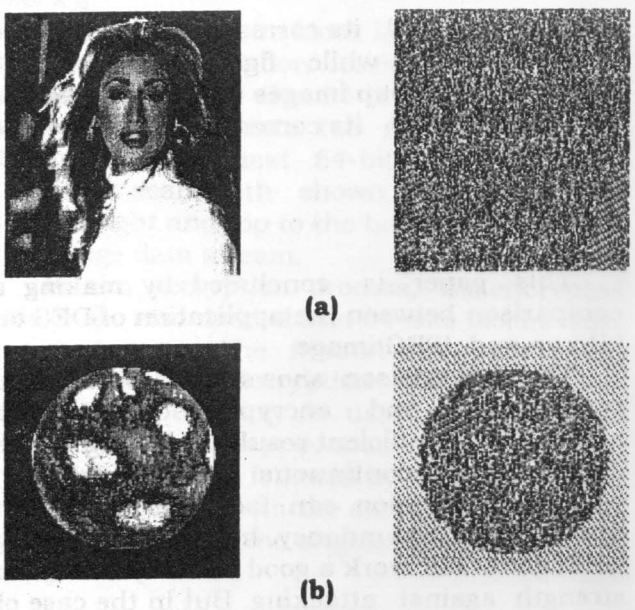

Fig. 5. BMP image and its corresponding encrypted BMP image.

computational cost due to the compression and decompression of the image, and this make the process is very slow.

In the future research, we would like to determine how to improve results of Encryption in case of Bitmap images, especially the images that have a large area of the same color or subtle gradations in colors like screen shots and simple painted images.

Also we would like to increase the speed of encryption in the case of JPEG images, especially lossy compressed as the facility that most used.

References

[1] M prashant, R Siddharth and Rajeev Kumar, "Formulation of an Encryption algorithm on basis of Molecular Genetics and image patterns", IEEE proceedings of the third international conference on computational intelligence and multimedia applications copyright© (1998).

[2] S. S. Maniccam and N. G. Bourbakis, "SCAN based lossless image and encryption", IEEE proceedings of the international conference on information intelligence and systems (1999).

[3] William Stallings, "cryptography and network security: principles and practice", second edition, by Prentice Hall, Upper Saddle River, New Jersey (1999).

[4] Carl E. Landwehr, Member, IEEE, and David M.Goldschlag, "Security Issues In Networks With Internet Security", Proceedings of The IEEE, Vol. 85 (12), December (1997).

[5] Alan Watt and Fabio Policarpo, "The computer image", published by Windcrest© /McGraw-Hill (1998).

[6] Gregory K.wallace, "The JPEG still picture compression standard", for publication in IEEE Transactions on Consumer Electronics, submitted in December (1991).

[7] Xiaolin Wu and Peter W.Moo, "Joint image/Video compression and Encryption Via high –order Conditional Entropy Coding of Wavelet Coefficients", proceedings the IEEE International Conference on Multimedia Computing and Systems, Vol. 2 (1998).

Received December 12, 2000
Accepted May 13, 2001