Image Encryption using Simplified Data Encryption Standard (S-DES)

Sanjay Kumar
Department ofComputerScience Engineering
Sobhasaria Engineering College,
Sikar, India

Sandeep Srivastava
Department ofComputerScience Engineering
Sobhasaria Engineering College,
Sikar, India

ABSTRACT

In this paper a number of image encryption algorithms based on chaotic maps has been proposed. Images are routinely used in diverse areas such as medical, military, science, engineering, art, entertainment, advertising, education as well as training. The fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Most of the available encryption algorithms are used for text data. However, due to large data size and real time requirement, the algorithms that are appropriate for textual data may not be suitable for multimedia data. Some cryptographic algorithms such as RSA, DES and AES are not sufficient for image encryption. We try to implement Image encryption using S-DES (Simplified Data Encryption Standard). In preceding work, most researchers used to make a image using a key and then encrypt the chaotic image using the same key, but in this paper first make a chaotic map of the image using S-DES. Then use that chaotic image as a key for encrypting the image using S-DES. Thus in this paper select the key when encrypt the image and use a chaotic image as a key not any other text. Thus the encryption speed is some faster in this implementation as compare to previous work. S-DES is the reduced algorithm of DES. DES uses a well-known block cipher; it adopts Fiestel structure to iterate. The key Quantities achieve 56 bits, using the only key in an encryption is not safe obviously. Therefore a new approach has been proposed named as S-DES, which also adopts Fiestel structure. Combining the chaotic map with S-DES system can enhance the security of system by using the characteristic of sensibility of original value and randomness in chaotic map. Thus the encryption speed is fast in this implementation as compare to previous work.

Keywords

Image, encryption , DES, S-DES, Chaotic map.

1. INTRODUCTION

Many digital services require consistent security in storage and transmission of digital images. Due to the quick growth of the Internet in the world, nowadays, the safety of digital images has turn into more necessary and much involved attention. In order to fulfill the security requirements of digital images, many image encryption approaches have been used [1]. Encryption algorithms of digital images are further important and should be used to aggravate enemy attacks from illegal access. Therefore, an encryption/decryption scheme can be developed if the secret parameters are chosen as keys [1]. Encryption is the secure method for data transmission. There are different encryption systems to encrypt and decrypt image data. In totaling to cryptography, chaotic image transformation technique are receiving appreciably more complex and have widely used. The chaotic image transformation techniques are best complement for encryption that allow a client to make some transformation in the image, and then the image is totally diffracted, so nobody could see that what information could be shown through that image[2].

1.1 Symmetric Key Algorithm

There are two primary types of symmetric algorithms:

(a) Block Cipher
(b) Stream Cipher

A block cipher is used to encrypt a text to produce a cipher text, which transforms a fixed length of block data size into same length block of cipher text in which a secret key and algorithm are applied to the block of data. Data Encryption Standard (DES), Triple-DES, IDEA, Simplifed-DES and RC2 are examples of symmetric block cipher [3]. The symmetric key algorithms employ a solitary key for encryption and decryption process.

1.2 Simplified-Data Encryption Standard (S-DES)

Simplified-Data Encryption Standard (S-DES) is a reduced adaptation of the Data Encryption Standard (DES) algorithm. It was designed as a test block cipher for learning about modern cryptanalytic techniques such as linear cryptanalysis, differential cryptanalysis and linear-differential cryptanalysis. It is a variation of basic DES. In Simplified-DES, the same key is used for encryption and decryption in fig1.1.

1.3 Advantages of S-DES

1. It is simpler than Data Encryption Standard.
2. It takes smaller block of plaintext and use small key in encryption than DES.
3. Its execution speed is faster than DES

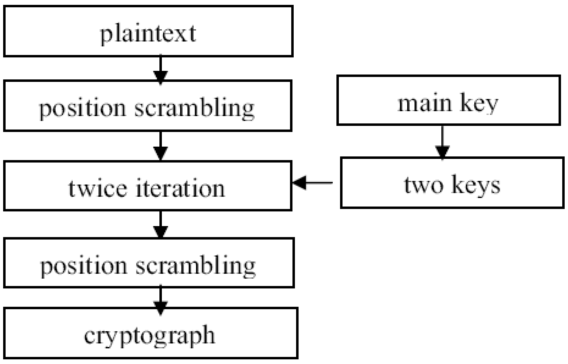


Fig.1. S-DES Structure

المنـــارة للاستشارات
www.manaraa.com

1.4 Limitations of S-DES

1. The key size is low in this algorithm.
2. Due to low key size, the security of S-DES algorithm is reduced.
3. If we use lots of data such as an image, then that algorithm can't satisfy the encryption requirement.

1.5 Chaotic Map

Chaos is a phenomenon that occurs in nonlinear definable systems responsive to initial situation and has a pseudo-random behavior. An imperative attribute that has caused this occurrence to take into thought for much cryptographic system is being definable in spite of its pseudo-random performance. Various cryptographic algorithms based on chaos theory are obtainable till now and some of them are one way or another employed in ways that are competent of image encryption addition to text encryption [4]. Image encryptions have to have particular skin such as suitable speed for enormous image data ciphering. The chaos is a procedure of exact pseudo-random series produced by nonlinear dynamics system. It's non- periodic, non-astringe and responsive to the unique price. Logistic map is a characteristic chaotic map and its look is shown as equation

$$Yn + 1 = bYn(1 - Yn) \qquad \text{Eq.(1)\textbackslash}$$

Where *Yn* Є [0, 1], when the worth of limitation *b* is between (3.569, 4), the system has the chaotic properties, and then the sequence generated by Logistic map is random and dependent on initial value. It can realize the position scramble of S-DES structure by collating the series of the chaotic map [5]. Working on the series can create the sufficient large keys, and it achieves encryption each time. It is obvious that combining the chaotic map with the S-DES encryption organization can enhance the randomness, and also increase the key quantity of system further.

KEY ENCRYPTION ALGORITHMS

A cryptographic system consists of the following:

● A plaintext message space M: a set of strings over some alphabet

● A cipher text message space C: a set of possible cipher text messages

● An encryption key space K: a set of probable encryption keys, and a decryption key space K1: a set of probable decryption keys

● A well-organized key age group algorithm G: N⟼K K1

● An efficient encryption algorithm E: M K⟼C

● An efficient decryption algorithm D: C K1⟼M.

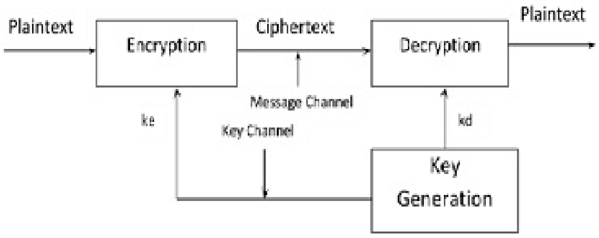


Fig.2. Crypto-system

Secret-key Cryptosystem: ke = kd Key Channel: e.g., Courier

Public-key Cryptosystem: ke ≠ kd Key Channel: e.g. Directory

Cryptosystems use secret keys as well as public keys.

In a secret-key cryptosystems encryption and decryption use the same key. The principal who encrypts a message must share the encryption key with the principal who will be receiving and decrypting the encrypted message.

In a Public-key cryptosystem, encryption and decryption use different keys; for every key keЄK, there exists kdЄK1, the two keys are different and match each other; the encryption key ke needn't be kept secret, and the principal who is the owner of ke can decrypt a cipher text encrypted under ke using the matching private key kd.

2. LITERATURE REVIEW

Conventional encryption algorithm (e.g. DES) has many disadvantage, such as the association complexity, the covered key singleness and the encryption pace slowly, and it is difficult to promise the encryption obligation of the picture that has plenty of data. The pixel's main attitude in lone picture can be unclear finally via encrypting, in arrange to appreciate the aspire of encryption.

According to [1] with the safety obligation development of the picture on the network, some characteristic image encryption method can't meet the stress of encryption, such as Arnold cat map and Hilbert alteration. S-DES organization can encrypt the input binary flow of image, but the fixed scheme structure and few keys will stationary convey some risk. However, the sympathy of first price that Logistic mixed-up map can be well sensible to the association of S-DES, which makes S-DES have improved accidental and key number. A dual image encryption algorithm based on S-DES and Logistic map is prospected. Through Matlab imitation research, the key amount will reach 1017 and the encryption speed of one depiction doesn't exceed one second. Compare to customary methods, it has some qualities such as easy to appreciate, rapid encryption velocity, large keys and compassion to initial value.

3. PURPOSED WORK
DES ALGORITHMS

The DES is a **block cipher** in which mail are alienated into data blocks of a permanent span and each block is treated as one message either in *M* or in *C*. In the DES, we have *M* = *C* = {0, 1}64 and *K* = {0, 1}56 ; that is, the DES encryption and decryption algorithms take as contribution of a 64-bit plain text or secret message text message and a 56-bit key, and output a 64-bit cipher text or plain text message [7].

The operation of the DES can be described in the following three steps:

1. Apply a fixed "initial permutation" IP to the input block. We can write this initial permutation as (L0, R0)← IP (Input Block) Eq. 2

   Here L0 and R0 are called "(left, right)-half blocks", each is a 32-bit block. Notice that IP is a fixed function (i.e., is not parameterized by the input key) and is publicly known, therefore this initial permutation has no apparent cryptographic significance.

www.manaraa.com

2. .Iterate the following 16 rounds of operations (for i=1, 2,……..,16)

$$L_i \leftarrow R_i - 1 \qquad \text{Eq.2}$$

$$R_i \leftarrow L_i - 1 \oplus f(R_i - 1, k_i) \qquad \text{Eq.3}$$

Here ki is called "round key" which is a 48-bit substring of the 56-bit input key, f is called "S-Box function" ("S" for replacement, we will give a brief account on this purpose later and is a substitution cipher). This process facial appearance exchange two semi block, that is, the left half block contribution to a around is the right half block production from the preceding around. The swapping operation is a simple transposition cipher, which aim to achieve a big degree of "message diffusion", essentially the mixing property modeled by Shannon. From our conversation we can see that this step of DES is a mixture of a substitution code and a transposition cipher.

3. The consequence from around 16, (L16, R16), is effort to the opposite of IP to cancel the result of the initial variation. The manufacture from this step is the output of the DES algorithm. We can write this final step as:

Output Block ← IP-1 (R16, L16) Eq.4

These three steps are shared by the encryption and the decryption algorithms, with the only difference in that, if the nearby key by one algorithm are k1, k2, …, k16, after that persons used by the extra algorithm should be k16, k15, …., k1. This way of position nearby keys is called "key schedule", and can be denoted by

$$(k'1, k'2, \dots\dots\dots\, k'16) = (k16\ , k15, \dots\dots\dots\dots .k1) \quad \text{Eq.5}$$

The Kernel functionality of the DES

The kernel part of the DES is inside the "S-box purpose" *f*. This is anywhere the DES realizes a chance and non-linear distribution of plaintext messages over the cipher text message space.

In the *i*-th round, $f(R_{i-1}, k_i)$ does the following two sub – operations:

i. Add the round key k_i, via bitwise XOR, to the half block R_{i-1}; this provides the randomness needed in message distribution;

ii. Substitute the result if (i) under a fixed permutation which consists of eight "substitution boxes" (S-boxes), each S-box is a non-linear permutation function; this provides the non – linearity needed in message distribution.

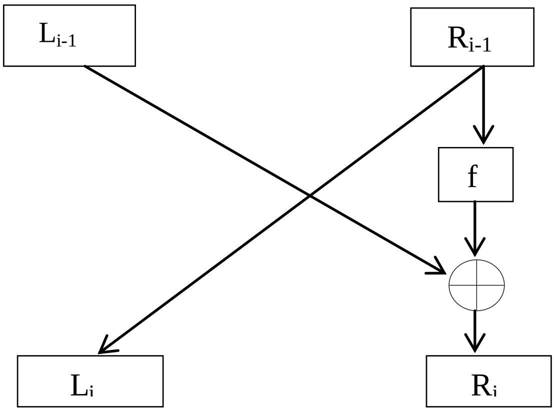


Fig. 3 Fiestel Structure

The non – linearity of S-boxes is very important to the security of the DES. We notice that the general case of the substitution cipher is nonlinear while the shift cipher and the affine cipher are linear sub cases. These linear sub – cases not only drastically reduce the size of the key space from that of the general case, but also render the resulting cipher text vulnerable to a **differential cryptanalysis** (DC) technique. DC attacks a cipher by exploiting the linear difference between two plaintext messages and that between two cipher text message. An interesting features of the DES is that the S-boxes in function $f(R_{i-1}, k_i)$ need not be invertible. Encryption and decryption working for arbitrary $f(R_{i-1}, k_i)$. This feature saves for the hardware realization of the DES.

4. RESULTS

The 10 bit key is used to make 2 different blocks of 8 bit sub keys where each block is used in a particular iteration. Let us denote the 10 bit key as KEY, the 8 bit sub keys as K1 and K2. The key-schedule used to generate the sub keys is denote as Ks. Figure 3 illustrates the calculation of K1 and K2 given KEY. KEY is subject to a first permutation, Permuted Choice 1 which is determined by the following table:

Table 1 PC-1

9	7	3	8	0
2	6	5	1	4

The table has been divided into two parts. The upper part determines the bits of C0 and the underneath part determines the bits of D0 .The bits of KEY are number from 0 to 9. Thus, the bits of C0 are bits 9, 7, 3… of KEY and the bits of D0 are bits 2, 6, 5… of KEY. A solitary left transfer is then executing on both C0 and D0. The effect of a single left shift of C0 and D0 is C1 and D1. To form K1, D1 is concatenated to C1 (with the most significant bit of C1 as the most significant bit of K1, and the most important bit of D1 following the least important bit of C1) and then subjected to a variation, Permuted Choice 2 which is resolute by the following table:

Table 2 PC-2

3	1	7	5	0	6	4	2

Table 3 E-BIT SELECTION TABLE

3	0	1	2	1	2	3	0

المنارة للاستشارات
www.manaraa.com

Thus, the first three bits of E(R) are bits 3, 0, 1 of R.

The 8 bit E(R) is then XORed with the 8 bit sub key K. The sub key K1 is used for round 1 and K2 is used for round 2. The result of the XORing operation is then split into two blocks, the first four bits from the most significant bit being B1 and the remaining bits being B2. B1 and B2 are then applied to S0 and S1 respectively.

	S_1 **Column Number**			
Row No.	0	1	2	3
0	0	3	1	2
1	3	2	0	1
2	1	0	3	2
3	2	1	3	0

S0 and S1 are S-Boxes which take in a 4 bit input and yield a 2 bit output.

We take S0 as an example to illustrate how the output block is determined. S0 takes the first bit and the last bit of the 4-bit block and used them to represent in base 2 a number in the range of 0 to 3. For example, for a block of bits 1101, 11 are obtained and are subsequently converted to 3. This is used to determine the row, in this case, row 3. The middle 2 bits is used to represent in base 2 a number in the range of 0 to 3. This is used to determine the column. In the case of our example block, the two bits in the middle represents column 2. From S0 above, a number from row 3 column 2 is selected, thus yielding the number 2, which in binary is written as 10. The result of S0 and S1 are concatenated to form a four bit block which is then applied to a permutation, P. This function is defined by the following table:

Table 4 P
1 0 3 2

Result of P will be the 4 bits returned by the function f.

Color Histogram

In this proposed approach we are using only first iteration of the chaotic image of original image of lena, and this chaotic image treated as the key for encryption of the original image of lena. Original image of lena and chaotic image of first iteration of the unique image are shown as below:

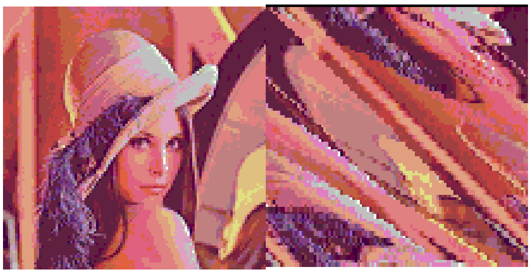
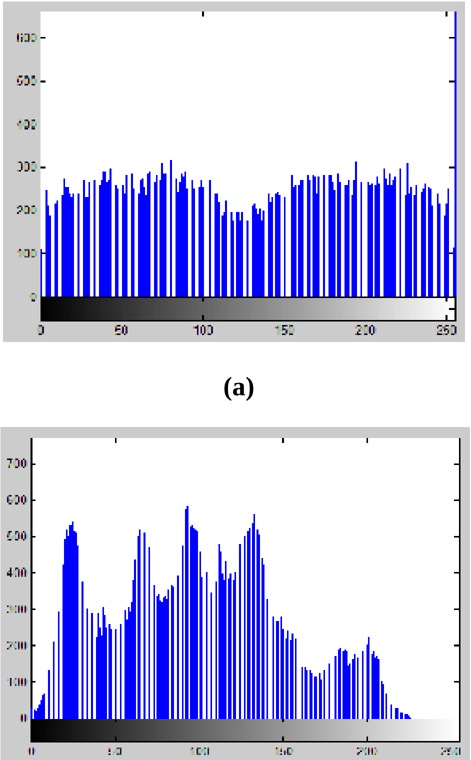


Fig.4.1 Main Image Fig-4.2 First Iteration of Arnold cat-map of main image



(a)

(b)

(a) Is histogram of the red, green and blue channels of the lena image in fig 4.1 (b)) are the histogram of the red, green and blue channels of the encrypted image of lena (Fig. 4.2)

After getting the chaotic image of the original image we need to make the binary image of the chaotic image, this binary conversion of the chaotic image will be treated as the key for S-DES to encrypt the original image.

	S_0 **Column Number**			
Row No.	0	1	2	3
0	1	0	2	3
1	3	1	0	2
2	2	0	3	1
3	1	3	2	0

Encryption

We are using S-DES (Simplified Data Encryption Standard) for encrypting the original image, where we use the chaotic image of the original image as a key. Since S-DES gives fixed system structure and few keys, therefore it takes less time than DES. But fixed system structure and few keys make some risks in encryption of an image that’s why we use chaotic image as a key in the encryption. Chaotic map make large random and key quantities and it will make this encryption more secure and gives fast operation speed.

المنارة للاستشارات
www.manaraa.com

5. CONCLUSIONS

In this paper, a color image encryption scheme is proposed, which is based on S-DES using Chaotic map of the original image. The transformation modeled by the Chaotic map and then found a chaotic image of the original image, that chaotic image is then used for encryption of the original image. Thus the resulted encrypted image shows the randomness of the algorithm. The use of S-DES algorithm increases the confusion of the encrypted image. Indeed, all performance analysis proves the security robustness of the proposed algorithm.

6. REFERENCES

[1] Ahmad, Musheer, Chanki Gupta, and Ankit Varshney. "Digital image encryption based on chaotic map for secure transmission." In Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International, pp. 292-295. IEEE, 2009.

[2] Salleh, M., Ibrahim, S., & Isnin, I. F. (2003, May). Enhanced chaotic image encryption algorithm based on Baker's map. In Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on (Vol. 2, pp. II-508). IEEE.

[3] Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). A new chaotic algorithm for image encryption. Chaos, Solitons & Fractals, 29(2), 393-399.

[4] Mao, Y., Chen, G., & Lian, S. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. International Journal of Bifurcation and Chaos, 14(10), 3613-3624.

[5] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08), 2129-2151.

[6] Wong, Kwok-Wo, Bernie Sin-Hung Kwok, and Wing-Shing Law. "A fast image encryption scheme based on chaotic standard map." Physics Letters A 372, no. 15 (2008): 2645-2652., 2007.

www.manaraa.com