International Journal of Modern Engineering Research (IJMER)

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-955-959 ISSN: 2249-6645

A Study of Binary Image Encryption Using Partial Image Encryption Technique

Parameshachari B D[1], Dr. K M S Soyjaudah[2]

*(Department of Electronics & Communication Engg., JSS Academy of Technical Education, Avenue Droopnath Ramphul, Bonne Terre,Vacoas, Mauritius)

** (Department of Electrical & Electronic Engineering, University of Mauritius, Reduit, Mauritius)

ABSTRACT

Chung and Chang proposed an encryption scheme for binary images based on two-dimensional run-encoding (2DRE) and scan patterns. In this paper, we indicate that their scheme is still not secure and efficient enough. Hence, an improvement scheme is proposed. There are two contributions in the proposed improvement scheme using partial image encryption techniques. One is to scrambling the pixel position and other second is by using SCAN mapping method. Hence, the improvements on encryption time, compression ratio and security are possible.

Keywords: **image security, mapping, partial encryption, SCAN, scrambling,**

I. INTRODUCTION

With the rapid advance of the computer network, large-sized information such as digital images can be easily transmitted. Therefore, the security of digital images has become an important issue. The traditional cryptology techniques are well defined for the security of textual data, but these techniques are not directly suitable to deal with digital media such as images, audio and video. The main reason is that the size of image data is much greater than the size of textual data. It is necessary to design a low complexity encryption/decryption method according to the properties of images. Hence, many schemes have been proposed especially for binary image encryption (Bourbakis, 1986; Bourbakis, 1992; Chang and Liu, 1994 and Chung and Chang, 1998).

In (Chung and Chang, 1998) Chung and Chang proposed an encryption scheme with higher security for binary images. In their scheme, different scan patterns are placed at the same level in the quadtree structure and then two-dimensional run-encoding (2DRE) is used to compress the encrypted images. Therefore, their scheme has higher security and a better compression ratio than previous research. However, in Chung-Chang's scheme, there are three problems worthy to discuss further.

Time-consuming

Since encryption is prior to compression, the data to be encrypted is still large. Hence, encryption is still more time-consuming. If compression is performed before encryption, the smaller size speeds up the encryption performance.

Compression ratio

When a binary image is encrypted using scan patterns, the more massed the same bits in the binary image, the better the compression ratio. If the scan patterns are uniformly random, the black bits or white bits will not mass and the result after encryption should not be suitable to be compressed. It implies that if the black bits or white bits don't mass after encrypting, the compression ratio will be decreased. Obviously, it is not a good method to encrypt before compression. On the contrary, if compression operation is priori to encryptions, it is possible to further increase compression ratio.

Security

The total number of black and white bits in the plainimage is the same as that in the cipherimage after scan patterns. This condition may disclose some important information. Especially, if a block contains all black or white bits, the result of scan patterns will also be all black or white bits in the cipherimage. This implies that if a cryptanalyst takes a cipherimage with many blocks that contain all black (white) bits, the cryptanalyst will know that those blocks are all black (white) bits in the plainimage. Hence, the cryptanalyst may infer the partial image from those redundancies and use it to break the cipherimage. Furthermore, since cryptanalysis relies on exploiting redundancies in the plainimage, compressing an image before encryption can reduce these redundancies.

In this paper, we propose an improvement scheme for Chung-Chang's scheme to address the problems mentioned above. First, exchange the sequence of compression and encryption. The data redundancy decreases after compression and encryption is then a time-saver process compared with Chung-Chang's. Simultaneously, higher compression ratio of the original image is possible because of the property of high similarity among adjacent pixels that exists in most natural images.

The remainder of the paper is organized as follows. In Section 2, we briefly introduce 2DRE and Chung-Chang's scheme. The proposed improvement scheme is illustrated in Section 3. In Section 4, the experimental results are shown. In Section 5 gives the applications. Finally conclusion is presented in section 6.

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-955-959 ISSN: 2249-6645

II. RELATED WORK

A. *Two-Dimensional Run-Encoding (2DRE)*

The main concept of 2DRE is counting how many times the same bits successively repeat according to scan order. Thus, we record the first bit of scan order and then save the successively repeated counts according to scan order. This process should be recursively and repeatedly done for the other bits until the end of the image is reached. For example, we have the following bit string:

0000000000000000
1111000000001111
0000011111100000
1111111111111111

The result of 2DRE according to the row scan order is shown as follows:

0 16 4 8 4 5 6 5 16

The first position is the initial bit and the others are the counting results. “0" and “1" are interleaving in the string; that is, we have 16 “0", 4, “1", 8, “0" and so on. We need 5 bits to represent each value, because the maximum value in the compressed string is 16. Hence, the total bits of the compressed string is 45 (9×5). Since the original size is 64 bits, the compression ratio is 1.42 (64/45).

There is no doubt that the 2DRE scheme is a good tool to compress binary data, however, a good compression ratio cannot be guaranteed simultaneously. In the following, we show the downside of the 2DRE:

1100011000111000
1111000011110001
0000011111000011
0000000000000000

The compressed result of the above example is as follows:

1 2 3 2 3 3 3 4 4 4 3 1 5 5 4 2 16

The total bits of the compressed string are then 85 (17×5), which obviously does not achieve the expectation of the compression.

Fortunately, the property of high similarity among adjacent pixels exists in most natural images, so we can directly utilize the 2DRE technique to compress the natural binary image and the compression ratio is still good.

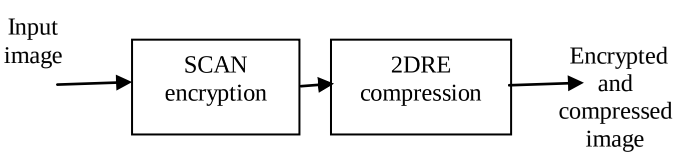
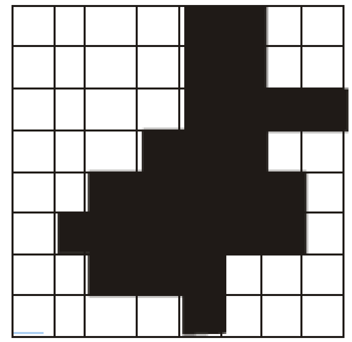
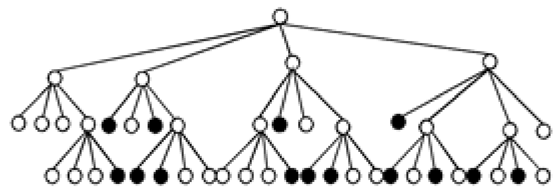


Fig 1: Chung-Chang’s Encryption Scheme.



(a)



(b)

Fig 2: (a) 23x23 binary image (b) the corresponding quadtree

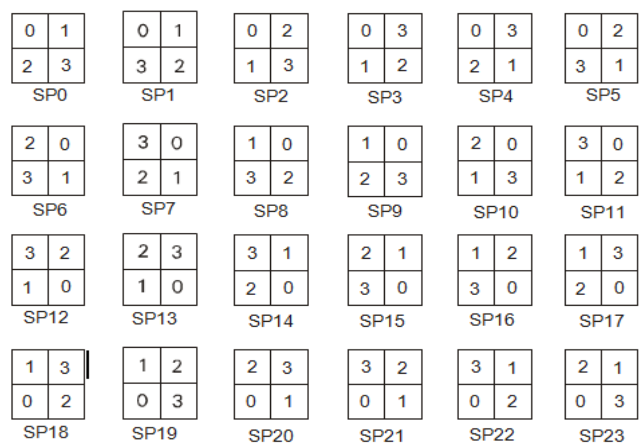


Fig 3: Scan Patterns

The main concept of Chung-Chang’s scheme (Chung and Chang, 1998) is shown in Fig. 1. In their scheme, they first use a quadtree to represent a binary image and put different scan patterns at the same level in the scan quadtree structure as encryption. Fig. 2(a) presents a binary image and Fig. 2(b) illustrates the corresponding quadtree hierarchical decomposition. Each block in Fig. 2(a) is represented by one bit of a binary image. The quadtree scheme recursively divides the original image into four uniform parts. Please refer to (Chang and Liu, 1994) for details relating to the quadtree scheme.

The quadtree is then encrypted according to the 24 scan patterns originally defined in (Chung and Chang, 1998) and shown in Fig. 3. SCAN language is used to produce the scan rules shown in Fig. 4(a), where S, Li and SPi are respectively defined as the start symbol, the set of different scan patterns at

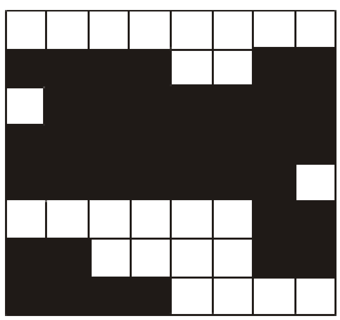
www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-955-959 ISSN: 2249-6645

the i^{th} level in the scan quadtree and the i^{th} scan pattern. Interested readers may refer to (Bourbakis, 1986) for more details about SCAN language. Furthermore, the encrypted image can be displayed using the raster scanning method and the result is shown in Fig. 4(b).

The 2DRE technique is used to compress the result of the raster scanning. The size of the original image in Fig. 2(a) is 8×8=64 (bits). However, the result from 2DRE requires only 60 (bits), so the compression ratio is 64/60–1.067.

S → L1 L2 L3
L1 → SP9
L2 → SP19 SP17 SP19 SP22
L3 → SP20 SP12 SP10 SP 9 SP16 SP3 SP18 SP3 SP19 SP0 SP11 SP0 SP6 SP2 SP19 SP6

(a)

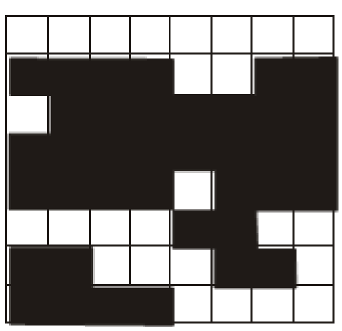


(b)

Fig 4: (a) SCAN language (b) the encryption result of Fig. 2(b)

S → L1 L2 L3
L1 → SP9
L2 → SP19 SP17 SP19 SP22
L3 → SP20 SP12 SP10 SP 9 SP16 SP3 SP18 SP3 SP19 SP0 SP11 SP0 SP6 SP2 SP19 SP6

(a)



(b)

Fig. 5: (a) New SCAN language (b) the encryption result of Fig. 5(b)

Unfortunately, as in 2DRE, the compression ratio cannot be guaranteed. Because the sequence of scan patterns is randomly produced, it is reasonable to arbitrarily change the sequence. Here we only change two scan patterns, using bold font, in Fig. 4(a) and the result is shown in Fig. 5(a). Fig. 5(b) is the result of encryption. The compression ratio then becomes 0.71 (64/90). On the other hand, if we directly utilize 2DRE for compression, it requires only 54 bits. The compression ratio is 1.185. This fact implies that the locality property of the natural image makes the direct use of 2DRE produce a compressed image with a high compression ratio.

III. The Proposed Improvement Scheme

The 2DRE technique is directly used to compress a binary image before encryption. Because high similarity among adjacent pixels exists in most natural images, we can apply this property to preserve a good compression ratio. A smaller size can also make the encryption process easier and thus reduce the time to encrypt. Three stages are involved in our scheme: (1) employing 2DRE to compress a binary image, (2) employing scan patterns and (3) mapping the image based on SCAN pattern. The Fig.6 illustrates the main concept of the proposed scheme.

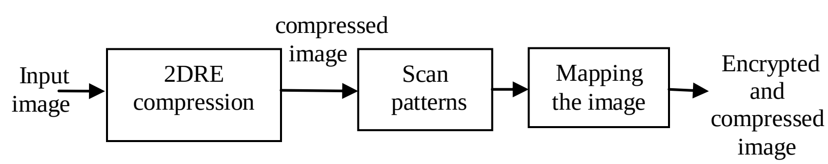


Fig 6: The proposed improvement scheme

Step 1: 2DRE

Because high similarity among adjacent pixels exists (i.e., local property) in most natural images, the compression ratio is still more effective than that after encryption. So the original image directly compressed by 2DRE in our scheme will produce a compressed image with a higher compression ratio compared to Chung-Chang's scheme.

Step 2: Scan patterns

The compressed binary image is treated as a bit string for simplicity, then each x bits are grouped together to form a block for encryption. For each block, we randomly select one scan pattern and change position according to the selected scan pattern. We can use a pseudo random generator to generate a sequence of selected scan patterns. Hence, there are at most x! kinds of scan patterns that can be selected, where the symbol "!" is defined as a factorial.

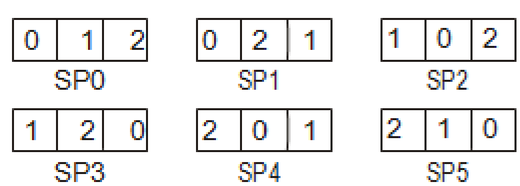


Fig 7. Scan patterns

www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-955-959 ISSN: 2249-6645

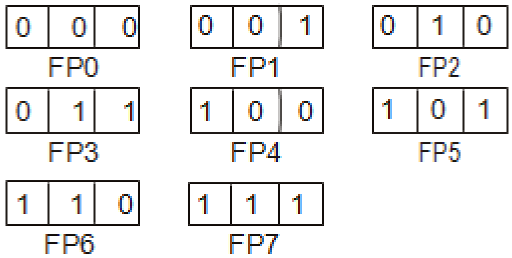


Fig 8: Scan mapping patterns

x can be flexible. Without loss of generality, the size of the compressed bit string is divisible by x.
Here we also take Fig. 2(a) according to the row scan order and use it as our example. The 2DRE compression result is as follows:

0 4 2 6 2 6 4 3 3 4 5 2 6 3 3 7 1 3

Because the maximum value is 7, 3 bits are necessary to represent each element. The following is the compressed bit string:

000 100 010 110 010 110 010 011 011 010 101 010 101 011 011 111 001 011

We can also take Fig. 3 as our scan patterns. To show our flexibility and to simplify, we use x=3 for our example. Hence, there are 3! =6 scan patterns shown in Fig. 7.
Because the size of the scan patterns is 3 bits, the above string should be grouped every
3 bits. Then for each group of 3 bits, we randomly choose a scan pattern to change bit position according to it. The scan pattern determines the substituted position. For example, for the tuple (0, 1, 2) and the selected pattern SP3 (1, 2, 0), the result is (2, 0, 1). If we take SP0 to SP5 recursively, the result of the scan patterns is as follows:

000 100 100 101 001 011 010 011 101 001 011 010 101 011 101 111 010 110

However, after the scan patterns, the total number of black and white bits in the plainimage is still the same as that in the cipherimage. This condition may disclose some important information. Just as in Chung-Chang's encryption scheme, if a block consists of all black or white bits, the result of the scan patterns will also be all black or white bits in the block.
Step 3: Scan mapping
To solve the mentioned above problem using the mapping image based on the scan pattern. Convert every pixel of the image to be encrypted into its equivalent 8-bit binary number. The concept of combination of nibble value of a pixel is used as a mapping function. Using the scan mapping method is increase strength of encryption techniques.

IV. EXPERIMENTAL RESULTS

We use two 256X256 binary image. Table 1 shows the results of the proposed scheme. The experimental results of Chung-Chang's scheme are shown in Table 2. In Table 2, since the compression ratio changes with the different sets of scan patterns in their scheme, the results are the average compression ratio of 5000 random sequences of scan patterns in the two original images. Comparing Table 1 and Table 2 shows that our scheme's compression ratio for the two binary images is better than that of Chung-Chang's scheme.

	Lena image	Step image
2DRE encrypted image	8067 bits	10345 bits
compression ratio	6.000	3.67345

Table 1: Experimental results of the proposed scheme

	Lena image	Step image
2DRE encrypted image	5000 random sequences	5000 random sequences
compression ratio	2.58318	1.742823

Table 2: chung-chang's scheme

V. APPLICATIONS

Digital multimedia content is becoming widely used over networks and public channels (cable, satellite, wireless networks, Internet, etc.), which is unsecured transmission media. Many applications that exploit these channels (pay-TV, videoconferences, medical imaging, etc.) need to rely on access control systems to protect their content. Standard cryptographic techniques can guarantee high level of security but at the cost of expensive implementation and important transmission delays. Partial encryption comes as an alternative that aims at providing sufficient security with an important gain in computational complexity and delays. This allows a variety of possible applications for partial encryption.

VI. CONCLUSIONS

In this paper, we enhance Chung-Chang's scheme and then a more efficient and secure encryption scheme is obtained. First, we exchange the sequence of compression and encryption to speed up encryption operation and to increase compression ratio simultaneously. Second, there are two added operations to enhance the security: Hence, the proposed scheme improves on Chung-Chang's scheme on the part of encryption time, compression ratio and security. One is to scrambling the pixel position and other second is by using SCAN mapping method. Hence, the proposed scheme improves on Chung-Chang's scheme on the part of encryption time, compression ratio and security. Furthermore, image size affects the speed of encryption; that is, the higher the compression, the better the efficiency. Because the property of natural pictures preserves a good compression ratio, our scheme achieves a good efficiency.

REFERENCES

[1] Bourbakis, N., 1986. A language for efficient accessing of a 2D array, *IEEE Workshop on LFA*, Singapore, pp: 52-58.

[2] Bourbakis, N. and C. Alexopoulos, 1992. Picture data encryption using SCAN patterns, *Pattern Recognition, 25*: 567-581.

[3] Chang, K.C. and J.L. Liu, 1994. An image encryption scheme based on quadtree compression scheme, *Proceedings of Internat. Comput. Symp*, Taiwan, pp: 230-237.

[4] Chung, K.L. and L.C. Chang, 1998. Large encrypting binary images with higher security, *Pattern Recognition Letters, 19*: 461-468.

[5] Stallings, W., 1999. *Cryptography and Network Security* (Prentice Hall International, Inc, 2nd Ed).

[6] Wu D.C. and W.H. Tsai, 2000. Spatial-domain image hiding using image differencing, *IEE Proceedings on Vision Image and Signal Processing*, 147: 29–37.

[7] Parameshachari B D, Chaitanyakumar M V:Image Security using SCAN Based Encryption Method,*42nd IETE Mid-term symposium on Telecom Paradigms - Indian Scenario*,April 2011, Bangalore, pp 115-118.