IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Implementation of Image Encryption and Compression using Chinese Reminder Theorem and Chaotic Logistic Maps

V.V.M Sireesha[1], Y.V.D. Pushpa Latha[2]

Student, Department of CSE, MVGR College of Engineering, Vizianagaram, India[1]

Assistant Professor, Department of CSE, MVGR College of Engineering, Vizianagaram, India[2]

Abstract: When the image data are regularly changed, existing image encryption algorithm is easy to be decrypted. In modern technology encryption of data is necessary to provide security when it is transmitted and stored in internet world. To employ this we are using different types of encryption algorithms such as AES, DES, and 3DES and also Blow Fish which are common. These encryption techniques does not provide more security when are used in real time encryption process. In this we use a new algorithm called Chinese Reminder Theorem along with compression which helps in encrypting the data and secure it from unauthorized access. Along with chaos based mapping, Chinese remainder theorem (CRT) which is used long with compression of an image along with Fibonacci series is also used. In order to improve the security of encryption algorithm, this paper proposes an image encryption algorithm based on chaotic mapping and Chinese remainder theorem. The encryption algorithm is divided into pixel scrambling and image diffusion. Firstly, the Chebyshev mapping is used to generate a chaotic sequence, which is used to scramble the image pixel bit value. Then, the pixel position is scrambled by formula. Finally, the scrambled image is substantially changed by the application of the Chinese Remainder Theorem with compression and Fibonacci series. Simulation results show that, compared with other typical encryption algorithm, the proposed encryption algorithm has better effect on the key sensitivity, histogram statistics, information entropy analysis and correlation analysis.

Keywords: Chebyshev Chaotic Mapping, Chinese Remainder Theorem, Fibonacci series, Compression, Pixel scrambling, Image diffusion.

1. INTRODUCTION

With the development of Internet, more multimedia information have been stored and transmitted. Having the characteristics of intuition and vividness, image transmissions hold a high proportion. Image encryption produces is a core technology of image security and is an effective means of protecting the image and is direct. For information hiding image encryption process is an indispensable technology at the same time. Text encryption is different from image encryption due to correlation. Almost all encryption techniques are symmetric key cryptosystems. Present research of encryption is based on these aspects: spatial domain, transforming domain, neural networks, based on chaotic, based on cellular automat and quantum code. These characters leads to change in pixel in plain image is not drastically change the cipher image. The solutions to overcome the problem is by using chaos theory and these includes different mapping techniques for pixel scrambling. Thus chaos is very sensitive to changes in initial values and produces some relevant effects as confusion and diffusion. The relationship between cryptosystems and chaos theory is very close. Chaotic maps produces chaotic sequences. Decryption is possible after encryption process. Reverse mapping is seen in case of decryption process. Rather than forward and sequences are reversed. Pixel wise shuffling is possible based on tent maps and row – column shuffling is used for diffusion in logistic maps. This is one of the mapping techniques in chaos theory and play an important role in diffusion process and reduces complexity and increases speed of an encryption. Confidentiality is seen in encryption process Chinese remainder theorem (CRT) which is based on number theory also used in compression of an image. Cryptographic primitives are constructed by CRT and also processing time will be increased.

2. RELATED WORK

In modern technology encryption of data is necessary to provide security when it is transmitted and stored in internet world.. To employ this we are using different types of encryption algorithms such as AES, DES, and 3DES and also Blow Fish which are common. These encryption techniques does not provide more security when are used in real time encryption process. Different approaches re carried out by the researchers in order to improve the performance and security of an image of RSA cryptosystems. Good level of security is provided by RSA system to protect data from

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

unauthorized access. Large data can be protected because to enhance the performance of cryptosystem of RSA. In RSA cryptosystems we use large data especially decryption key to know the brute force attack. Exponential operations are involved in encryption-decryption procedure. Many scholars and experts have studied onimage encryption, and presented a lot of encryption algorithms.K. Deergha Rao et al proposed a new secure cryptosystem based on the BB equation andchaos for image encryption and decryption. Cryptanalysis of the proposed cryptosystem was also provided [1]. AmneshGoel and Nidhi Chandra introduced a new image encryption method which first rearranges the pixels within image on basis of RGB values and then forward intervening image for encryption [2]. MrinalKanti Mandal et al proposed a high security image encryption technique using logistic map. The proposed image encryption algorithm was described in detail along with its security analysissuch as key space analysis, statistical analysis anddifferential analysis [3]. Discrete wavelettransform and Modified Chaotic Key-Based Algorithm were proposed to enhance the security of CKBA. The enhanced security of the proposedalgorithm was analyzed through cryptanalysis [4]. A permutation technique based on the resolution of the system of three independent Diophantinenequations was presented. From this permutation algorithm, an efficient chaos-based block cipher using a chaotic logistic map was proposed [5].HimanKhanzadiet al proposed an algorithm for image encryption using the random bit sequence generator and based on chaotic maps. Chaotic Logistic and Tent maps were used to generate required random bit sequences [6].

Proposed algorithms:

2.1. Chebyshev chaos mapping

Chebyshev sequence is a one-dimensional chaotic mapping and the iterative equation is simple and easy to realize [7]. The k order Chebyshev mapping expression is present as in Eq.
(1).

Xn+1=cos(k arccos(x) (1)

In this equation, the valid value of
Xnisbetween -1 and 1. When k>=2, the system
enters chaotic state.

2.2. Chinese remainder theorem

The Chinese remainder theorem is a kind of method to solve a set of linear congruencies, and it is an important theorem in number theory. The main contents are as follows. Assume that mm m□ are n mutualprime number integers, for any given n integers:

Assume that $m_1, m_2, \cdots m_n$ are n mutual prime number integers, for any given n integers: $a_1, a_2, \cdots a_n$ (n>=2), Eq. (2) has unique solution.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \quad (2)$$

The unique solution is shown as in Eq. (3).

$$x \equiv M_1 M_1^{-1} a_1 + M_2 M_2^{-1} a_2 + \cdots + M_n M_n^{-1} a_n \pmod{m} \quad (3)$$

In the formula, M_i^{-1} is the number of M_i inverse modulo m_i. At the same time, the formula meets $M_i\ M_i^{-1} \equiv 1 \pmod{m_i}$, i=1, 2…n. The m value meets $m=m_1 \times m_2 \times \ldots \times m_k$, $m=M_i m_i$, i=1, 2… n.

2.3. Fibonacci sequence

Fibonacci sequence is a group of regular integer values. The rule is shown as in Eq. (4).

$$F(n) = \begin{cases} 1 & n \le 2 \\ F(n-1) + F(n-2) & n > 2 \end{cases}$$

In the formula, F(n) represents Fibonacci Series value when the parameter is n.

2.4 Image compression

Image compression is a type of data compression applied to digital images, to reduce their cost for storage or transmission. Algorithms may take advantage of visual perception and the statistical properties of image data to provide superior results compared with generic compression methods.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Lossless image representation formats:
BMP (bitmap) is a bitmapped graphics format used internally by the Microsoft Windows graphics subsystem (GDI), and used commonly as a simple graphics file format on that platform. It is an uncompressed format.
PNG (Portable Network Graphics) (1996) is a bitmap image format that employs lossless data compression. PNG was created to both improve upon and replace the GIF format with an image file format that does not require a patent license to use. It uses the DEFLATE compression algorithm, that uses a combination of the LZ77 algorithm and Huffman coding. PNG supports palette based (with a palette defined in terms of the 24 bit RGB colors), greyscale and RGB images. PNG was designed for distribution of images on the internet not for professional graphics and as such other color spaces

Comparison with JPEG:
• JPEG has a big compressing ration, reducing the quality of the image, it is ideal for big images and photographs.

• PNG is a lossless compression algorithm, very good for images with big areas of one unique color, or with small variations of color.

• PNG is a better choice than JPEG for storing images that contain text, line art, or other images with sharp transitions that do not transform well into the frequency domain.

Comparison with TIFF:
• TIFF is a complicated format that incorporates an extremely wide range of options. While this makes it useful as a generic format for interchange between professional image editing applications, it makes supporting it in more general applications such as Web browsers difficult.

• The most common general-purpose lossless compression algorithm used with TIFF is LZW, which is inferior to PNG and until expiration in 2003 suffered from the same patent issues that GIF did. TIFF (Tagged Image File Format) (last review 1992) is a file format for mainly storing images, including photographs and line art. It is one of the most popular and flexible of the current public domain raster file formats. Originally created by the company Aldus, jointly with Microsoft, for use with PostScript printing, TIFF is a popular format for high color depth images, along with JPEG and PNG. TIFF format is widely supported by image-manipulation applications, and by scanning, faxing, word processing, optical character recognition, and other applications. Compression types include
• uncompressed
• PackBits - is a fast, simple compression scheme for run-length encoding.
• Lempel-Ziv-Welch (LZW)
• CCITT Fax 3 & 4 – protocol for sending fax documents across telephone lines.

3. PROPOSED SYSTEM

The Idea of the CMCRTCOMPRESSION-IEA Algorithm
The CMCRTCOMPRESSION -IEA algorithm is consists of two processes, image scrambling and image diffusion. Image scrambling includes bit value scrambling and pixel position scrambling. In the image diffusion stage, the Chinese remainder theorem and Fibonacci sequence are used to completely change the image pixel value.

3.1. Scrambling Bit value
A plain image can be used to indicate by a matrix M, which has h rows and w columns. Theheight of the plain image is h, and the width is w.Each element in the M is represented by an integerbetween 0 and255. Each pixel consists of 8 bitbytes, and pixel scrambling refers to change the 8bit value.

3.2 Pixel position scrambling
Through the above algorithm, pixel scrambling changes pixel values. However, pixel location information has not been changed, which brings hidden trouble to the safety of image data. It is necessary to change the position information ofpixel, so as to improve the effect of image dataencryption.

3.3. Image diffusion
Through change the value and location of each pixel, a certain effect of encryption has obtained. However, a considerable part of the plaintext information has not been hidden and the encryption effect is not ideal. In the CMCRT COMPRESSION-IEA algorithm, scrambling image is diffused by Chinese remainder theorem and Fibonacci sequence. Now, image is compressed using lossless compression so that the original image resolution will not be changed. It also reduces the cost of transmission and reduces the bandwidth for storage.

Copyright to IJARCCE

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

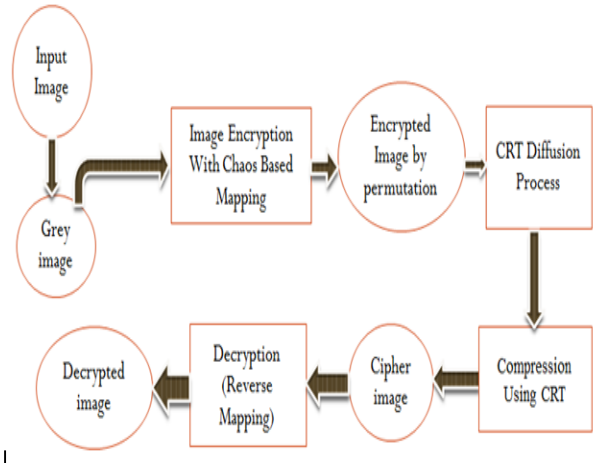


Fig.1Process state diagram

Now from the converted grayscale image we use Chebyshev sequence which is used for chaos based mappings are used and is a one- dimensional chaotic mapping and the iteration process takes place. CMCRTC-IEA algorithm used to encrypt the image. In this we should compress the key first for security purpose.Chinese remainder theorem (CRT) is a theorem of number theory and also remainders and also it is widely used for computing large integers.In this CRT is used for compression of an image.Two types of compression techniques used in this lossy compression and lossless compression.

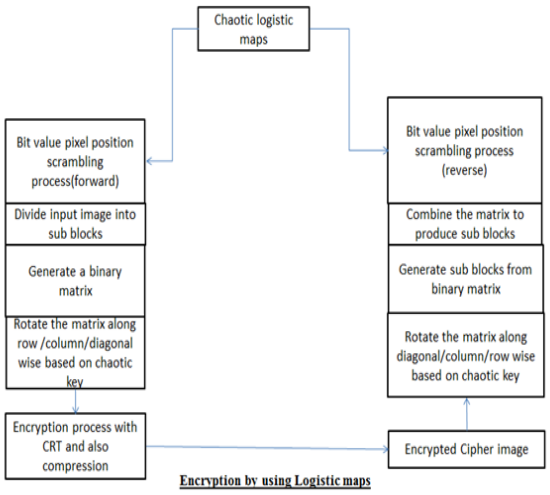


Fig 2 .Diffusion Process

With lossless compression every file which is presented that was originally in file remains same after compression.With lossy compression data will be changed after compression. These techniques reduces number of plain and cipher images.By using logistic maps from chaos theory which acts as a bit value scrambling, pixel position scrambling image and also diffusion process takes place along with Permutation process.By using complex matrix generated by a plain image diffusion process takes place. Along with diffusion compression by using CRT takes place. This will be having high correlation among pixel and high key space. In this chaos based techniques are used for pixel scrambling and positioning the image and is divided into sub blocks and also a binary matrix is generated .Now pixels re being shuffled by rotating the matrix long column and row wise and also diagonal wise.No useful information will not be leaked during this process and a cipher image will be created.This can achieved a very large key space and produce strong sensitivity and helps in more securing the data.Thus , by using reverse mapping techniques the cipher images will be decrypted.Thus the process of decryption takes place with reverse mapping techniques.

4. EXPERIMENTAL RESULTS AND ANALYSIS

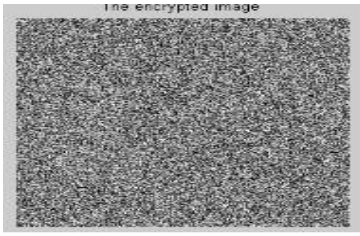
In the simulation process, vegetables is chosen to evaluate the algorithm performance. The experiment platform is shown as follows .TheSimulationsoftwareisMATLAB2010.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Fig 3 (a) Original Image



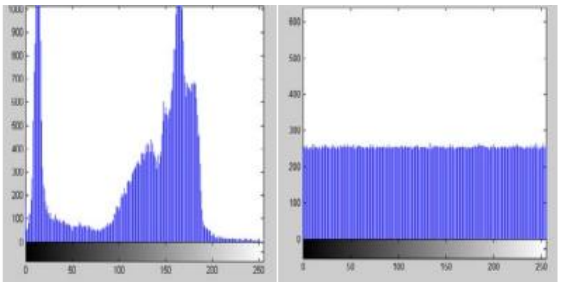
3 (b) Encrypted image

4.1. Sensitivity analysis of the key

Decryption is the inverse of the encryption process. In the internal pixel image scrambling, the key is set to k=4, x=0.123456. The original imageand encrypted image by the CMCRT COMPRESSION-IEA algorithm are contrasted as shown in Figure 1.When the decryption key and encryption key is the same, the right decryption image is got. When the decryption key is set to k=4.000001,x=0.1234561, decryption image is obtained). Inthe process of decryption, the decryption image and original image are different when key slightly changes. This shows that the CMCRT COMPRESSION -IEA algorithm is highly sensitive to the key.

4.2. Statistical characteristic analysis

The image gray histogram is a distribution map, which can reflect the distribution of pixel values. X-axis parameters are the gray values. And y-axis parameters are the number of the gray value. Plaintext and ciphertext image histogram are shown as Figure . It can be seen that the uneven pixel values distribution of original image is become uniform distribution by the CMCRTC-IEA algorithm. Figure shows that pixel value of the cipher image in the range of [0, 255] basicallypresent uniform distribution, the correlation of cipher text is greatly reduced. The cryptanalystcannot get any information about plaintext from the encrypted image histogram



(a)The plain image scatter diagram (b) The ciphered image scatter diagram
Fig 4.The Diagonal Direction Of The Scatter Diagram

The cryptanalystcannot get any information about plaintext from the encrypted image histogram. Therefore, theencrypted image can resist the attack of statistical characteristic analysis.

4.3. Information entropy analysis

Information entropy is one of the important indexes of sequence random properties. If the information entropy is bigger, the random sequence has better performance. The information entropy is expressed in Eq. (8).

$$H(S) = -\sum_{i=0} p(s_i) \log_2 p(s_i)$$

The cipher text information entropy of some images is shown in Table 1. And theseimages are encrypted by the CMCRT-IEAalgorithm. The cipher text information entropy ofimage is shown, which isencrypted by different encryption algorithms. Itcan be seen from the table that cipher text information entropy of the CMCRT-IEA

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

algorithmis closer to the ideal value 8 than literature [1] andliterature [3]. This shows that the CMCRT-IEAalgorithm can resist information entropy statisticalattack, and has better performance of encryption.

Table 1. Information entropy of ciphered vegetables image

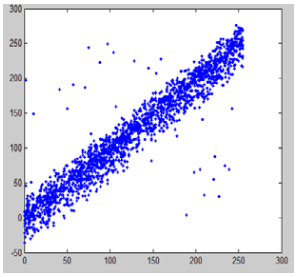
Encryption algorithm	Information entropy
Literature [1]	7.9932
Literature [3]	7.9946

4.4. Analysis of the correlation between adjacent pixels

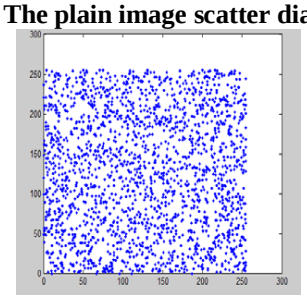
Because the plain image gray value is generally continuous, the correlation between adjacent pixels is high. For good encryption algorithm, the correlation between the adjacent pixels of cipher image should be lower .Correlation of adjacent pixels is done quantitative analysis.

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)D(y)}}$$

Among them, x and y said two adjacentpixel gray value. rxysaid correlation coefficient. E(x) and D(x) express expectation and variance onvariable x. In the horizontal, vertical and diagonaldirections, the 2000 gray values are randomlyselected to compare the correlation between pixels.In the diagonal direction, the correlation betweenadjacent pixels plaintext and cipher text is shown as below.



4 (a) The plain image scatter diagram



(b) The ciphered image scatter diagram

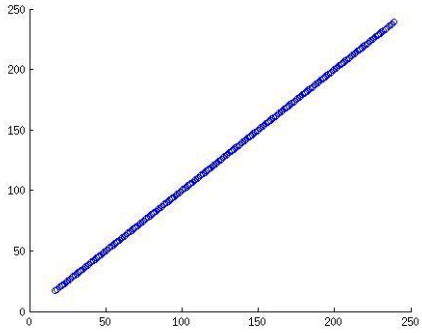


Figure 4. The diagonal direction of the scatter diagram

Compared with the literature [1] and [3], the results of operations are shown as Table 2. Itcan be seen that correlation between adjacentpixels of the original image is high, and the valueis close to 1. The correlation coefficient of the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

encrypted image is close to 0. This suggests thatthe correlation of the encrypted image is greatly reduced. Compared with encryption algorithms inLiterature [1] and Literature [3], the correlationcoefficient of the CMCRTC-IEA algorithm is the least. This shows that the CMCRTC-IEA algorithm has the better performance in the aspect of resist the correlation.

Table 2.The correlation coefficient between the plaintext and cipher text image

Direction	Plaintext image	CMCRT-IEA	Literature [1]	Literature [3]
Horizontal	0.9215	0.0129	0.0168	0.0150
Vertical	0.9538	0.0135	0.0153	0.0167
Diagonal	0.9032	0.0092	0.0129	0.0124

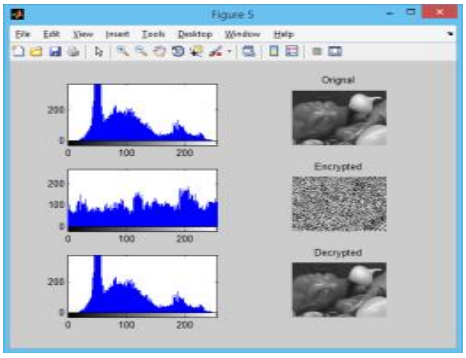


Fig 5.Final histogram

5. CONCLUSION

In order to improve the effect of image encryption algorithm, this paper has proposed an encryption algorithm of pixel level image based on chaotic mapping and Chinese remainder theorem. The image scrambling and diffusion image are combined in the algorithm. The Chebyshev chaotic mapping is introduced in the process of scrambling, and Chinese remainder theorem is introduced to diffuse image and later compression takes place which is lossless .The CMCRTC-IEA algorithm not only retains the merits of the "scrambling-diffusion" algorithm, but also overcomes the shortcomings of the plaintext attack in the existing algorithms and also reduces bandwidth and also storage is easy. Simulation experiment is carried out in the key sensitivity, statistical characteristics, information entropy and pixel correlation. The experiment results show that the proposed algorithm is stability and can resist correlation attack. Therefore, the algorithm is a secure image encryption algorithm and is worthy to be popularized.

REFERENCES

[1] J.Chen, J.Zhou,K.-W.Wong, A modified chaos-based joint compression and encryption scheme,IEEETrans.CircuitsSyst.II58(2)(2011)110–114.
[2] C.-C.Chang,T.-X.Yu, Cryptanalysis of an encryption scheme for binary images, PatternRecognit.Lett.23(14)(2002)1847–1852.
[3] D.Klinc,C.Hazay,A.Jagmohan,H.Krawczyk,T.Rabin, On compression of data encrypted with block ciphers, IEEETrans.Inf.Theory58 (11)(2012)6989–7001.
[4] V.Jagannathan, A.Mahadevan, R.Hariharan, S.Srinivasan, Number theory based image compression encryption and application to image multiplexing, in: Proceedings of IEEE International Conference on Signal Processing, Communications and Networking,2007, pp. 59–64.
[5] J.Yang, C.Chang, C.Lin, Residue number system oriented image encoding schemes, ImagingSci.J.58 (1)(2010)3–11.
[6] C. Li,K.-T.Lo, Optimal quantitative cryptanalysis of permutation- only multimedia ciphers against plaintext attacks, SignalProcess.91 (4) (2011)949–954.
[7] T.-H.Chen,C.-S.Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Inf.Sci. 180(9)(2010)1690–1701.
[8] S. Li, C. Li, K.-T. Lo, G. Chen, Cryptanalysis of an image encryption scheme, J. Electron. Imaging 15 (4) (2006) 043012.
[9] H.K.L. Chang, J.L. Liu, A linear quad tree compression scheme for image encryption, Signal Process. 10 (4) (1997) 279–290.
[10] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proceedings of the IEEE International. symposium on circuits and systems, Scottsdale, AZ, USA, 2002
[11] N.K. Pareek, Vinod Patidar, K.K. Sud, Discrete chaotic cryptography using external key, Phys. Lett. A 309 (2003) 75–82.
[12] N.K. Pareek, Vinod Patidar, K.K. Sud, Cryptography using multiple one-dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul. 10 (7) (2005) 715–723.
[13] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52
[14] Refregier, B Javidi, Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett. 20 (1995) 767–769.
[15] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption algorithm for image cryptosystems, J. Syst. Software 58 (2001) 83–91.
[16] N. Bourbakis, C. Alexopoulos, Picture data encryption using SCAN pattern, Pattern Recogn. 25 (1992) 567–581.