

Image Encryption using Modified 4 out of 8 code and chaotic map

Sunil Kumar K.M

Lecturer

Dept. of Telecommunication Engineering
KIT,Tiptur
Karnataka

Kiran

M.Tech

Dept. of E and C Engineering
Mce,Hassan
Karnataka

Anand U Hiremath

Lecturer

Dept. of Telecommunication Engineering
KIT,Tiptur
Karnataka

ABSTRACT

Recently, several image encryption schemes based on chaotic maps have been proposed. Most of them hinder the system performance, security, and suffer from the small key space problem. This paper presents a image encryption using modified 4 out of 8 code and chaotic map. Generally image encryption involves permutation and substitution network. Here permutation is done by using chaotic map and using modified 4 out of 8 code carrier image is generated with the help of alpha-numeric keywords and also special characters. Substitution done by performing XOR operation between permuted image and carrier image to get a encrypted image. Simulations have been carried out and the results demonstrate the superior security and high efficiency of the proposed scheme.

General Terms:

Information security, Image encryption

Keywords:

4 out of 8 code, Carrier image, Chaotic map

1. INTRODUCTION

Image is one of the most important information representation styles and is widely used in many applications like military communication, telemedicine, medical images, etc. Images are often exchanged between two parties over insecure networks. Therefore, the protection of image data from intercepting, copying, and destruction has become a hot problem studied by experts and researchers. Image encryption is the process of realigning the original image into an incomprehensible one that is non-recognizable in appearance, disorderly and unsystematic..

Zhi-liang Zhu [8] presented A chaos-based symmetric image encryption scheme using a bit-level permutation. Bit level permutation is not only changes the position of the pixel but also alters its value. Here image cryptosystem employing the Arnold cat map for bit-level permutation and the logistic map for diffusion. G.A.Sathish Kumar et.[2] all proposed A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD] utilizing duo chaos mapping applicability in wireless systems.The algorithm makes use of full chaotic property of logistic

map and reduces time complexity. The algorithm calculates the permuting address for row by bit xoring the adjacent pixel values of original image. Similarly, the algorithm calculates the permuting address for column by bit xoring the adjacent pixel values of original image.The diffusion is performed after scrambling and is based on two chaotic maps.Prasanna et. el [5] have presented an image encryption method with magnitude and phase manipulation using carrier images. Here they used the concept of carrier images and one dimensional Discrete Fourier Transform for encryption purpose and it deals with private key cryptosystem, works in the frequency domain. Ahmed A.abd El-Latif et.al have proposed a hybrid chaotic system and cyclic elliptic curve for image encryption and provides a external secret key of 256 bit and one generalized chaotic logistic map. using the cyclic elliptic curve to derive generated key stream are mixed with key sequences[1]. Panduranga H.T presented a novel image encryption using 4 out of 8 code. it is a unique 8 bit code in which each nibble is having 2 ones and two zeros to create a 36 different 8 bit number. We have 26 alphabets and 10 numerals to form 36 alphanumeric characters. These alphanumeric characters are assigned with unique codes of 4 out of 8 codes[3]. ZhiZhong et. al[9] proposed a novel double image encryption method utilizing double pixel scrambling technique and random fractional Fourier domain encoding. One of the two original images is encoded into the phase of a complex signal after being scrambled by one matrix, and the other original image encoded into its amplitude after being scrambled by another matrix. The complex signal is then encrypted into stationary white noise by utilizing double random phase encoding in fractional Fourier domain. By applying the correct keys with fractional orders, the random phase masks and the pixel scrambling operation, the two original images can be retrieved without cross-talk. Narendra K Pareek [4] proposed the image encryption scheme using a secret key of 144-bits. Here in the substitution process, image is divided into blocks and subsequently into color components. Each color components are modified by performing bit-wise operation which depends upon the secret key as well as few most significant bits of its previous and next color components. Analysis is done using entropy and other parameter.

2. BASICS OF 4 OUT 8 CODE

Here we are defining a new code called 4 out of 8 code. This code is of 8 bit length with 4 number of ones and 4 number of zeros and

we made one consideration that each nibble must have 2 number of ones and 2 number of zeros. In the below table we listed all 36 possible combinations of the 4 out of 8 code and each code is assigned to an alphanumeric character. Since 26 alphabets (capital letters or small letters) and 10 numerals forms to give 36 alphanumeric characters, this code is more suitable to assign a unique code to each alphanumeric character.

2.1 Modified 4 out 8 code

Modified 4 out of 8 code is 8 bit length with 4 number of ones and 4 number of zeros. Here we are not taking any consideration like each nibble must have 2 number of ones and 2 number of zeros. Here only consider that total number of ones in byte is four. According to modified 4 out of 8 code, we listed all 70 possible combinations of the 4 out of 8 code and each code is assigned to an alphanumeric character and also special character. Since 26 small letters i.e a to z, 26 capital letters i.e A to Z, 10 numerals and 8 special characters forms to give 70 alphanumeric and special characters, this code is more suitable to assign a unique code to each alphanumeric character and special characters. Generated 4 out of 8 code shown in Table 1.

3. CHAOTIC MAP

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behavior regarding complexity, chaotic properties cycle length, chaotic interval, periodic windows, etc., sensitivity to initial conditions and reaction to trajectory perturbations, etc., that influence the structure or behavior of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map and efficiency, it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to fulfill the security and efficiency requirements of a good cryptosystem.

For their mathematical simplicity there are two options: logistic map and tent map. The logistic map is represented by

$$X_{n+1} = rX_n(1 - X_n) \quad (1)$$

The logistic map chaotic signal used has primary values of $X_0 \in [0, 1]$ and $r \in [3.57, 4]$.

4. PROPOSED METHOD

Block diagram of Proposed method as shown in Figure 1. The proposed Block diagram consists of permutation and carrier image generation block. Initially input image of size $m \times n$ is applied to permutation block. Input image is permuted using chaotic map to produce permuted image.

4.1 Permutation using chaotic map

The detailed permutation procedure is described as follows:

Step 1: consider the input image of size $m \times n$.

Step 2: convert input image into one dimensional vector.

Step 3: based on initial key x_0 and using chaotic map Eq.1 with $r=3.9999$ generates chaotic sequence of the iteration of $m \times n$ and obtain chaotic sequences as

$X = x_1, x_2, x_3, \dots, x_{m \times n}$

Step 4: The chaotic sequences X is sorted in ascending order and

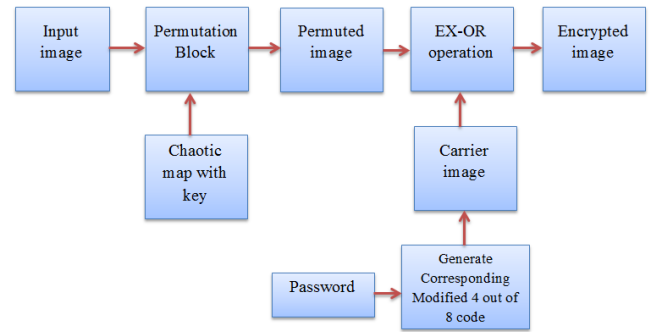


Fig. 1. Block diagram of proposed method

stores the index values into another variables index.

Step 5: According to the index values, one dimensional vector is permuted and converted back into matrix.

Step 6: Get permuted image.

4.2 Carrier image Generation

As we enter the different keywords, each keyword is taken and rearranged in a matrix form of size equal to the size of original image. If the length of the keyword is very small then the same keyword is repeated till the length is become equal to size of original image. By using look up table of the alphanumeric special character and modified 4 out of 8 code as shown in Table 1, a carrier image is created. Depending on the number of keywords number of carrier image is generated. different carrier images generated using different passwords as shown in Table 2.

Finally the permuted image and Carrier image generated from modified 4 out of 8 code undergo Ex-or operation to produce Encrypted image.

5. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

5.1 Statistical analysis

In the proposed encryption algorithm, the diffused image is randomly distributed. This is shown by a test on the histograms of the cipher-images in Section 5.1.1, the information entropy of the cipher-image in Section 5.1.2 the correlations of adjacent pixels in the plain-image and cipher image in Section 5.1.3, Analysis of differential attack in section 5.1.4.


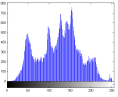
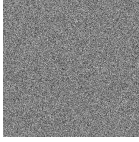
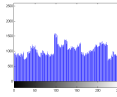

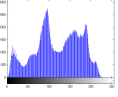
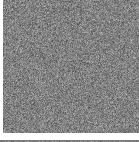
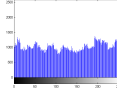

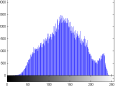
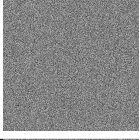
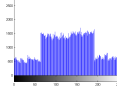
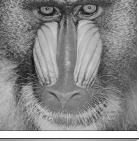
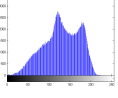
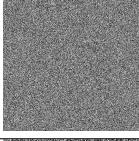
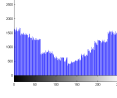

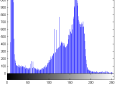
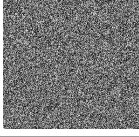
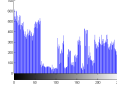
5.1.1 Histogram analysis. An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each gray scale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should not leak any information about the plain-text or the relationship between plain-text and cipher-text. Table 3 shows the histograms of plain-images and its ciphered images generated by the proposed scheme respectively. It's clear from that the histograms of the cipher-images are fairly uniform and significantly different from that of the plain image and hence do not provide any clue to employ statistical attack.

5.1.2 Information entropy analysis. In information theory, entropy is the most significant feature of disorder, or more precisely

Table 1. 70 possible combination of 4 out of 8 code along with alphanumeric and special character

Serail No.	Binary form	Hex Decimal form	Decimal form	Alphanumeric-special character
1	00001111	F	15	a
2	00010111	17	23	b
3	00011011	1B	27	c
4	00011101	1D	29	d
5	00011110	1E	30	e
6	00100111	27	39	f
7	00101011	2B	43	g
8	00101101	2D	45	h
9	00101110	2E	46	i
10	00110011	33	51	j
11	00110101	35	53	k
12	00110110	36	54	l
13	00111001	39	57	m
14	00111010	3A	58	n
15	00111100	3C	60	o
16	01000111	47	71	p
17	01001011	4B	75	q
18	01001101	4D	77	r
19	01001110	4E	78	s
20	01010011	53	83	t
21	01010101	55	85	u
22	01010110	56	86	v
23	01011001	59	89	w
24	01011010	5A	90	x
25	01011100	5C	92	y
26	01100011	63	99	z
27	01100101	65	101	A
28	01100110	66	102	B
29	01101001	69	105	C
30	01101010	6A	106	D
31	01101100	6C	108	E
32	01110001	71	113	F
33	01110010	72	114	G
34	01110100	74	116	H
35	01111000	78	120	I
36	10000111	87	135	J
37	10001011	8B	139	K
38	10001101	8D	141	L
39	10001110	8E	142	M
40	10010011	93	147	N
41	10010101	95	149	O
42	10010110	96	150	P
43	10011001	99	153	Q
44	10011010	9A	154	R
45	10011100	9C	156	S
46	10100011	A3	163	T
47	10100101	A5	165	U
48	10100110	A6	166	V
49	10101001	A9	169	W
50	10101010	AA	170	X
51	10101100	AC	172	Y
52	10110001	B1	177	Z
53	10110010	B2	178	0
54	10110100	B4	180	1
55	10111000	B8	184	2
56	11000011	C3	195	3
57	11000101	C5	197	4
58	11000110	C6	198	5
59	11001001	C9	201	6
60	11001010	CA	202	7
61	11001100	CC	204	8
62	11010001	D1	209	9
63	11010010	D2	210	!
64	11010100	D4	212	@
65	11011000	D8	216	#
66	11100001	E1	225	\$
67	11100010	E2	226	%
68	11100100	E4	228	^
69	11101000	E8	232	&
70	11110000	F0	240	*

Table 3. Resultant Encrypted Images and its histogram of proposed method

Input Image	Histogram	Encrypted Image	Histogram	password
				mysoreuniversity5732*\$%
				\$ELECTRONICS14576*!@\$%
				1789imageproce\$\$ing
				KIRAN\$\$UNIL14756
				KALPATARUINSTITUTION\$124

unpredictability. To calculate the entropy $H(X)$ of a source x , we have:

$$H(X) = \sum_{i=1}^n Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \quad (2)$$

where X denotes the test image, x_i denotes the i^{th} possible value in X , and $Pr(x_i)$ is the probability of $X = x_i$, that is, the probability of pulling a random pixel in X and its value is x_i . For a truly random source emitting $2N$ symbols, the entropy is $H(X) = N$. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be $H(X) = 8$. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security [6]. The entropies for plain image and ciphered images using various images are calculated in Table 4. Apparently, the proposed algorithm is much closer to the ideal situation. This means that information leakage in the encryption process is negligible and the cryptosystem is secure against entropy attack.

5.1.3 Analysis of correlation of adjacent pixels. For an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should produce the cipher image with sufficiently low correlation in the adjacent pixels. The visual testing of the correlation of adjacent pixels can be done by plotting the distribution of the adjacent pixels in the plain image and its corresponding cipher image. The correlation distribution of two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels of the plain image and the cipher image produced by the proposed scheme is shown in Table 5, respectively. It is clear that the strong correlation between adjacent pixels in plain image is greatly reduced in the

cipher image produced by the proposed scheme. To quantify and compare the correlations of adjacent pixels in the plain and cipher image, the following procedure is carried out. First, randomly select 1000 pairs of adjacent pixels in each direction from the plain image and its ciphered image. Then, calculate the correlation coefficient $r_{x,y}$ of each pair by using the following four formulas:

$$cov(x, y) = E(x - E(x))(y - E(y)) \quad (3)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N X_i \quad (4)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (X_i - E(X_i))^2 \quad (5)$$

where x and y are grayscale values of two adjacent pixels in the image and N denotes the total number of samples, $cov(x, y)$ is co-variance, $D(x)$ is variance, $E(x)$ is mean.

Fig. 2 shows Horizontal, vertical and diagonal directional pixel values of plain image and cipher image respectively.

5.1.4 Analysis of differential attack. A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain-image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change rate (NPCR) and Unified average chang-

Table 5. Correlation coefficients of two adjacent pixels in plain-image and ciphered-images of proposed method.

Image	Plain image			Encrypted Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9691	0.9841	0.9842	-0.0058	0.0017	0.0035
Peppers	0.9733	0.9764	0.9809	-0.0008	0.0001	0.0022
Babon	0.8652	0.7524	0.7567	-0.0017	-0.0018	0.0001
Cameraman	0.9333	0.9565	0.9564	-0.0516	0.0227	0.0262
Elaine	0.9738	0.9695	0.9697	0.0090	-0.0098	-0.0079

Table 2. Dfifferent carrier images with different passwords

Password	Carrier Image
mysoreuniversity5732*\$%	
\$ELECTRONICS14576*!@\$%	
1789imageproce\$\$ing\$%	
KALPATARUINSTITUTION\$124	

Table 4. Entropy

Input Images	size	Plain Image Entropy	Encrypted Image Entropy
Lena	512x512	7.4451	7.9774
Peppers	512x512	7.5937	7.9883
cameraman	256x256	6.971	7.7126
Babon	512x512	7.3583	7.9883
Elaine	512x512	7.5060	7.8639

ing intensity (UACI) [7]. The equation to calculate UACI is Eq. 6

$$UACI = \frac{1}{M * N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \times 100\% \quad (6)$$

Where, M stands for images width, N stands for images height, c1(i,j) means the gray-scale value of cipher-image in position (i,j), and c2(i,j) means the gray-scale value of the new cipher-image which is the encryption result of modified plain image that has just one different pixel to the original plain-image. NPCR can be calcu-

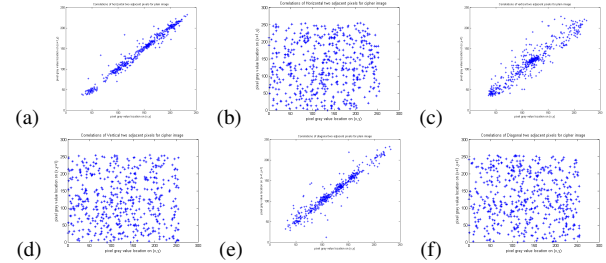


Fig. 2. Correlations of two adjacent pixels for lena image of size 512*512 (a) horizontal direction of the plain image, (b) horizontal direction of the cipher image, (c) vertical direction of the plain image, (d) vertical direction of the cipher image, (e) diagonal direction of the plain image, and (f) diagonal direction of the cipher image.

Table 6. NPCR and UACI of Proposed method

Image	NPCR(%)	UACI(%)
Lena	99.5724	27.8096
Peppers	99.6067	30.3366
cameraman	99.6063	34.1013
Babon	99.7311	32.0549
Elaine	99.5007	24.4800

lated by Eq. 7

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (7)$$

Where, M stands for images width, N stands for images height and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1 & \text{if } C1(i,j) \neq C2(i,j); \\ 0 & \text{if } C1(i,j) = C2(i,j). \end{cases}$$

When one bit of a pixels gray-scale value in the plain image is changed, then a new plain image is generated from the original one. Encrypt the two images with the same secret keys, then take cipher images into Eqs. 6 and 7 and results are shown in Table 6.

From the Table 6 results we can find that our algorithm is very sensitive to tiny changes in the plain image, even if there is only one bit difference between two plain images, the decrypted images will be completely different.

6. CONCLUSION

Image encryption using modified 4 out of 8 code and chaotic map is simple and effective. Here permutation is done by using chaotic map sequence and carrier image is generated using alpha-numeric special character keywords with the help of modified 4 out of 8 code table. By increasing number of carrier images in encryption

process to get a highly distorted image with respect to original image. Simulation results show that the NPCR, UACI and information entropy of the proposed schemes are better than existing method. All these results justify the superior security and computational efficiency of our cryptosystems.

7. REFERENCES

- [1] Xiamu Niue Ahmed A. Abd El-Latif. A hybrid chaotic system and cyclic elliptic curve for image encryption. *PInt. J. Electron. Commun. (AE)*, 2012.
- [2] V.Vivekanand G.A.Sathish Kumar, K.Bhoopathy Bagan. Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [iispd] utilizing duo chaos mapping applicability in wireless systems. *Procedia Computer Science*, 2011.
- [3] Naveenkumar S.K Panduranga H.T. A novel image encryption method using 4 out of 8 code. In *proc. CommV09*, 2009.
- [4] Narendra K Pareek. Design and analysis of a novel digital image encryption scheme.
- [5] Prasanna SRM. An image encryption method with magnitude and phase manipulation using carrier images. *IJCS*, page 132137.
- [6] Joseph P. Noonan Yue Wu. Shannon entropy based randomness measurement and test for image encryption. *Information Sciences*, pages 1–23, 2011.
- [7] Joseph P. Noonan Yue Wu and Sos Agaian. Npcr and uaci randomness tests for image encryption. *Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, November 2011.
- [8] Kwok-wo Wong Hai Yu Zhi-liang Zhu, Wei Zhang. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, 181:11711186, 2011.
- [9] ZhiZhong. Double image encryption using double pixel scrambling and random phase encoding. *Optics Communications*, 2012.