SECRET IMAGE TRANSMISSION WITH DYNAMIC CRYPTOGRAPHY

Prof. Vijay Karra[1], Prof. J B Jawale[2]
[1,2] Dept. of E&TC Engg. , AIT, Pune, Maharashtra, India.
Email: vkarra@aitpune.edu.in[1], jjawale@aitpune.edu.in[2]

Abstract

Nowadays, data encryption is important to maintain privacy. In the digital world, the security of digital images is becoming more essential because of digital products communications networks occur more and more frequently. We propose a technique in which the color table is used to generate a picture carrier, the carrier image is added to the original image. The encrypted image obtained is unclear and can't be seen. To make it even more secure model SCAN pattern is used to blend the pixels of the image. The resulting image is decrypted using the inverse of the scan pattern. Thus the carrier image and original image is obtained at the output.

The technique uses color map encryption technique, which retains the image quality.

It provides three levels of security.

Level 1 – Overlap of color map & Original Image.

Level 2 – Shuffling of pixels using scan patterns.

Level 3 – System Generated Key.

Keywords*:* Decrypted Image, Encrypted image, Picture Carrier, SCAN Pattern.

I. Introduction

In the world today, the image encryption systems have been increasingly developed to meet the requirements for secure transmission on communication channels. In addition, special and reliable security in the storage and transmission of digital images is necessary in many applications, such as pay television, medical imaging systems, military base image data and communications, and the confidentiality of video conferencing, etc. In recent years, some consumer electronic devices, specially mobile phones and handheld devices have also started to provide the function of saving and replacing digital images via the support of MMS over wireless networks.

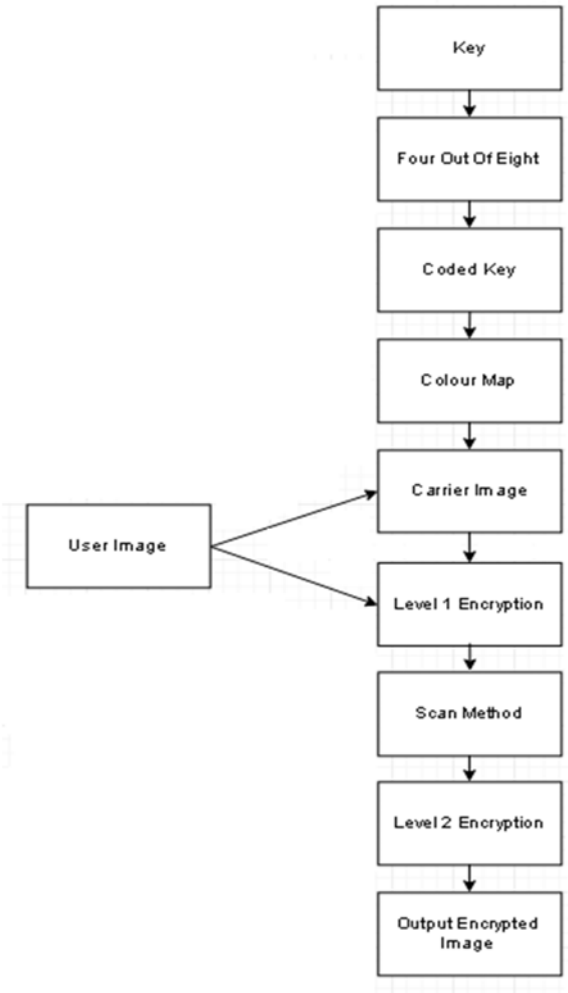


Fig.1 Image Encryption

II. Encryption Algorithm

Input : An m × n size image. and key of any size is taken.

Output : Output image is unreadable and unclear image with Double layer protection .

Step 1 : Since key contain any characters it has to be filter using table1.the characters must lie in the range 36 possible combinations.

Step 2 : Generate a color map as explained in the color map
section .

Step 3 : Using the key , color map , generate a carrier image , its explanation is provided in the carrier image section.

Step 4 : XOR the carrier image and original image this is level 1 encryption .

Step 5 : Use any of the scan patterns to shuffle the image pixels of level one encryption .Using of scan patterns provides the double layer protection .this step provides level two encryption. SCAN patterns information is provided in Level 2 encryption section.

III. Carrier Image Creation

We define hear a new code this is called 4 of 8 code. This code is 8 bits in length, the first 4 bits must contains 2 ones and two zeros, similar with the last four bits. We listed the 36 possible combinations of 4 of 8 code and each code is assigned to an alphanumeric character in Table 1. For 26 alphabets (upper or lower case) and 10 figures shapes to give 36 alphanumeric characters, the code is more appropriate to assign a unique code to each alphanumeric character. As we enter the different keywords, each keyword is taken and reorganised in a matrix form of equal size to the size of the original image.

If the keyword length is very low when the same word is repeated until the length has become equal to the size of the original image. Using the table of alphanumeric character, obtain corresponding binary value of character, based on the first four bits and last four bits row and column of colour map is selected and that value is used to obtain carrier image.

Now, XOR the carrier image and the original image. Encrypted image obtained is used for level two encryption.

Fig.2 Carrier Image

Table1 Carrier Image creation

SL NO.	BIN	HEX	DEC	ALPHA NUMERIC
1	00110011	33	51	A,a
2	00110101	35	53	B,b
3	00110110	36	54	C,c
4	00111001	39	57	D,d
5	00111010	3A	58	E,e
6	00111100	3C	60	F,f
7	01010011	53	83	G,g
8	01010101	55	85	H,h
9	01010110	56	86	I,i
10	01011001	59	89	J,j
11	01011010	5A	90	K,k
12	01011100	5C	92	L,l
13	01100011	63	99	M,m
14	01100101	65	101	N,n
15	01100110	66	102	O,o
16	01101001	69	105	P,p
17	01101010	6A	106	Q,q
18	01101100	6C	108	R,r
19	10010011	93	147	S,s
20	10010101	95	149	T,t
21	10010110	96	150	U,u
22	10011001	99	153	V,v
23	10011010	9A	154	W,w
24	10011100	9C	156	X,x
25	10100011	A3	163	Y,y
26	10100101	A5	165	Z,z
27	10100110	A6	166	0
28	10101001	A9	169	1
29	10101010	AA	170	2
30	10101100	AC	175	3
31	11000011	C3	195	4
32	11000101	C5	197	5
33	11000110	C6	198	6
34	11001001	C9	201	7
35	11001010	CA	202	8
36	11001100	CC	204	9

IV. Color Map

Color map is the combination of random colors in the matrix of size [3][10][10].The primary colors - Red ,Blue & Green combinations could generate 16 million colors .

The color map generated in the technique is using random selection of colors from the 16 million color combinations.

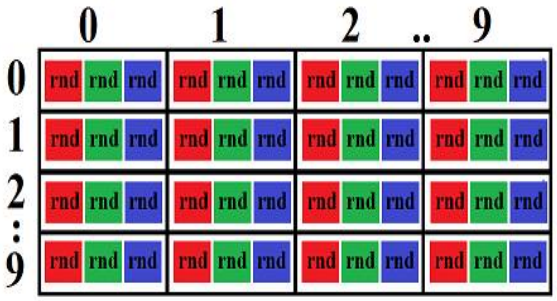


Fig. 3 *Color Map Generation*

Level 1 Encryption:

Level1 encryption is obtained by XOR original image with carrier image (color map).

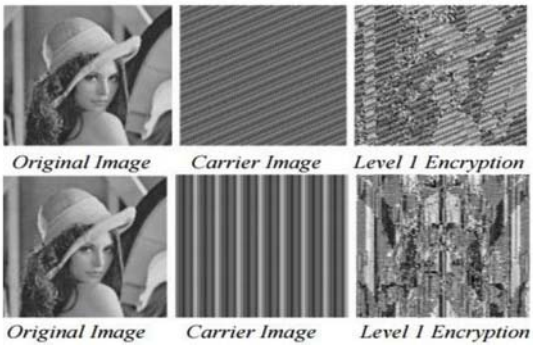


Fig. 4 Level 1 Encryption a) Original Image b) Carrier Image c) Color map

Using key user key, a color map is generated – Carrier Image

Original Image + Carrier Image = Level I Encryption

Level 2 Encryption:

The method used to converts a 2D image into a 1D list, and uses a SCAN language to describe the converted result. In this language, there are several letters SCAN. Each letter represents a SCAN type of scanning order. Different types of SCAN letter combinations can generate different types of secret images.

After determining the combination of letters SCAN, the system then generates a string of SCAN. This string defines the order of scanning of the original image. Then, this method digitizes the original image in the determined order, and further encrypts the SCAN chain using commercial cryptosystems. Given that illegal users can not get the correct SCAN chain, the original image is secure. There is no compression of the image in this method.

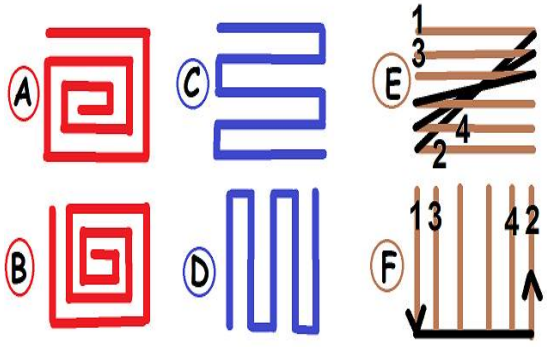
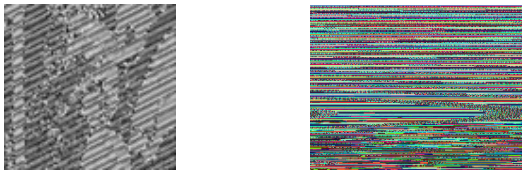


Fig 5 Scan Patterns

V. Experimental Result of Level Two Encryption



Level 1 Encryption Level 2 Encryption

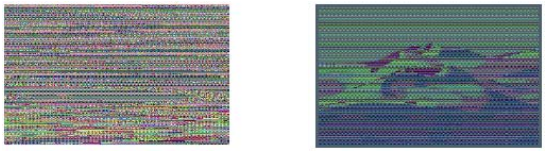
Fig. 6 Experimental result

Level 2 Decryption

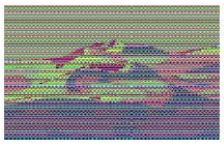
Decryption follows the reverse process of the encryption level 2 .The pixels of the image are encrypted unshuffled according to the scan pattern. The unshuffled image is stored as encrypted image.

Level 1 decryption

Using the output file from level 2 decryption and the carrier image earlier generated. The original image is generated by XOR of level 1 encrypted image and carrier image.



Level 2 Encrypted Image Level 1 Encrypted


Level 1 Encrypted


Original Image

Fig. 7 Level 2 Decryption

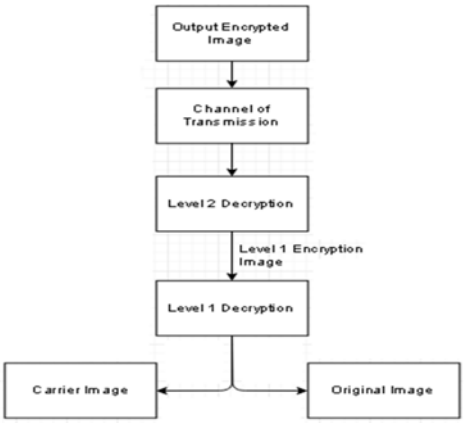


Fig.8 Image Decryption

VI. Conclusion

Applying scan patterns on level 1 encryption gives double layer protection to secretly send original image. A combined and effective method has been proposed in this paper for image encryption using carrier image and SCAN-mapping method. This paper has presented a concept of combination of nibble value of a characters is used as a mapping function to generate carrier image ,merging of carrier image and original image generate level 1 encryption.
Scan patterns cannot be hacked. More secure scan pattern provides for security.

Reference

[1] Ismet Ozturk and Ibrahim Soguk pinaar, "Analysis and Comparison of Image Encryption Algorithms," Transaction on engineering, Computer and Technology, 2004, vol.3, pp.38-44

[2] S.S. Maniccam and N.G. Bourbakis, "Image and video encryption using SCAN patterns," Pattern Recognition, 2004, vol. 37, pp. 725-737.

[3] Bibhudendra Acharya et. el., "Image encryption using advanced hill cipher algorithm", International journal of recent trends in engineering, ACEEE, Vol. 1, No. 1, May 2009.

[4] Said E. El-Khamy , "A partial image encryption scheme based on the DWT and ELKNZ chaotic stream ciper", MASAUM journal of basic and applied science, Vol. 1, No. 3, October 2009.

[5] Bibhudendra Acharya, "Image encryption using advanced hill cipher algorithm", International journal of recent trends in engineering, ACEEE, Vol. 1, No. 1, May 2009.