ISSN No:-2456-2165

A Novel Image Encryption/Decryption Scheme via Amended 4 out of 8 Code and Chaos Map

Anmol Pant, Sarvesh Kaushik
School of Computer Science and Engineering
Vellore Institute of Technology, Vellore
Tamil Nadu, India

Abstract:- Information hiding has been on an ascent lately. New steganography strategies have evolved to make our data more secure and thereby enhance privacy. With the development of information technology, images have now become the center of network information transmission and has replaced text. But as images are now being increasingly used, there has also been an evolution in image information theft technology. To keep pace with the progressing theft technology, we must look for more efficient encryption procedures so as to further enhance our security prospects.

The 4 out of 8 code image encryption techniques deploys transporter or carrier picture creation for encryption. Here the carrier image is made with the help of alphanumeric key phrase that is associated with each image. Each alphanumeric key will have its own unique 8-character bit value created by cutting edge 4 out of 8 code. This recently delivered carrier image is added with the actual image that we want to hide, to get the encoded picture. The opposite technique results the decoded picture. So as to further improve the protection from cyber assaults we even incorporate a cryptographic function which gives authenticity and security to the secret key produced which is to be given to the receiver so as to decode the encrypted image.

Keywords:- *Amended 4 out of 8 code, carrier image, image encryption, file management system, cipher image, cryptography.*

I. INTRODUCTION

The most active subjects in the security related communities are the necessary protection against the data thieves. This gives an importance and the value of exchanged data over the Internet or other media types. As data is an invaluable resource, preventing data leakage and ensuring its protection is the need of the hour. As many cyber security professionals are working day and night to enhance our current data encryption and encapsulation techniques, some techniques like 4 out of 8 encoding, logistic chaotic map, etc. that have been proposed after years of research are being widely used.

The significance of securing data/image has come to its most significant levels in the ongoing years because of the attacks by hackers in order to steal your data and cause harm to the society and individuals' security.

The idea of network security empowers us to store touchy data or transmit it crosswise over shaky networks with the goal that it can't be perused by anybody aside from the expected beneficiary. Image encryption has application in internet communication, videoconferencing, and telemedicine, distance education through video on demand, multimedia systems, military and satellite image processing.

Steganography is the technique of encapsulating data discretely within an ordinary file or any other multimedia file or message in order to avoid detection. The concealed information can then be drawn out and used where it was originally intended to be used. The art of steganography coupled with the practice of cryptography can be very effective as it provides an additional layer of security for hiding data and preventing it from being captured by the attacker. Cryptography is the process of protecting sensitive data using ciphers i.e. mathematic algorithms by data leaking or exposing from the attackers. Modern cryptography is used for providing confidentiality, integrity, non- repudiation and authentication. Key management system involves the generation, storage, exchange and usage of the keys, destruction and replacement of keys using ciphers and cryptographic protocols in order to provide security to the used methodology.

II. LITERATURE SURVEY

A. 4 out of 8 Code

4 out of 8 code is a code for image disintegration for saving the image from unforeseen attacks by converting it into an entirely different image unrecognized by the hackers trying to steal information.

Image permutation can help protect against statistical cryptanalysis. At the same time, it can also change and shuffle the correlation among adjacent pixels by changing over alphanumeric characters to pre-defined binary configuration which includes four one's and four zeros' in which two one's happen to be in the first half while two happen in the last half of the code. It takes a shot at 70 characters in particular.

The carrier image is produced with the assistance of one of a kind code got as 4 out of 8 code, and by adding the carrier image to the unique image we get the ciphered image. As we enter the various keywords, every keyword is taken and changed over into its binary code (4 out of 8 code) and afterward to its corresponding decimal equivalent.

a) Mathematical Model:

Since 26 alphabets (capital letters or small letters) and 10 numerals give 36 alphanumeric characters, this code is more reasonable to allot a one of a kind code to each alphanumeric character. As we enter the various keywords, every keyword is taken and reworked in a matrix form of size

ISSN No:-2456-2165

equivalent to the size of original picture. On the off chance that the length of the keyword is extremely small, at that point a similar keyword is rehashed till the length has gotten equivalent to the estimate of the original picture. By utilizing table of the alphanumeric character and 4 out of 8 code as appeared in table 1, a carrier image is made. Depending on the keyword, carrier image is created and utilized in the subsequent procedure to produce an encoded or encrypted picture**.**

A file system is introduced as well to save the previously generated password and use the pass-word for calculations when another image is encrypted using the cipher. This provides additional security as only the first input will be known to the attacker and rest of the subsequent calculations will be unknown to the attacker.

The final encryption value is then calculated by multiplication of the password stored in the file and the ASCII value of each keyword entered by the sender, which can be stored in a separate array, based on their character lengths. If the character length is even, then the sum of the first and last ASCII value, sum of the second and second last ASCII value, and so on, are multiplied with the password stored in the file. If the character length is odd, then the sum of the first and second ASCII value, sum of third and fourth ASCII value and so on are multiplied to the password stored in the file.

The remainder after performing the modulus of the final result with 10000 generates the required 4 - digit password. This 4-digit password is then shared to the receiver by the sender in order to decrypt the image securely and replace the old password in the file system.

Letter	ASCII	Binary	Letter	ASCII	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010
k	107	01101011	K	075	01001011
l	108	01101100	L	076	01001100
m	109	01101101	M	077	01001101
n	110	01101110	N	078	01001110
o	111	01101111	O	079	01001111
p	112	01110000	P	080	01010000
q	113	01110001	Q	081	01010001
r	114	01110010	R	082	01010010
s	115	01110011	S	083	01010011
t	116	01110100	T	084	01010100
u	117	01110101	U	085	01010101
v	118	01110110	V	086	01010110
w	119	01110111	W	087	01010111
x	120	01111000	X	088	01011000
y	121	01111001	Y	089	01011001
z	122	01111010	Z	090	01011010

Table 1: Conventional 4 out of 8 encoding Combinations

B. Chaos Map

Chaos theory is a non-deterministic theoretical system based on nonlinear systems and randomness. Chaos is a random process found in non-linear, dynamical system, which is non-period, non-converging and bounded. Moreover, it has a very sensitive dependence upon its initial condition and parameter.

However, the current image chaotic encryption technology still fails to break through the category of two-dimensional integer-order chaotic systems, and there is still room for improvement in dynamic characteristics of the proposed algorithm. The following mathematical model could help better explain the process of encryption the chaos map adopts.

Using simple chaotic maps, large combinations of random digits can be formed. Here, we are using two chaotic maps in parallel, which are cross connected to each other. Each of the map generates one random digit in each run i.e. one number per iteration.

- **Mathematical Model:** The step by step proposed chaos map encryption procedure is presented below.
- **The Permutation Phase -** The Logistic chaos map is used to generate a random sequence. The values are chosen with a precision of 10 digits. The sequence generated by the above step is used to permute the pixels of plain image.
- **The Substitution Phase -** The permuted data is then converted to DNA sequence (C). The same sequence is again used to generate a random bit sequence. For this purpose, this binary sequence is also converted to its DNA sequence (D).

The DNA sequences C and D are added together which results in a new DNA sequence E. E is again converted back to sequence of 8 bit (integer) F form.

Finally, XOR-ing of each element of the sequence is done with the elements previous to that index on F which gives the final encrypted image.

III. PROPOSED ALGORITHM–AMENDED 4 OUT OF 8 ENCODING

This code is of 8-bit length with 4 number of one's and 4 number of zero's. This would give us 70 combinations, which is more than twice the number of combinations offered by the conventional 4 out of 8 encoding based approach. Since 52 letters in order (capital letter and small letters) and 10 numerals and 8 special characters which combines to give 70 alphanumeric characters, this code is increasingly

reasonable to allot an exceptional code to every alphanumeric character. As we enter the various keywords, every keyword is taken and changed over into its binary code (4 out of 8 code) and afterward to its decimal equivalent.

This code helps accommodate special and alphanumeric characters, which was not possible previously in the normal 4 out of 8 encoding. This technique might be computationally expensive as it requires double the storage space, but at the same time, it also helps convey double the information about the contents of each and every bit.

IV. PROPOSED METHODOLOGY AND CIPHER USED

Here the 8 bits account for over 70 characters that can be encoded into different binary equivalents. The below table (II) sums up all the possible character combinations that are provided by the advance 4 out of 8 encoding method.

For each pixel of the image, a password is decided and stored in a file, the password is nothing but a binary representation of an alphanumeric character, with which every encoded pixel can be multiplied or divided to get the required encrypted pixel.

The final encryption value is then calculated by multiplication of the password stored in the file and the converted value of each pixel frame entered by the sender, which can be stored in a separate array, based on their character lengths and memory constraints.

Advance 4 out of 8 encoding follows the same conventions when it comes to the addition of bits based on the character length, if the character length is even, then the sum of the first and last ASCII value, sum of the second and second last ASCII value, and so on, are multiplied with the password stored ln the file. If the character length is odd, then the sum of the first and second ASCII value, sum of third and fourth ASCII value and so on are multiplied to the password stored in the file.

The remainder after performing the modulus of the final result with 10000 generates the required 4 - digit password. This 4-dlglt password is then shared to the receiver by the sender ln order to decrypt the image securely and replace the old password in the file system.

Serial No.	Binary form	Hex Decimal form	Decimal form	Alphanumeric- special character
1	0000 1111	F	15	a
2	0001 0111	17	23	b
3	0001 1011	1B	27	c
4	0001 1101	1D	29	d
5	0001 1110	1E	30	e
6	0010 0111	27	39	f
7	0010 1011	2B	43	g
8	0010 1101	2D	45	h
9	0010 1110	2E	46	i
10	0011 0011	33	51	j
11	0011 0101	35	53	k
12	0011 0110	36	54	l
13	0011 1001	39	57	m
14	0011 1010	3A	58	n
15	0011 1100	3C	60	o
16	0100 0111	47	71	p
17	0100 1011	4B	75	q
18	0100 1101	4D	77	r
19	0100 1110	4E	78	s
20	0101 0011	53	83	t
21	0101 0101	55	85	u
22	0101 0110	56	86	v
23	0101 1001	59	89	w
24	0101 1010	5A	90	x
25	0101 1100	5C	92	y
26	0110 0011	63	99	z
27	0110 0101	65	101	A
28	0110 0110	66	102	B
29	0110 1001	69	105	C
30	0110 1010	6A	106	D

ISSN No:-2456-2165

35	0111 1000	78	120	I
36	1000 0111	87	135	J
37	1000 1011	8B	139	K
38	1000 1101	8D	141	L
39	1000 1110	8E	142	M
40	1001 0011	93	147	N
41	1001 0101	95	149	O
42	1001 0110	96	150	P
43	1001 1001	99	153	Q
44	1001 1010	9A	154	R
45	1001 1100	9C	156	S
46	1010 0011	A3	163	T
47	1010 0101	A5	165	U
48	1010 0110	A6	166	V
49	1010 1001	A9	169	W
50	1010 1010	AA	170	X
51	1010 1100	AC	172	Y
52	1011 0001	B1	177	Z
53	1011 0010	B2	178	0

64	1101 0100	D4	212	@
65	1101 1000	D8	216	#
66	1110 0001	E1	225	$
67	1110 0010	E2	226	%
68	1110 0100	E4	228	ˆ
69	1110 1000	E8	232	&
70	1111 0000	F0	240	*

Table 3: All possible combinations of amended 4 out of 8 encoding along with alphanumeric and special characters.

V. RESULTS

The above proposed algorithm was implemented using MATLAB and the results obtained for carrier image and encrypted image for numerous different values (of varying complexity) of the encryption key are shown below.

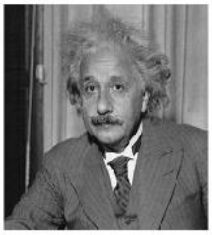
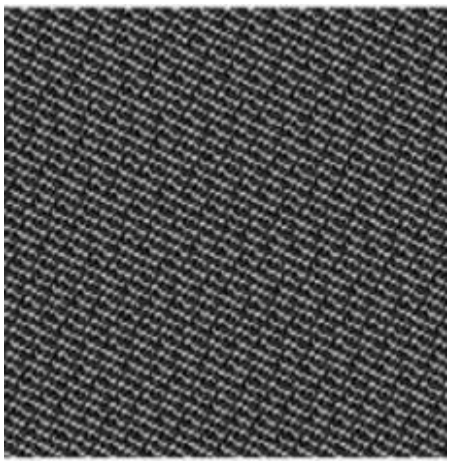


Fig.1: Actual Image (Original image before encryption)

A. *Key- hello*

a)



b)

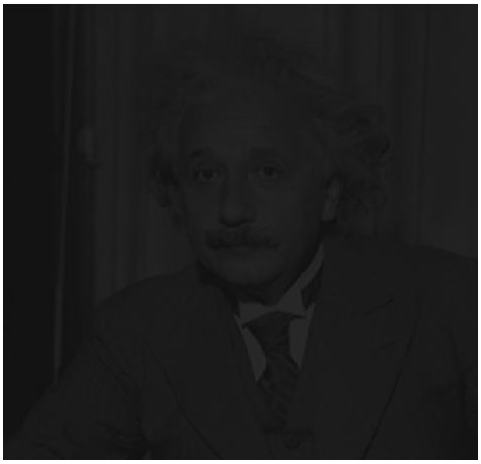
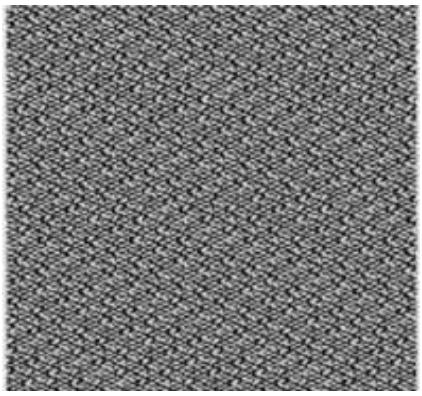


Fig.2. a) Carrier Image b) Encrypted Image

B. *Key- hello123*

a)



b)

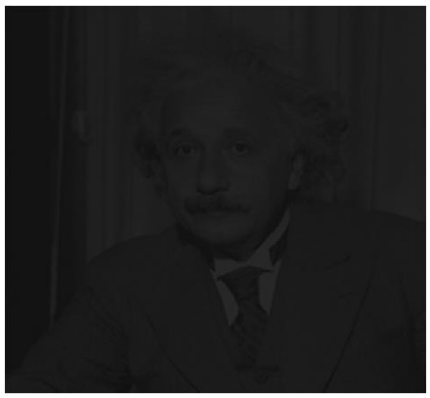
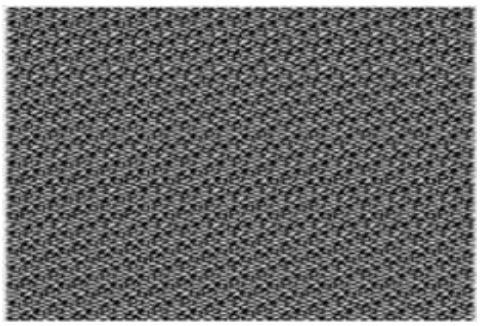


Fig.3. a) Carrier Image b) Encrypted Image

C. Key- @ello#123

a)



b)

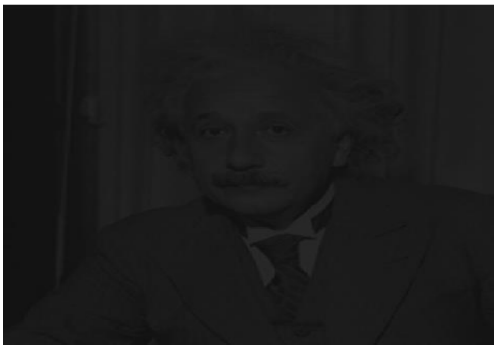
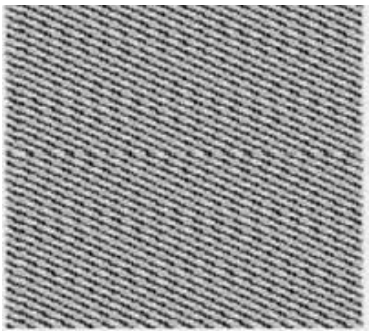


Fig.4: a) Carrier Image b) Encrypted Image

D. 5.4: Key- !12@3#

a)



b)

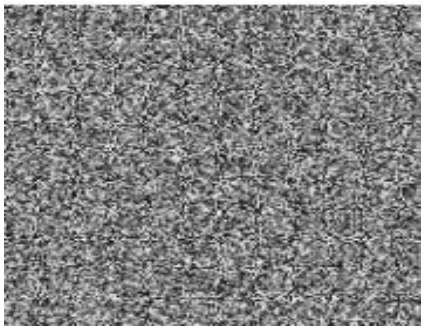
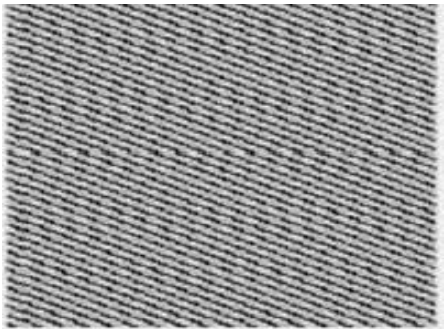


Fig.5: a) Carrier Image b) Encrypted Image

E. Key- the quick brown fox jumps over the lazy dog

a)



b)

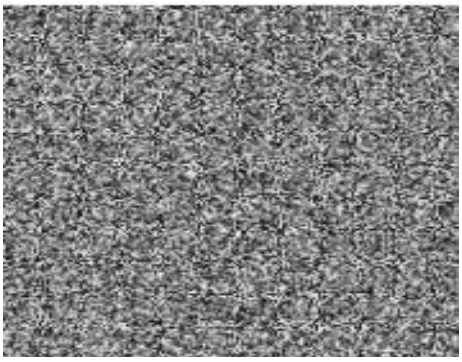
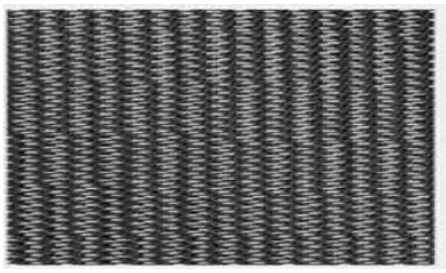


Fig. 6: a) Carrier Image b) Encrypted Image

F. *Key@*thequickbrownfoxjumpsoverthelazydog#1234!56789

a)



b)

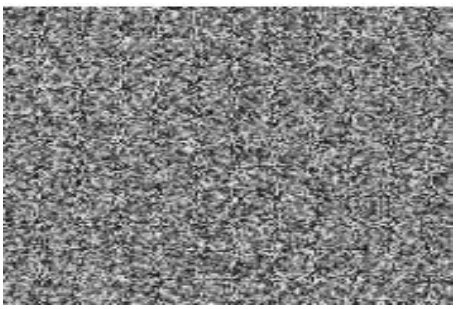
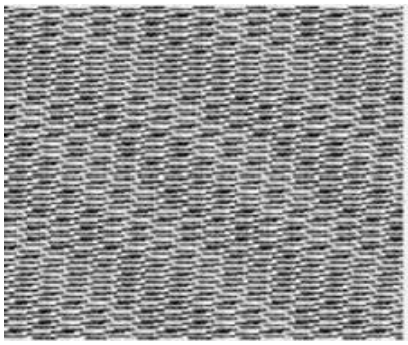


Fig.7: a) Carrier Image b) Encrypted Image

*G. 5.7: Key- 1!2@3#4$5%6^7&8*9*

a)



b)

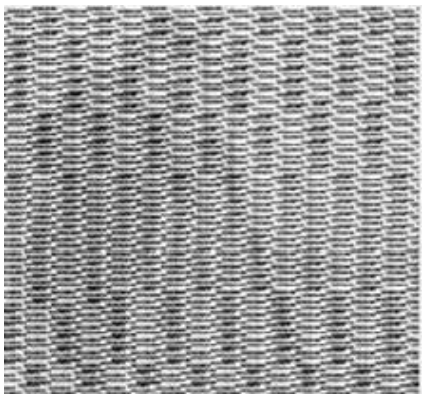


Fig. 8: a) Carrier Image b) Encrypted Image

H. Decryption

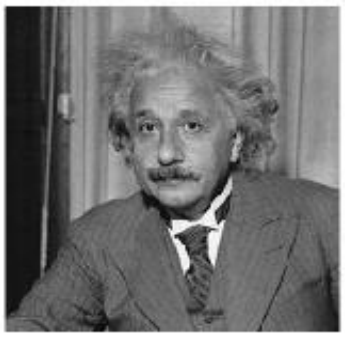


Fig. 9: Decrypted Image (received image)

VI. COMPARISON

The proposed algorithm, an upgrade over the conventional 4 out of 8 encoding, is both feasible to implement and easy to use. Coupled with the fact that it is lossless and permutes each pixel on almost 70 characters (including numbers and special characters) rather than its conventional counterpart that uses just 26 letter combinations, it has the potential to be incorporated in web applications and replace some of the contemporary industrial level encryption algorithms out there.

It boasts of an end to end file management system, so that the intermediate carrier images generated are also not lost, adding another layer of security. The algorithm, works with compound cipher and carrier images and hence, it is harder for attackers to intercept and decrypt the images without the key and the password.

VII. CONCLUSION

The above algorithm proposes an 8 bit alternative to the conventional 4 bit encoding technique, which makes it a little more memory consuming, but at the same time, makes room for more complex permutations of characters as keys, which accounts for a higher degree of distortion in the encrypted image. The algorithm is both feasible to implement (as done here) and provides a higher degree of security as compared to its conventional counterpart.

The future work for the proposed algorithm could be to add two factor authentication to the file system, so that the attacker cannot extract the encrypted image even if the password is somehow breached, thereby making the communication and image transmission over the network all the more secure.

ACKNOWLEDGMENT

We would like to thank Dr. Jayakumar K., Associate Professor Grade 1, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, for his unwavering support and guidance throughout the tenure of this research study that led to its successful completion.

REFERENCES

[1.] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li.,A new chaotic algorithm for image encryption, Chaos, Solitons & Fractals,Volume 29, Issue 2, 2006.
[2.] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani. A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013)
[3.] Mitra, A. & Rao, Y. & Prasanna, S. (2006). A new image encryption approach using combinational permutation techniques.
[4.] New Image Encryption Approach using Combinational Permutation Techniques Mitra, Y. V. Subba Rao and S. R. M. Prasanna
[5.] New Image Encryption Approach using Combinational Permutation Techniques Mitra, Y. V. Subba Rao and S. R. M. Prasanna
[6.] Iøsmet Öztürk and øbrahim Soukpınar. Analysis and Comparison of Image Encryption Algorithms International Journal of Information Technology Volume 1 Number 2.
[7.] Panduranga H.T, Naveen Kumar S.K. Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images. International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010.
[8.] Taneja, N., Raman, B. & Gupta, I. Combinational domain encryption for still visual data. Multimed Tools Appl 59**,** 775–793 (2012).
[9.] G.A. Sathish Kumar, K. Bhoopathy Bagan, V. Vivekanand, A Novel algorithm for image encryption by integrated pixel scrambling plus diffusion [IISPD], Procedia Computer Science, Volume 3, 2011.
[10.] Maniccam, S. S. and Nikolaos G. Bourbakis. "Image and video encryption using SCAN patterns." Pattern Recognit. 37 (2004): 725-737.
[11.] Pan, H., Lei, Y. & Jian, C. Research on digital image encryption algorithm based on double logistic chaotic map. J Image Video Proc. 2018, 142 (2018).
[12.] Zhi Zhong. Double image encryption using double pixel scram-bling and random phase encoding. Optics Communications, 2012.
[13.] Prasanna SRM. An image encryption method with magnitude and phase manipulation using carrier images.IJCS, page132137.