Secured Image encryption/decryption using advanced 4 out of 8 code

Rahul Siddhartha, RaghavJhawar, Harsh Saxena

B.Tech Computer Science with Specialization in Information Security & VIT University Vellore, India

Abstract:
Information hiding has been on a rise in recent times. New steganography techniques have evolved to secure data and enhance privacy. The image encryption employs carrier image creation for encryption. Here the carrier image is made with the assistance of alphanumeric key phrase. Each alphanumeric key will have a unique 8-bit value produced by advanced 4 out of8code.This newly produced carrier image is added with actual image to get encrypted image. The reverse procedure results the decrypted image. In order to improve the security against attacks we even include a cryptographic function which provides authentication and security to the received password generated which is to be given bythe receiver to decrypt the encrypted image. This paper involves a key management system in which every time a new password is generated according to the keyword entered by the sender.

Keywords: *Steganography, carrier image, advanced 4 out of 8 code, authentication, security, key management system.*

I. Introduction

The evolution of internet gave another advanced approach to spreading the data allthe more easily. Data is an important and has a worth like some other resource. As a benefit, information should be secured from various malicious attacks by the people on internet. In light of the attribute of digital pictures, some security issue turns out other than the broad utilization of these pictures. 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 guidance of 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, telemedicine, distance education through video on demand, multimedia systems, military and satellite imageprocessing.

Steganography is the technique of hiding data secretly within a normal, ordinary file or any multimedia file or message in order to avoid detection. The hidden secret data is then extricated at its destination. The art of steganography along with cryptography can be very effective as it provides an additional method 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 algorithmsbydataleakingorexposingfromthe attackers. Modern cryptography is used for providing Confidentiality, Integrity, Non-repudiation andAuthentication.

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. We have developed a key management system in our work which generates key using the keywords given by thesender.

In our work, we are using image encryption using carrier image. All of us know that image encryption is much safer than the text encryption. Text encryptions can be easily hacked but it is difficult to crack the image encryption techniques. Thus, image encryption

provides us a much safer way for transmission of our details. Carrier images are the images superimposed over the original image to hide the information of the original image.
Carrier images are developed using the keyword from the user and is also of the sizeof the original image. In order to reveal the information at the destination, it is the carrier image that has to be removed from the encryptedimage.

In our work, we use advanced 4 out of 8 code which converts alphanumeric character and special character keyword to binary and works on 70 characters. Each predefined binary format has four zero’s and four one’s. We have removed the concept of two one’s in nibble.
So, in our work, we have tried to come up with a code that will encrypt and decrypt an image so that it can further be transmitted over the insecure network as image modification and working on image is advantageous on MATLAB.

II. Proposed Algorithm

4 out of 8 code is a code to change over alphanumeric characters to pre-defined binary configuration which included four one's and fourzeros'inwhichtwoone'shappeninthefirst half while two happen in the last half. It takesa shot at 70 characters inparticular.

The carrier image is produced with the assistance of one of a kind code got as 4 out of 8 code, by adding the carrier image to unique image we get the ciphered image. Here we are characterizing a new code got advanced 4 out of 8 code.

This code is of 8-bit length with 4 number of one's and 4 number of zero's. We recorded every one of the 70 possible combinations of the advanced 4 out of 8 code and each code is relegated to an alphanumeric character intable 1. Since 52 letters in order (capital letters 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 alpha-numeric 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 itsdecimal structure lastly they are revamped in a matrix form of size equivalent to the size of actual image. On the off chance that the length of the keyword is little, at that point a similar keyword is rehashed till the length becomes equivalent to measure of original image. By utilizing lookup table of the alpha-numeric character and 4 out of 8 code, a carrier image is made. Depending upon the keyword, carrier image is created and utilized in the expansion procedure to produce a encrypted image. Keyword size impact the overall complexity of the carrier image. Using the small key-word with special characters will results in the complex carrier image pat-tern while large keyword with single type of character will result in the simple pattern of the carrierimage.Usingreverseprocedure,wewill get the decrypted process. For expanding the security level, we will present a figure through which a sender will produce a secret phrase and which is to be shared to the receiver before decrypting the image. 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 thecipher.

This provides security as only the first input will be known to the attacker and rest of the calculations will be unknown to the attacker. Hence, the pro-posed algorithm is a lossless which doesn’t impact the size of the image or the loss of information in the encrypted image transmitted over the network.

III. BlockDiagram

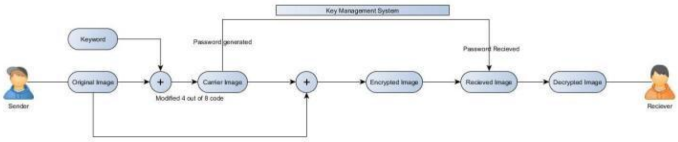


Fig 1.1 Block Diagram

IV.Table I. 70 possible combination of advanced 4 out of 8 code along with alphanumeric and specialcharacters

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
31	0110 1100	6C	108	E
32	0111 0001	71	113	F
33	0111 0010	72	114	G
34	0111 0100	74	116	H
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
54	1011 0100	B4	180	1
55	1011 1000	B8	184	2
56	1100 0011	C3	195	3
57	1100 0101	C5	197	4
58	1100 0110	C6	198	5
59	1100 1001	C9	201	6
60	1100 1010	CA	202	7
61	1100 1100	CC	204	8
62	1101 0001	D1	209	9
63	1101 0010	D2	210	!
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	*

V. Cipherused

1. A random four-digit password is stored in a file.

2. Each keyword entered by the sender is converted into its ascii values and stored in array.

3. Length of the array is calculated and it is checked whether it is even orodd.

4. Each keyword entered by the sender is converted into its ascii values and stored in array.

5. Length of the array is calculated and it is checked whether it is even orodd.

6. If length is even, then the sum of the first and last ascii value, sum of the second and second last ascii value, and soon…

7. Each sum is multiplied and stored in a variable which changes dynamically as the sum of the ascii values is performed.

8. Finally,theresultofmultiplicationismodby 10000, this generates the 4-digitpassword.

9. If length is odd, then the sum of the first and last ascii value, sum of the second and second last ascii value, and soon…

10. Each sum is multiplied and stored in a variable which changes dynamically as the sum of the ascii values is performed.

11. Finally, the middle value of the odd length array is added to the result of multiplication. Then the final result is mod by 10000, this generates the 4-digitpassword.

12. This 4-digit password is shared to the receiver by the sender in order to decrypt the imagesecurely.

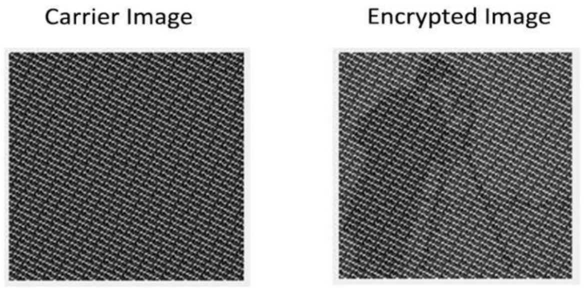
13. Finally, the middle value of the odd length array is added to the result of multiplication. The final value is calculated by multiplication of the pass-word stored in file and the value generatedbystep8.Thenthefinalresultismod by 10000, this generates the 4-digitpassword.

14. This 4-digit password is shared to the receiver by the sender in order to decrypt the image securely and replace the old password in the filesystem.

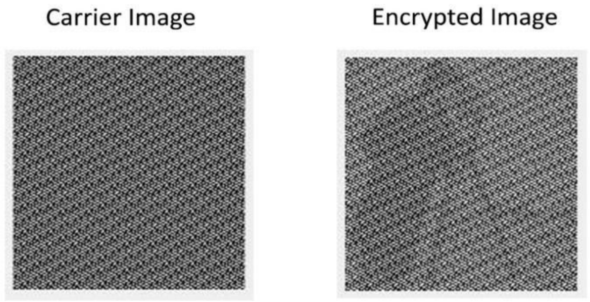
VI. Result andConclusion

Actual Image (Original Image)

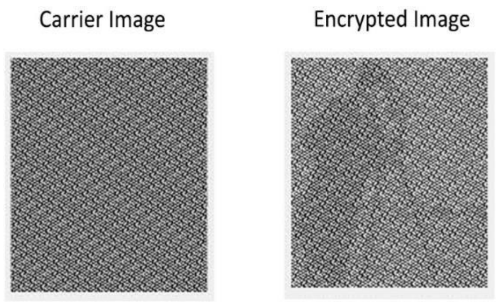
1) Key: hello



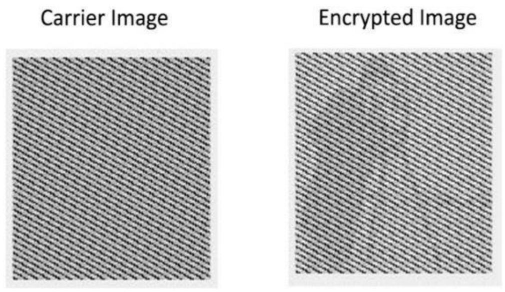
2) Key: hello123



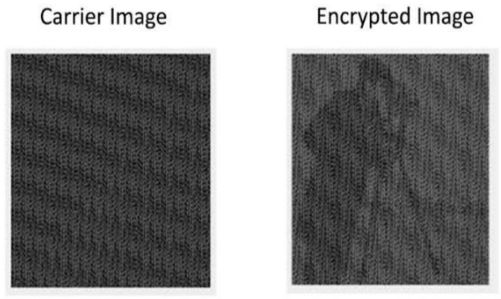
3) Key: #ello@123



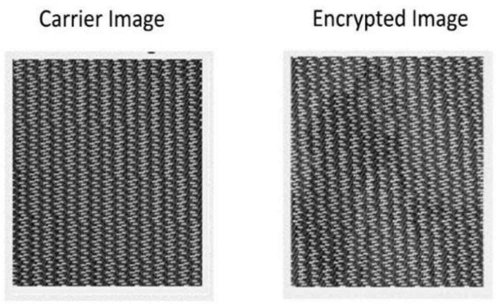
4) Key: 1!2@3#



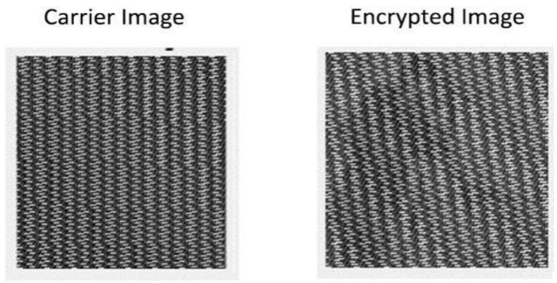
5) Key: thequickbrownfoxjumpsoverthelazydog



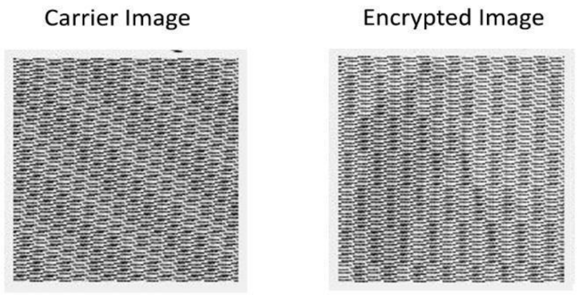
6) Key: thequickbrownfoxjumpsoverthelazydog987654321



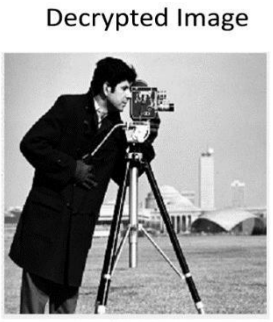
7) Key: #thequickbrownfoxjumpsoverthelazydog@123456789!



8) Key: 1!2@3#4$5%6^7&8*9



Decrypted Image (Received Image)



VII. Advantages

1. Hybrid approach for image encryption provide more security from attackers as compare to individual encryptionprocess.

2. This algorithm works with complex cipher and complex carrier images. Hence encrypted image becomes more distorted andsecured.

VIII. Conclusion

Hence, we can conclude, that the above results from the proposed algorithm that is secure image encryption and decryption using advanced 4 out of 8 code provides more complex patterns for the image encryption as compared with the individual encryption and decryption methods generally. Proposed algorithm allows to make use of more complex carrier-keywordsinordertomakecarrierimage more complex. Therefore, as the complexity increases the encrypted image becomes more distorted as compared to the result obtained from the simple keyword encryption. File system increases the security level so that adversary is not able to attack the encrypted image and extract the password from it Thus, the future work for this proposed algorithmcan be described as the use of more complexcipher like including file management system in order to make image transmission more secure over thenetwork.

IX. References

[1] Panduranga H.T, Naveen Kumar S.K, (Submitted on 5 Mar 2010), "*Hybrid approach for Image Encryption Using SCAN Patterns andCarrierImages*",IJCSE,Vol.2,No.2March 2010

[2] Sunil Kumar K.M, Kiran Kiran, Anand U. Hiremath, (Published 2013), "*Image Encryption usingmodified4outof8codeandchaoticmap*",International Journal of Computer Applications (0975 8887) Volume 74 - No. 11, July 2013

[3] T. Sivakumar and R. Venkatesan, (Published2014),"*ANovelApproachforImage Encryption using Dynamic SCAN Pattern*", International Journal of Computer Science 41(2):91-101, May2014

[4] Reza Moradi Rad, Abdolrahman Attar, and RezaEbrahimiAtani,(Published2013),"*ANew Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR*" International Journal of Signal Processing, ImageProcessing and Pattern Recognition Vol.6, No.5,2013

[5] A Mitra, YVS Rao, SRM Prasanna, (Published 2006), "*A New Image Encryption Approach using Combinational Permutation Techniques*", International Journal of Electrical and Computer Engineering 1:2,2006