International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 8231-8239

http://www.ripublication.com

Reserving Room before Encryption for Reversible Data Hiding with Scan Encryption

P.S.Gomathi[1], S.Sindumathi[2], B.Kalaavathi [3]

[1]Assistant Professor, [2]PG Scholar,
Department of Electronics and Communication Engineering,
V.S.B. Engineering College, Anna University, Karur, Tamil Nadu, India.
gomsps@gmail.com[1] , sinducgw@gmail.com[2],
[3]Professor, Department of Computer Science and Engineering,
K.S.R. Institute for Engineering and Technology, Anna University,
Tiruchengode, Tamil Nadu, India.
[3] kalabhuvanesh@gmail.com

Abstract

Nowadays, more attention turn towards reversible data hiding (RDH) in encrypted images, as because it upholds the outstanding property that the original image can be recovered without any loss after hidden information is taken out while protecting the secrecy of the image content. All former methods implant data by vacating room from the encrypted images that may lead to some errors while extracting the data as well as while restoring the image. In this paper, a novel method has been proposed with reserving room before encryption with a traditional RDH algorithm, and a hybrid approach called as Image Encryption using SCAN patterns and carrier images for encryption. Hence, it is easy for the data hider to reversibly embed data in the SCAN encrypted image. The suggested method can achieve real reversibility, that is, extracting the data and recovering the image are free of any error and the resulting encrypted image is found to be more distorted in hybrid technique. Experimental results show that this novel method can embed more than 10 times as large payloads for the same image quality as the previous methods, such as for PSNR =40 dB.

Keywords: Reversible data hiding, SCAN patterns, Image encryption.

1. INTRODUCTION

Reversible Data Hiding (RDH) is a technique, where the original image can be recovered without any loss after the hidden data is extracted. This important technique finds its application in the areas of medical imagery, military imagery and law

forensics, where no distortion of the original image is not permitted. There are number of works on data hiding in the encrypted domain. This method by Reserving Room before Encryption with a traditional RDH algorithm makes it easy for the data hider to reversibly embed data in the encrypted image. In addition, this novel method can achieve the extraction of data separately and reduces the loss on the quality of marked decrypted images. Experiments show that this method can embed more than 10 times as large payloads for the same image quality as the previous methods. The encryption technique used here is accomplished by the hybrid approach for Image Encryption using SCAN patterns and carrier images[7]. Although it involves existing method like SCAN methodology[2], the novelty of the work lies in hybridizing and carrier image creation for encryption. Keywords based on alphanumeric character are used to create the carrier image. Each key will have a sole 8 bit value generated by 4 out of 8-code. The newly produced carrier image is added with original image to obtain encrypted image. The SCAN based method can be applied to either original image or carrier image, after the addition of original image and carrier image to obtain highly distorted encrypted image.

After encrypting the entire data of an uncompressed image, the additional data can be embedded into the image by modifying a small proportion of encrypted data. One can first decrypt the data from the encrypted image using key and the decrypted version is similar to the original image.

2. RELATED WORK

In the existing system, more attention is paid to Reversible Data Hiding (RDH) in encrypted images[6,4], since it maintains the excellent property that the original cover can be losslessly recovered after embedded data is extracted while protecting the privacy of the image contents. All conventional techniques embed data by reversibly vacating room from the encrypted images, which may be lead to some blunders while extracting the data or image [4,5,6]. The conventional methods implement RDH in encrypted images by vacating room after encryption, as an alter to which we suggest by reserving room before encryption. So the data hider can get more space to make data hiding process effortless. Also the encryption technique used was the stream cipher method [3] and it does not provide more distorted encrypted image. However, since the entropy of encrypted images has been capitalized, these techniques can only achieve small payloads generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration.

3. PROPOSED METHOD

This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. This method can achieve the extraction of data separately and reduces the loss on the quality of marked decrypted images. This method by reserving room before encryption with a traditional RDH algorithm makes it easy for the data hider to reversibly embed data in the

encrypted image. Since the encryption technique based on SCAN pattern and Carrier images used in our proposed work gives more distorted encrypted image it is not easy for the hacker to know that it already contains some data.

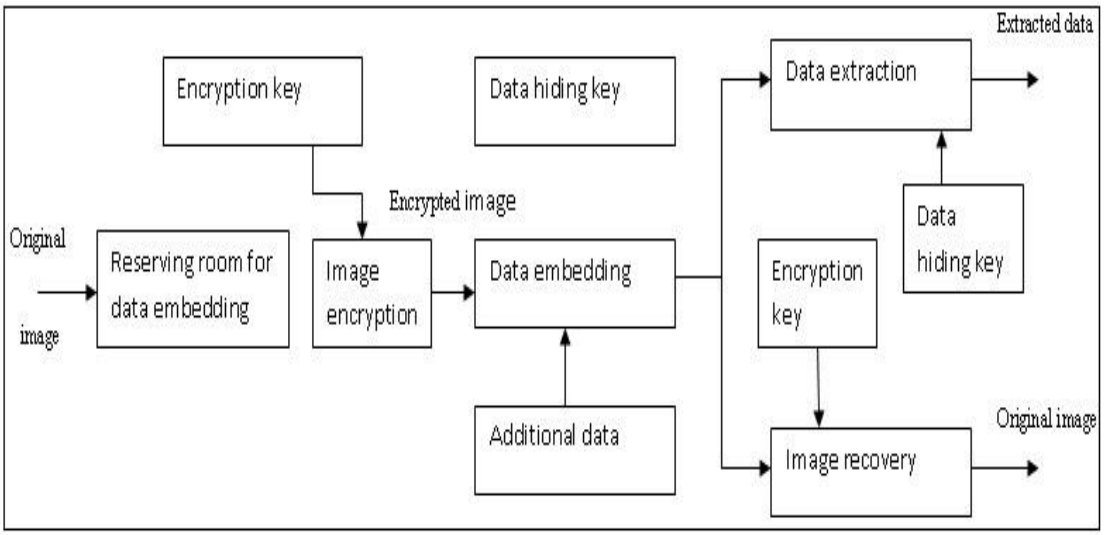

Figure 1: Block diagram of the proposed method.

3.1. MODULES

It consists of following modules.1.Encrypted Image Generation 2.Data Hiding in Encrypted Image 3. Data Extraction and Image Decryption.

1. Encrypted Image Generation

In this module, to construct the encrypted image it falls into three steps:

a) Image Partition,
b) Self Reversible Embedding followed by image encryption.

At first, partitioning of the original image into two parts has been done and then, the LSBs of one part are reversibly embedded into another with a standard RDH algorithm so that LSBs can be used for accommodating message.

a) Image Partition: The goal of image partition is to partition image into two parts and to construct a smoother area on which RDH techniques would give better result [1].

b) Self Reversible Embedding and Image Encryption: Many RDH techniques have been emerged recent years and most popular is based on difference expansion [8] in which difference of each pixel group is expanded and the LSBs of the difference can be used in embedding. The goal of self-reversible embedding is to embed the LSB-planes by employing traditional RDH algorithms. There are several methods for image encryption which deals in

their own ideas. In few image encryption algorithms, encryption process depends only on the keywords, but in some other algorithms they use only carrier image for encryption. The proposed idea is to hybrid the existing algorithms to get a new path for encryption. Hence the concept of hybridizing SCAN pattern and Carrier image for Image encryption emerges to get highly distorted Images.

The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. Each basic pattern has eight transformations numbered from 0 to 7. For each basic scan pattern, the transformations 1, 3, 5, 7 are the reverse of transformations 0, 2, 4, 6, respectively. Continuous scan C is used here.

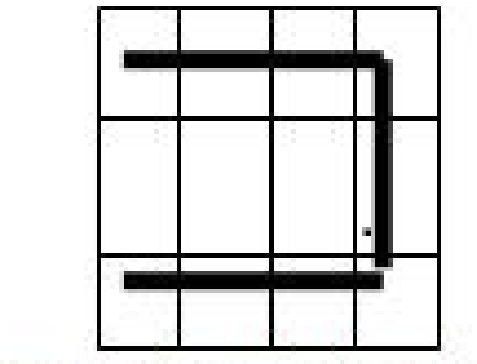

Figure 2: Continuous scan pattern

Carrier image is created by a new code called 4 out of 8 code [2,7]. This code is of 8 bit length with 4 number of one's and 4 number of zero's and we made one consideration that each nibble must have 2 number of ones and 2 number of zeros. This code can be used to generate code for all 26 alphabets and numbers ranging from 0-9.

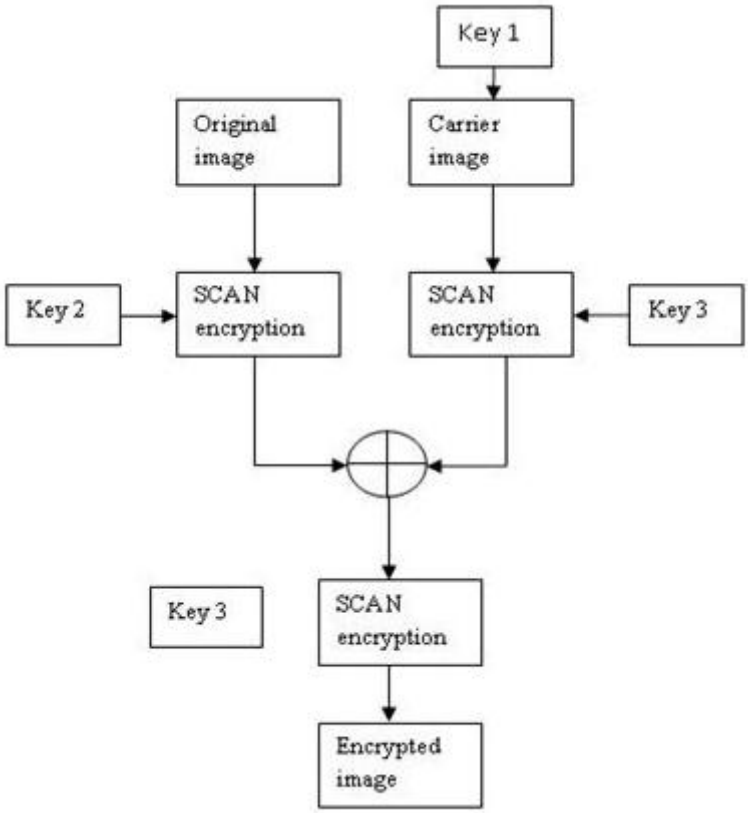

Figure 3: Block diagram of proposed image encryption approach using SCAN patterns and carrier images.

Table 1: 36 possible combination of 4 out of 8 code along with alphanumeric character.

Sl.No	Binary Number	Hexadecimal Number	Decimal Number	Alpha Numeric Character
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	172	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

As the different keywords have been entered by the user, each keyword is taken and rearranged in a matrix form of size equal to the size of original image. If the keyword length is very small then the same keyword is repeated till the length is become equal to size of original image. Depending upon the keyword, carrier image is generated and used in the addition process to generate an encrypted image [1].

2. Data Hiding In Encrypted Image

After producing the encrypted image, the next stage is to hand over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image in the space that has been reserved before encryption with the data hiding key.

3. Data Extraction and Image Recovery

In this module, when the database manager gets the data hiding key, database manager can decrypt and extract the additional data by directly reading the decrypted version. The feasibility of the work will be guaranteed if the hidden data is extracted out first followed by image decryption.

4. RESULTS AND ANALYSIS

Here 'lena.bmp' is taken as a reference image. The objective criteria PSNR(Peak Signal -to-Noise Ratio) is employed to evaluate the quality of marked decrypted image quantitatively.

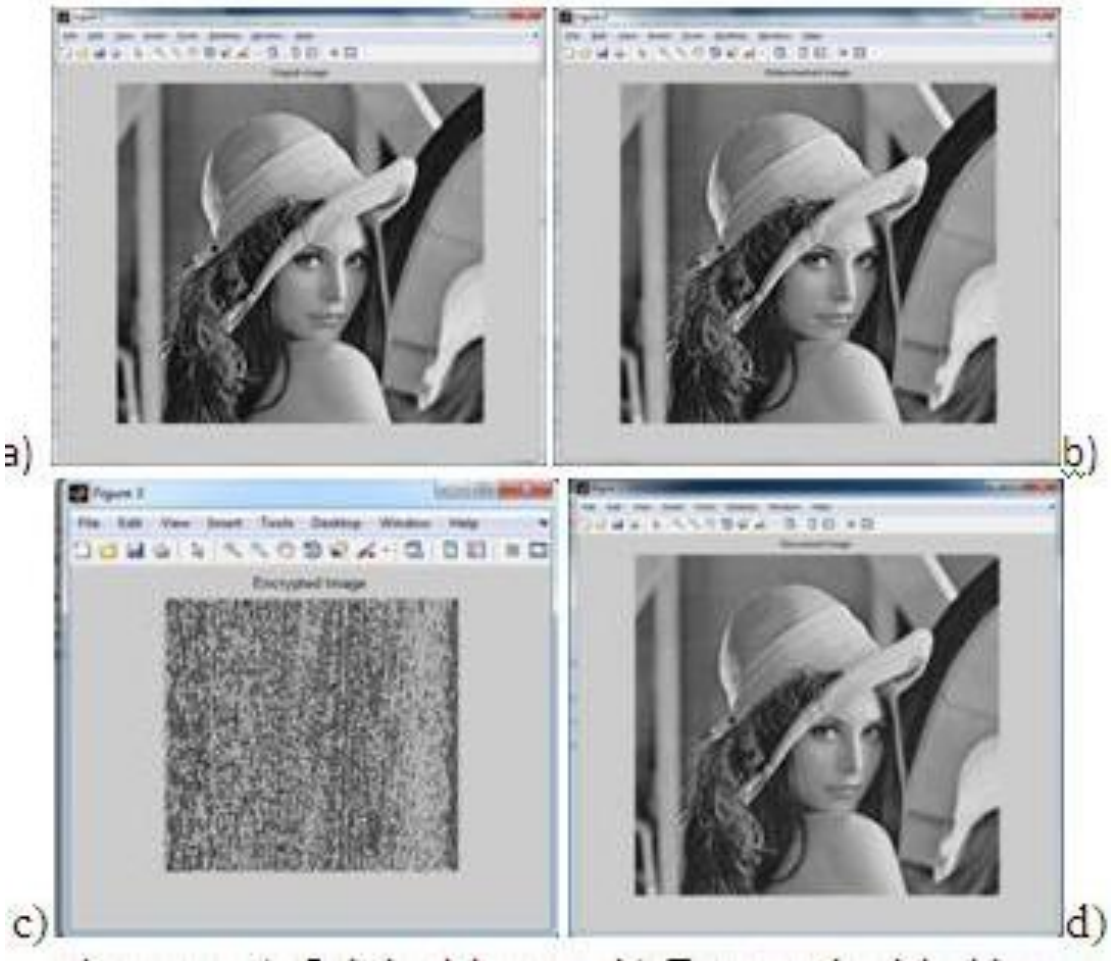

Figure 4 : a) Original image b) Data embedded image c) SCAN encrypted image d) Decrypted image.

Table 2: PSNR comparison for three different LSB plane choices under various embedding rates.

PSNR results(dB)						
Embedding rate(bpp)		0.1	0.2	0.3	0.4	0.5
Lena	1 LSB –plane	52.33	49.07	45.00	43.25	39.88
	2 LSB -planes	51.55	48.39	44.60	42.56	39.46
	3 LSB -planes	49.96	46.79	43.98	41.91	39.53

Table 2 shows the comparison results measured by PSNR for three different choices of LSB-planes where the embedding rate is measured by bits per pixel (bpp). The choice of single LSB-plane outperforms the other two at low embedding rate levels (less than 0.2 bpp). It is consistent with our spontaneous understanding: when embedding rate is small B has the capacity to embed LSBs of A in a single round without size improvement. Utilizing multiple LSB-planes can only introduce average distortion from 0.5 to 1.75 (case of two LSB-planes) in A , calculated by mean squared error (MSE).

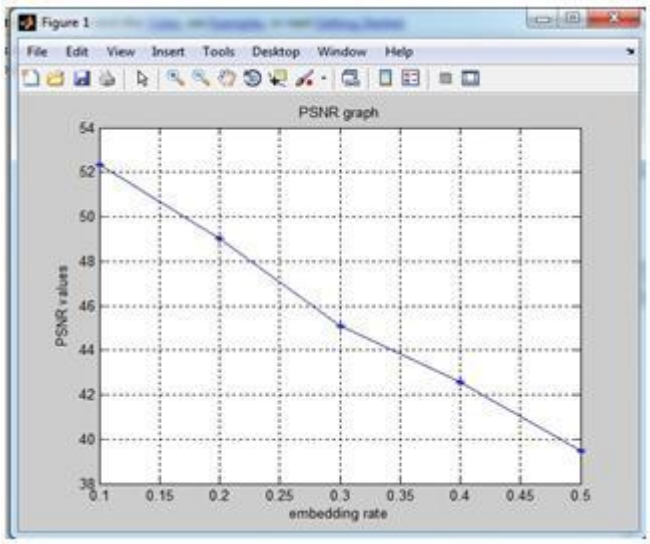

Figure 5: Graph showing PSNR values for different embedding rates.

5. CONCLUSION

Reversible data hiding in encrypted images is a new technique drawing attention because of the privacy-preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. The proposed hybrid approach for encryption results in producing more distorted

image that makes the hacker feel difficult to know what it contains actually. Furthermore, this novel method can achieve real reversibility, separate data extraction and reduces the loss on the quality of marked decrypted images.

REFERENCES

1. Yukthi.B.R, and Nuthan A.C, 2013, "FPGA Based Implementation of Image Encryption Using Scan Patterns and Carrier Images," International Journal of Science and Modern Engineering ,1(7),pp.45-47.
2. Saisubha V, Reenu R, Priyanka U,and Remya R, 2013,"Image encryption using SCAN pattern," Proceedings of AECE-IRAJ International Conference, Tirupati, India,pp.25-28.
3. Weiming Zhang, Kede Ma and Xianfeng Zhao,2013, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security,8(3), pp. 553-562.
4. W. Hong, T. Chen, and H. Wu, 2012, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett.,19(4), pp. 199-202.
5. X. Zhang, 2012, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security,7(2), pp. 826-832.
6. X. Zhang, 2011, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., 18(4), pp. 255-258.
7. Panduranga H.T, Naveen kumar S.K, 2010,"Hybrid approach for Image encryption using SCAN patterns and carrier images," International Journal on Computer science & Engineering, 2(2), pp.297-300.
8. J.Tian, 2003, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., 13(8), pp. 890-896.