Special Issue of Engineering and Scientific International Journal ISSN 2394-187(Online) ISSN 2394-7179 (Print)
*Proceedings of the UGC Sponsored - National Conference on "**Recent Statistical Computing Techniques and their Applications**"*
Department of Statistics and Department of Computer Science, Ramanujan College,University of Delhi, Delhi.
March 11-12, 2016. ***Published on January 2017***

Secure Image Encryption Algorithm Based on Playfair using Multiple Secret Keys, Scan Pattern and Pix Transformation

Bhavya Ahuja

Ramanujan College (University of Delhi), Kalkaji, New Delhi, India
success_bhavya19@yahoo.com

Abstract— Image encryption is a scheme designed to ensure that the image is securely shared between a sender and the intended receiver. Encryption encodes the image so that no adversary can interpret its content. In this paper, an image encryption scheme has been proposed based on the simple monoalphabetic polygraphic substitution cipher – Playfair. The intention is to achieve a completely scrambled encrypted image utilizing the benefits of Playfair's simplicity, security and high throughput. To achieve this, the algorithm additionally incorporates usage of several secure mechanisms which are XOR operation with a key, multiple secret key generation for encryption, scan patterns to select pixel value pairs for encryption and pixel value transformations. The algorithm uses the transformations used in the rounds of AES to generate multiple keys so that there is minimum correlation between the keys used for different blocks attributed to the properties of these transformations. The algorithm has been designed to give good results with all types of images; especially focusing on those with uniform background. The proposed cryptosystem is designed to offer security, simplicity and speed. Measures like histogram analysis and correlation coefficient show that the system is able to produce good encryption results. Also the decrypted image is similar in quality to the original image as shown by the PSNR and SSIM.

Keywords— Cryptography; Playfair Cipher; Image Encryption; Scan Pattern, AES; Pix Transformation.

1. Introduction

In the present scenario, security over communication media has become imperative. Interception of the network poses serious concern in case of confidential communication of data like text, images, audio etc. One of the security mechanisms is encryption which involves encoding the original message referred to as plain text into non-readable form, a coded message known as ciphertext so that it would not be interpreted by any eavesdropper. The receiver of the encrypted text then using a secret key retrieves the message sent in plain text form.

Substitution cipher is one of the basic techniques of encryption in which units of plaintext are substituted with ciphertext according to a regular system; the units comprise of mono, pairs, triplets of letters or their mixtures. The receiver of the ciphertext, then finds the original message by applying an inverse substitution on the cipher-text. The units of the plaintext are retained in the same sequence as in the ciphertext, but the units themselves are altered.

A polygraphic cipher operates on large group of letters. A monoalphabetic polygraphic substitution cipher Playfair has been used for image encryption in the proposed algorithm. The cipher has several advantages, such as disguising letter frequencies of the plaintext making frequency analysis attack difficult, simplicity, high speed and high throughput. Playfair has been used before in encryption of images[1,8]. In this paper, an algorithm is proposed to design a security mechanism using Playfair to encrypt digital images incorporating additional security mechanisms to devise a simple secure and fast system. The algorithm uses a Key Generation Method to generate multiple keys for encrypting each block of the image enhancing security, a scan pattern to form pixel pairs for encryption and applies pix transformations. The algorithm has been shown to perform well on grayscale images and can be easily extended to work with color images.

The organization of the paper is as follows. Following the introduction, the basic concept of Playfair cipher is outlined in Section 2. Section 3 discusses the proposed method for encrypting and decrypting the images. Section 4 summarises the experimental results obtained by application of the proposed algorithm.

2. Playfair Cipher

The Playfair cipher is a symmetric substitution cipher developed by Charles Wheatstone in 1854. The cipher encrypts pairs of letters or digraphs. The technique uses a 5X5 matrix constructed using a keyword. Below is an example:

S	O	L	A	C
E	B	D	F	G
H	I/J	K	M	N
P	Q	R	T	U
V	W	X	Y	Z

The keyword used in this case is Monarchy. First the matrix is filled with the keyword and then rest of the letters

are filled in from left to right. The encryption process is as follows:

- The plain text is first pre-processed. All whitespace characters are removed. The text is divided into pairs; if both the characters in a pair are same, then a filler character like 'X' is placed in between like 'ddc' is replaced by 'dx' and 'dc'. All the J's and I's are treated equivalently.
- Two plaintext letters in the same row of the matrix are replaced with the letter on its immediate right in the matrix. For the last element in the row, the first element of that row is used. For example, 'FG' is replaced by 'GE'.
- Two letters of the message in the same column are each replaced by the letter below, with the top element of the column circularly following the last. For example, 'SV' is encrypted as 'ES'.
- Otherwise, each letter of the pair in the plaintext is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter of the pair. Thus, 'BU' becomes 'GQ' and 'AP' becomes 'ST'.

Decryption is done following the reverse way.

- The cipher text is first divided into pairs.
- Two ciphertext letters lying in the same row are replaced by a letter on the left, the first element of the row circularly following the last.
- Two ciphertext letters in the same column are each replaced by the letter above, with the top element being replaced by the last element of the same column.
- Otherwise each ciphertext letter of the pair is replaced by a letter lying in its own row and other letter's column.

The Playfair cipher poses great improvement over simple monoalphabetic ciphers. With 26 English alphabets, there are 26 x 26 = 676 digraphs, so that identification of individual digraphs becomes cumbersome. Furthermore, it makes frequency analysis difficult as there is higher variation in relative frequencies of individual letters than digraphs. In this paper, playfair cipher is used for encryption of image pixel values. The matrix is of size 16X16 consisting of values 0-255.

3. Proposed Image Encryption Algorithm

In this section, an encryption scheme is proposed based on Playfair Cipher involving:

- XOR operation with a key,
- Multiple secret key generation (derived from AES),
- Encryption in order specified by scan pattern,
- Pix transformation.

The scheme intends to develop a secure, fast encryption algorithm producing an image that has no perceivable patterns even for images with uniform background. Fig. 1 demonstrates the pseudocode for the proposed algorithm.

3.1 Image Encryption by Playfair

In the proposed scheme, Playfair cipher is used to encrypt pairs of pixels from the 8X8 blocks of the image. First, the pixel values in each block are XORed with the XORing key. To improve the secrecy of the system, the pixels are chosen using a zigzag scan of the 8X8 block. An 8X8 zigzag-scan key is generated randomly containing values from 1-64. Each time the pair of pixel values is chosen by using the indexes obtained by scanning this key hence introducing pixel value rearrangement. For instance, for the given key,
Zigzag-scan key =

1	2	3	4	5	6	7	8	
23	55	63	21	64	35	7	2	1
41	34	26	19	44	15	45	4	2
17	11	42	38	33	8	40	28	3
36	29	30	27	60	10	22	54	4
9	39	59	57	53	6	1	14	5
31	61	48	13	24	5	50	25	6
56	52	32	37	51	62	46	43	7
18	20	47	49	16	3	58	12	8

The first pixel value pair used is (5,7) and (1,8). The next pixel pair is (8,6) and (2,8) and so on. Once the pair indexes are obtained, actual values in these indexes in the image block are compared for equality. In case they are equal, then playfair cannot be applied. Hence a pix transformation is done in which the second pixel value is incremented by 1. If the value becomes256, then it is decremented to remove the equality. This would result in getting a different pixel value while decryption but the change would not be perceptible utilizing the limitations of human visual system.

After this the secret key for the block is generated (section 3.2) and the pixel value pair is encrypted using playfair scheme utilizing this key. But this brings forward another consideration. If the block is uniform, it may result in the same pixel values in every pair, hence resulting in the same pixel values after encryption for the both the pairs. For instance, given the secret key and the block given in Fig. 2, pairs 1 and 2, both would result in new pixel value pairs: (181,168). This would lead to recognizable patterns in the encrypted image. To remove this problem, a pair is used only once. If the same pixel values are encountered again, then pix transformation is used and the second pixel value of the pair is incremented

till either we get an unused pair or the value becomes 256.

```
Input: The image to be encrypted
Output: The Encrypted image Begin
        Randomly generate key to be used for XORing: XORing-key and zigzag-scan key Divide the image into 8X8
        blocks
        Do for each block
                XOR the values in the block with the XORing-key Generate
                a secret key for encryption of the block Select pixel value
                pairs using zigzag-scan key
                Encrypt pairs of pixel values using playfair cipher applying pix
                transformation if required
        Endo
        Create a new image with these new pixel values
End
```

Fig. 1: Pseudocode for proposed image encryption algorithm

In the first case, the pair is encrypted using the key. In the second case, the value is decremented by the same amount and further by 1 till again an unused pair is obtained or we get -1. If we get -1, then the same logic is used with the first pixel value. Through this we can ensure that the encrypted image would have no perceptible patterns and be non-uniform.

Playfair Secret Key =

60	35	94	61	0	145	47	237	96	180	201	141	46	123	56	127
111	241	82	158	118	76	85	34	249	14	153	199	213	99	4	66
28	165	25	142	10	90	104	232	69	110	159	246	225	50	188	23
3	113	156	174	78	58	190	253	227	162	251	51	197	255	59	121
112	202	5	17	204	122	168	53	194	45	248	97	164	31	133	250
181	87	247	203	160	73	105	9	101	93	211	64	98	18	234	222
231	208	172	67	40	187	7	236	183	207	16	226	42	186	167	86
198	243	233	229	150	22	189	128	143	216	157	200	120	196	218	88
52	100	37	175	215	21	210	15	223	212	235	177	244	119	140	26
102	108	228	131	72	138	20	193	209	68	182	83	245	166	1	152
240	155	81	38	114	184	221	171	224	151	2	169	252	107	63	54
77	13	217	132	176	146	185	48	117	65	115	147	139	135	129	239
70	206	191	36	8	32	57	19	205	154	109	75	230	27	74	173
103	161	149	106	195	92	137	6	116	134	84	170	43	41	136	12
238	148	124	30	125	192	254	242	44	79	62	126	80	163	11	220
178	39	179	130	33	91	29	144	55	95	49	214	24	89	219	71

Image Block=

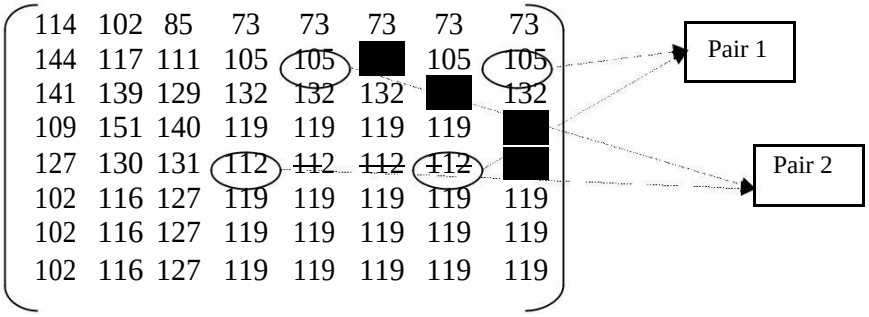


Fig. 2: Example of a secret key and image block to explain encryption

After this the new blocks are used to form the encrypted image which is then transmitted to the receiver along with the zigzag-scan key, secret key used to encrypt the last block and the key used for XORing with each block.

3.2 Key Generation

To make the scheme more secure, every 8X8 block of the image is encrypted using a different 16X16 playfair matrix. To generate these keys, some transformations used in the symmetric block cipher AES [3] are used. The cipher includes ten rounds where each round is composed of the following transformations:

- Substitute Bytes
- Shift Rows
- Mix Columns
- Add Round Key

These transformations were made in AES so as to introduce minimum correlation between input and output bits and the property that the output cannot be described as a simple mathematical function of the input. To utilize the advantages brought in by these transformations, Substitute Bytes and Shift Rows have been used to generate different keys for each image block. First a 16X16 key is randomly generated by the sender consisting of values 0-255. Then for every subsequent image block, Substitute Bytes is applied in which each individual byte of the key is replaced by byte indexed by row (left 4-bits) & column (right 4-bits) of the S-box (a permutation of all possible 256 8-bit values). Then, Shift Rows is applied to the key in which the bytes in the last fifteen rows of the key are cyclically shifted; the offset of the left shift varies from one to fifteen bytes.

3.3 Decryption

The pseudocode for the proposed algorithm's decryption process has been demonstrated in Fig. 3.This is just the reverse of the encryption process. For each block starting from the last, the pixel value pairs are chosen based on the zigzag-scan key and decrypted using the secret key by the applying playfair cipher. The values are then XORed with XORing-key. The decrypted image may have pixel values different from the original image in case pixel value transformations have been applied. But the difference is not perceptible using limitations of HVS as can be seen in the experimental results.

4. Experimental Results

In this section, the simulation results of the proposed encryption algorithm have been presented. The encryption and decryption algorithms are implemented in MATLAB 7.7.0(R2013a). The results for the algorithm are demonstrated in Fig. 4. The more the features of an image are hidden, better the cryptosystem. But mere visual inspection is not a good performance evaluator. A good encryption scheme must be robust against all kinds of cryptanalytic, brute force and statistical attacks. Below is an analysis of the performance of the proposed encryption scheme.

4.1 Histogram analysis

The histogram analysis shows the pixel distribution in an image by plotting the number of pixels at each intensity level. Fig. 4 shows histogram analysis on some test images using proposed algorithm. The histogram of encrypted image has uniform distribution which is considerably different from original image and has no statistical resemblance in appearance. A relatively uniform distribution in the encrypted image's histogram points out good quality of encryption method.

4.2 MSE and PSNR

Mean Square Error (MSE) is the cumulative squared error between original image f and decrypted image f´. A lower value of MSE means less error in decryption of the image. The formula used is given below:

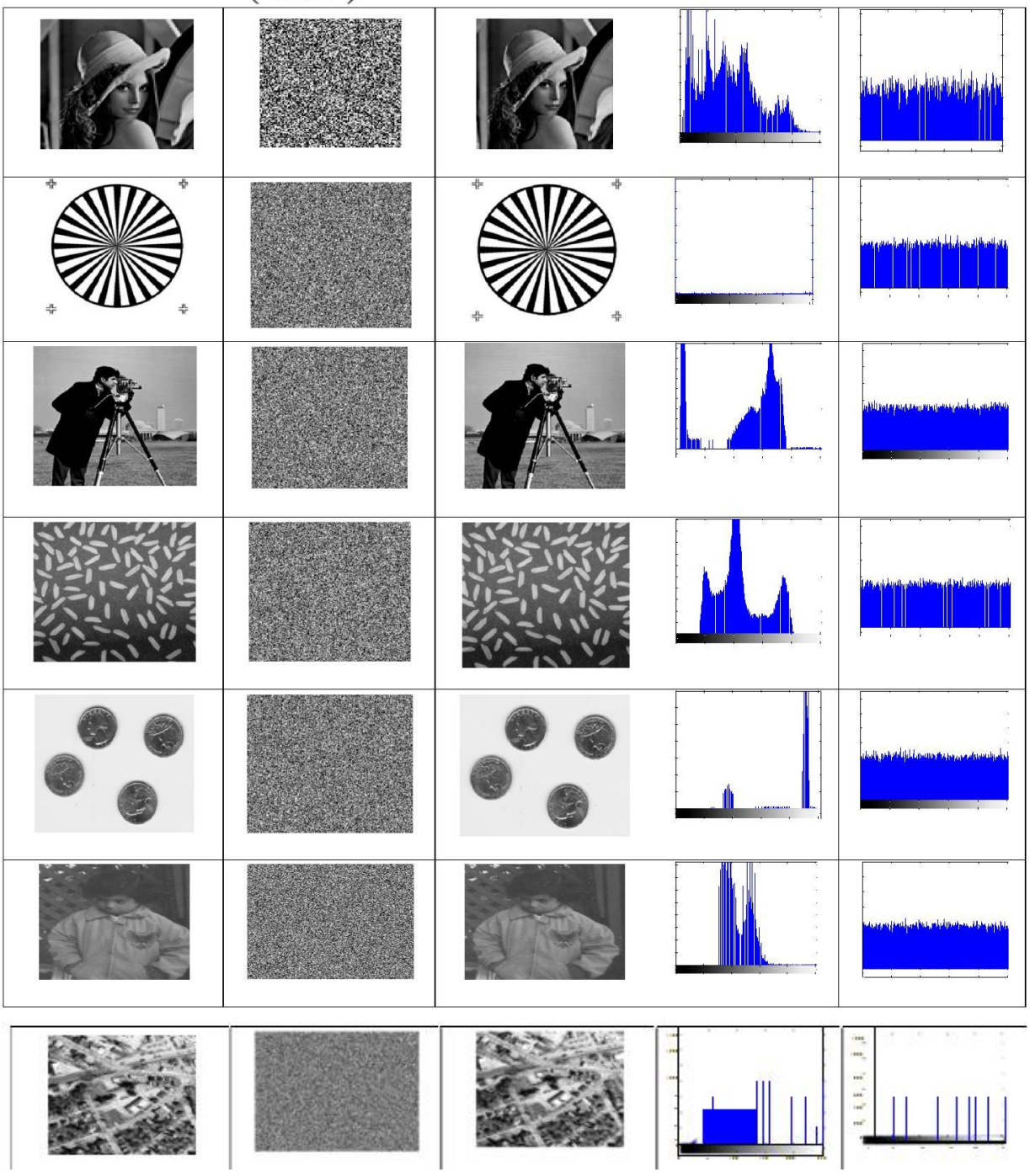
$$MSE = \frac{1}{N.M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[|f(i,j) - f'(i,j)|^2]$$

Input: The image to be decrypted, XORing-key, secret key, zigzagscan-key Output: The Original image
Begin
Divide the image into 8X8 blocks
Do for each block starting from the last Generate the secret key for the block
Decrypt pixel values picking pairs using zigzagscan-key XOR the values in the block with the XORing-key
End
Create the new decrypted image with these new pixel values End

Fig. 3: Pseudocode for proposed image decryption algorithm

The image is of size M X N. Peak Signal to Noise Ratio can be used as a measure of recovered image quality. It is calculated using MSE as:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$



(a) (b) (c) (d) (e)

Fig. 4: Encryption and decryption results using proposed algorithm: (a) Original Image, (b) Encrypted Image, (c) Decrypted Image, (d) Histogram of Original Image, (e) Histogram of Encrypted Image

4.3 Correlation

A good encryption algorithm must generate an encrypted image independent of the original image. So they must have a very low correlation coefficient that is very close to zero. The correlation between original and encrypted image has been calculated and shown in Table 1. A low value of correlation coefficient shows that there is no straight relation between the original and encrypted images. The formula used to calculate correlation coefficient is given as:

$$C.C = \frac{\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(x))^2} \sqrt{\sum_{i=1}^{N} (y_i - E(y))^2}}$$

C.C: correlation coefficient

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i,$$

4.4 Structural Similarity Index Measure (SSIM)

SSIM is a measure that determines the similarity between two images. It is a full reference metric. It is intended to provide better results than methods like PSNR and MSE which have proven to be inconsistent with human eye perception. The metric is computed on various windows of an image. The measure between two windows *x* and *y* of common size *N*×*N* is:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

with μ_x the average of x; μ_y the average of y; σ_x^2 the variance of x, σ_y^2 the variance of y, σ_{xy}.

The resulting SSIM index is a float value between -1 and 1, and value 1 is only reachable in the case of two identical sets of data. SSIM between original and decrypted images has been shown in Table 1. It can be seen that the values are very close to one.

Table. 1: Results of the proposed algorithm on different images

Image	MSE	PSNR	Correlation Coefficient between Original and Encrypted Image	SSIM
Lenna.gif	0.2665	53.8738	0.0086	0.9999
Spokes.png	1.3365	46.8711	0.0019	0.9999
Cameraman.tif	0.1308	56.9653	-1.4425e-04	1.0000
Rice.png	0.0934	58.4267	-0.0020	1.0000
Coins.tif	0.7146	49.5902	-0.0024	0.9999
Pout.tif	0.4828	51.2929	0.0080	0.9996
Map.png	0.1016	58.0616	-0.0014	1.0000

Conclusion

In this paper an image encryption scheme based on playfair cipher is presented. The proposed system uses a different secret key for each block encryption, thereby significantly increasing its resistance to various attacks. The possibility of known plaintext attack is highly reduced as the key used changes with every block.

The XOR operation in the beginning also increases the security of the scheme. The pixel value pairs are chosen using a scan key which leads to pixel value rearrangement. For an image with uniform background, the results are improved due to usage of scan pattern, changing keys and not using the same pair of the secret key while applying playfair. It can be seen that the perceptual difference between close pixel values has been increased. There may be cases in which the decrypted results are not completely similar to the original image when pixel value transformations have been applied. But the difference is not very extreme and visible as shown by the simulation results. Hence the scheme offers a fast, simple and secure technique for digital image communication across unsafe media.

References

[1] Safwat Hamad, Amal Khalifa, Ahmed Elhadad, S. Rida, "A Modified Playfair Cipher for Encrypting Digital Images" J. of Commun. & Comput. Eng., ISSN 2090-6234, Volume 3, Issue 2, 2013, Pages 1:9.
[2] Nisarga Chand, Subhajit Bhattacharyya, "A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1, January 2014.
[3] William Stalling, "Cryptography and Network Security Principles and Practices", Fourth Edition.
[4] R.B. K, S.U. Kumar, A.V. Babu, I. Aditya, P. Komuraiah, "An Extension to Traditional Playfair Cryptographic Method", International Journal of Computer Applications., Vol. 17, No.5, March 2011
[5] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani, "Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009. 1793-8201.
[6] V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhavani, "Modified Playfair Cipher for a Large Block of Plaintext", Inter. Journal of Computer Theory and Engineering, Vol.1, No.5, Dec 2009.
[7] Kallam Ravindra Babu, S.Udaya Kumar, A.Vinaya Babu, "An Improved Playfair Cipher Cryptographic Substitution Algorithm", IJARCS, Volume 2, No-1, January-February 2011, pages: 211to214.
[8] V Saisubha, U Priyanka, K R Remya, R. Reenu, "Image Encryption Using Scan Pattern", Proceedings of AECE-IRAJ Inter. Conference, 14th July 2013, Tirupati, India, ISBN: 978- 81-927147-9-0.
[9] H.T Panduranga, S.K. Naveen Kumar, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images", Inter. Journal on Comput. Science and Engineering, Vol. 02, No.02, 2010, 297-300.

Bhavya Ahuja is MSc in Computer Science from Department of Computer Science, University of Delhi. She finished BSc(H) in Computer Science from University of Delhi. She is presently an Assistant Professor in Department of Computer Science, Ramanujan College, University of Delhi. Her areas of interest include cryptography, information security and data mining.