A Novel Image Encryption Using Calligraphy Based Scan Method and Random Number

T Sivakumar[1] and R Venkatesan[2]
[1] Department of Information Technology
[e-mail: sk@ity.psgtech.ac.in]
[2] Department of Computer Science and Engineering
[e-mail: ramanvenkatesan@yahoo.com]
PSG College of Technology
Coimbatore, Tamilnadu - 641 004, India
*Corresponding author: T Sivakumar

Received October 7, 2014; revised April 10, 2015; accepted May 5, 2015; published June 30, 2015

Abstract

Cryptography provides an effective solution to secure the communication over public networks. The communication over public networks that includes electronic commerce, business and military services, necessitates the requirement of simple and robust encryption techniques. In this paper, a novel image encryption method which employs calligraphy based hybrid scan and random number is presented. The original image is scrambled by pixel position permutation with calligraphy based diagonal and novel calligraphy based scan patterns. The cipher image is obtained by XORing the scrambled image with random numbers. The suggested method resists statistical, differential, entropy, and noise attacks which have been demonstrated with a set of standard images.

***Keywords**: Image encryption, scan pattern, calligraphy based scan, random number, statistical and differential attack analysis*

http://dx.doi.org/10.3837/tiis.2015.06.020 **ISSN : 1976-7277**

1. Introduction

Securing communications over public networks makes fascination commerce activities, transactions and services possible. The need for data privacy and security has increased in digital communication because of increase in security breaches. Transmission of sensitive information over the public networks has increased due to the advancement of computer networking and communication technologies. The growth of multimedia applications like personal photograph album, medical imaging systems, military image communications and confidential video conferences has so many security issues during transmission, storage, and retrieval. Confidential information exchange through open networks can be secured by the methods like steganography and cryptography. Cryptography is used to protect the data transmitted through an insecure network. The data confidentiality is attained by using the process of encryption. Symmetric key encryption and asymmetric key encryption are the two types of encryption methods. In symmetric key scheme, the communicating persons must agree on a secret key before they start to communicate. In asymmetric key scheme, each user uses a pair of keys called as public key and private key. The Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA) are the popular symmetric key algorithms used to protect sensitive data. Because of computational complexity, the asymmetric algorithms are typically used to provide the services like authentication, key exchange, and digital signature.

The key difference between the characteristics of the text and image data is that the size of image is much larger than that of text data. The traditional algorithms are not sufficient to encrypt images due its size, that is is always much greater than text, which increases its the computational cost [1].

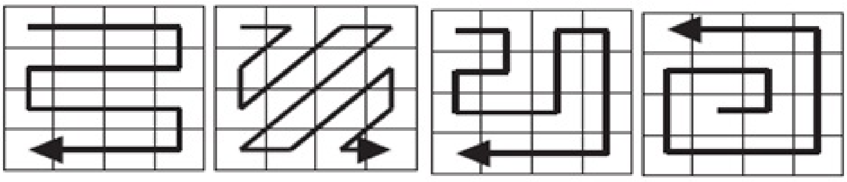
1.1 Image Encryption

Typically, the image encryption algorithms utilize both substitution and permutation to provide confusion and diffusion properties. In diffusion, the attributes of the original image is distributed into distort-level of randomness in the encrypted image and this is achieved by repeatedly performing several permutations. The confusion process seeks to make the relationship between the statistics of the encrypted image and the encryption key as complex as possible and this is achieved by complex substitution methods [1, 2].

The major types of image encryptions based on permutation are classified as bit permutation [3-5], pixel permutation [6-15], and block permutation [16-19]. In bit permutation, the bits of each pixel taken from the image are permuted with the key chosen from the set of keys by using the pseudorandom index generator. In pixel permutation, the pixel position of the image is rearranged using the key selected from the set of keys and the size of pixel group is same as the length of the keys. In block permutation, the image is divided into blocks and these blocks are permuted based on the random key. The edges of the original image does not appear clearly in the encrypted version, if the blocks are very small in size and this leads to better encryption result [20].

1.2 Scan Pattern

Scan pattern is a formal language-based two dimensional spatial-accessing methodology to generate a wide range of scanning paths to permute the pixels of an image. It is also defined as, scanning of a two-dimensional array in which each element of the array is accessed exactly once [6, 7]. The pixels of an original image are permuted to obtain the scrambled image using scan patterns. The scan patterns shown in **Fig. 1** are usually used to permute the pixles of an image.



(a) Raster (b) Diagonal (c) Orthogonal (d) Spiral

Fig. 1. Basic scan patterns

1.3 Calligraphy

Language is a system that consists of symbols and well defined rules. To share information using a language it is necessary that the persons involved in the process should know the symbols and rules of the communicating language. This is similar to the encryption methods used now a day's for information exchange. Calligraphy is an art of writing the characters/symbols of a language. Hence, the Calligraphy based image encryption method can be considered as a novel idea. The sample images of calligraphy are shown in **Fig. 2(a) and (b)**.

(a) Bradley Hand ITC (b) Edwardian Script ITC

Fig. 2. Sample models of Calligraphy

This paper proposes an image encryption method based on scan pattern generated using calligraphy and random number. The rest of the paper is organized as follows. The review of existing image encryption methods are given in section 2. Section 3 describes the proposed image encryption method. The implementation results and analysis are presented in section 4, and section 5 concludes the paper.

2. Literature Survey

Cryptography is necessary when communicating secret information through open networks. Today's cryptographic techniques have become the immediate solution to protect information against attacks. The major security services needed for today's communication era are confidentiality, authentication, key exchange, integrity, and digital signature.

Hongjun Liu et al. [3] proposed an image encryption method using confusion and diffusion techniques. The method permute the pixels by transforming the nucleotide into its base pair for random times, the other is to generate the new keys according to the plain image and the common keys, which can make the initial conditions of the chaotic maps change automatically in every encryption process. After permuting the rows and columns using the arrays generated by piecewise linear chaotic map (PWLCM), each pixel of the original image is encoded into four nucleotides by the deoxyribo nucleic acid (DNA) coding.

Maniccam and Bourbakis (2001) [6] introduced a methodology which performs both lossless compression and encryption of binary and gray-scale images. An overview of SCAN, compression and decompression algorithms, encryption and decryption algorithms and the test results of the methodology are presented. Maniccam and Bourbakis (2004) [7] presented a technique for image and video encryption using SCAN patterns. The image encrypted by SCAN-based permutation of pixels and a substitution rule to form an iterated product cipher.

Khaled Loukhaoukha et al. [8] proposed an image encryption method based on the principle of Rubik's cube. The pixel positions are reordered based on Rubik's cube principle to produce scrambled version of the original image. The bitwise XOR operation is applied to the odd rows and columns and then to even rows and columns of the scrambled image using secret keys to get the cipher image. Avi Dixit et al. [9] suggested an image encryption method using permutation and rotational XOR techniques. Here, 8 bit key is generated using pseudorandom index generator. The pixel decimal value is converted into binary stream which contain 8 bits. Based on the 8 bit key, each pixel of the original image is permuted. Then the entire image is divided into blocks of size 8×8 pixels and the blocks are permutated using same 8 bits key. After that the binary stream is converted into decimal value and considered as cipher image.

Huang et al. [10] adopted the chaotic system as the fundamental base and combined with row, column shuffling to obtain secure encrypted images. Adrian-Viorel Diaconu et al. [12] presented an improved version of the image encryption algorithm using the Rubik's cube principle and a digital chaotic cipher. The method resists exhaustive, differential and statistical attacks but has no immunity to the additive noise and cropping attacks. Panduranga et al. [13] suggested a hybrid technique for image encryption by using carrier image and basic scan patterns. The alphanumeric keyword is used to create the carrier image such that each alphanumeric key will have a unique 8 bit value generated by 4 out of 8-code.

Sathishkumar et al. [14] presented a pixel shuffling, base 64 encoding based algorithm, which is a combination of block permutation, pixel permutation and value transformation. The crypto system uses a simple chaotic map for key generation, and a logistic map was used to generate a pseudo random bit sequence. Huang and Nien [15] proposed a pixel shuffling method for image encryption based on unpredictable character to reduce the exhaustive key search attack by disordering the distributive characteristics of RGB levels. Han Shuihua et al. [17] introduced a novel asymmetric image encryption scheme based on matrix transformation is presented to scramble the original image. A block-based transformation algorithm based on the combination of image transformation and the well known Blowfish algorithm is presented in [18]. The original image is divided into blocks (3×3 pixels, 5×5 pixels and 10×10 pixels) and rearranged into a transformed image using transformation algorithm.

Tzung-Her Chen et al. [21] presented a Random Grids (RG) based Visual Secret Sharing (VSS) scheme with the capability of encrypting multiple secret images at once into only two circular cipher-grids. In order to decrypt the secrets, decoders stack the two circular cipher-grids to disclose the first secret and then gradually rotate one circular cipher-grid at a fixed degree to reveal the second image. Lin and Wang [22] presented an image encryption algorithm based on chaos and piecewise linear memristor in Chua′s circuit. Image scrambling and pixel replacement are the two main operations in this encryption algorithm. The chaos-based image encryption methods offer limited security due to small key space.

Jawad Ahmad et al. [23] established a framework to evaluate the efficiency of image encryption schemes based on the parameters correlation, information entropy, histogram, peak signal-to-noise ratio, number of pixel change rate (NPCR) and unified average change intensity (UACI). Yue Wu et al. [24] established a mathematical model for ideally encrypted images to evaluate the strength of image encryption algorithms using NPCR and UACI test.

Chen W et al. [25] presented a method for optical image encryption using multilevel Arnold transform and rotatable phase-mask noninterferometric imaging. The image encryption scheme is developed in the gyrator transform domain, and one phase-only mask is rotated and updated during image encryption. For the decryption, an iterative retrieval algorithm is used to extract high-quality plainimages. This optical encoding scheme can effectively eliminate security deficiency and significantly enhance cryptosystem security. Chen W et al. [26] proposed a novel method to enhance the security for conventional interference-based optical image encryption in the fractional Fourier transform domain. A series of random and fixed phase-only masks is used in the optical paths, and subsequently interference principle is applied to extract two phase-only masks during encryption. Feasibility and effectiveness of the method is demonstrated by computer simulations. The result demonstrates that the method is simple, effective, and the security of conventional interference-based optical cryptosystem can be dramatically enhanced. Chen W et al. [27] made a review of optical technologies for information security with the theoretical principles and implementation examples to illustrate each optical security system. The authors also discussed the advantages and potential weaknesses of each optical security system. The review not only provide a clear picture about the current development in optical security system but also shed some light on future developments.

The optical method has emerged as an effective and powerful tool for image encryption due to it multidimensional and multiparameter capabilities. Information security with optical means, advantages and potential weaknesses of each optical security systems are analyzed and discussed in the recent research works [25-27]. To deal with optical encryption systems, researchers need to possess competent knowledge in optical signal processing, image processing, optical theories, and computer technologies. Also requires a number of optical systems to be designed for practical implementation of optical encryption schemes which incur considerable amount of money. Because of the expertise knowledge requirement in multiple high end technologies and implementation cost it is not readily usable for all users.

Thus, the image encryption methods based on bit permutation, pixel permutation and block permutation, chaos and optical systems have been studied and it is observed that the existing encryption methods based on pixel permutation are not secure against all types of security attacks. In this paper, a novel image encryption method using Calligraphy based scan pattern and random number is proposed to improve the security.

3. The Proposed Image Encryption Method

The pixel position of the original image is permuted with Calligraphy based diagonal scan and the calligraphy based scan to obtain the scrambled image. Both scans are accomplished with the support of secret keyword. The secret keyword is a symmetric key shared by the communicating persons to carry out the encryption and decryption processes. The pixel value of the scrambled image is XORed with random numbers generated by using Blum Blum Shub (BBS) generator. The BBS generator is chosen because of its cryptographic strength [2]. The block diagram which indicates the various stages of the proposed image encryption and decryption is shown in Fig. 3.

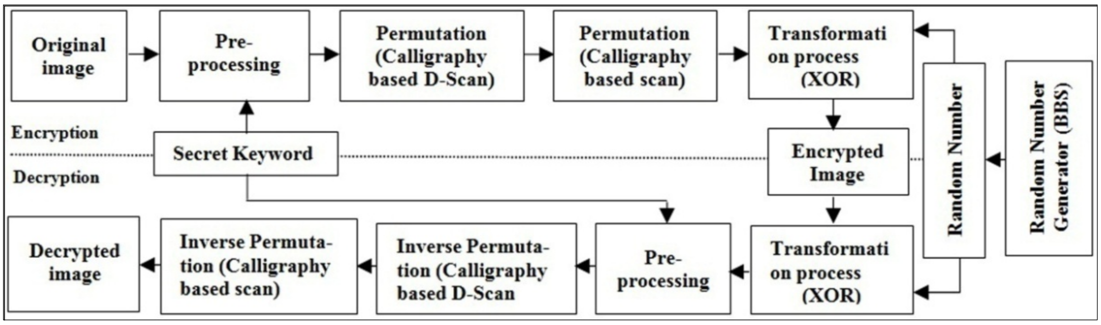

Original image
Pre-processing
Permutation (Calligraphy based D-Scan)
Permutation (Calligraphy based scan)
Transformati on process (XOR)
Encryption
Decryption
Secret Keyword
Encrypted Image
Random Number
Random Number Generator (BBS)
Decrypted image
Inverse Permuta-tion (Calligraphy based scan)
Inverse Permuta-tion (Calligraphy based D-Scan
Pre-processing
Transformati on process (XOR)

Fig. 3. Block diagram of proposed method

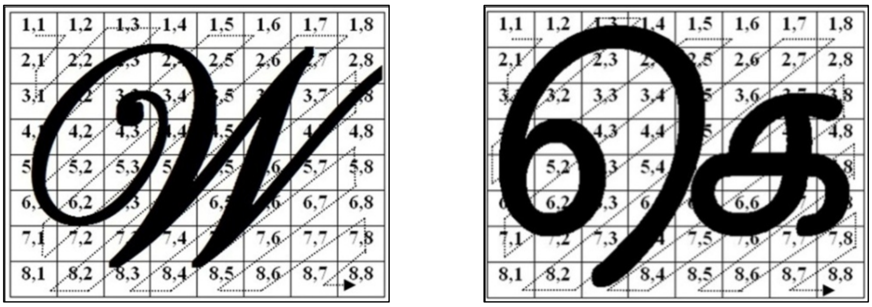
The propsoed method consists of three stages namely, pre-processing, pixel permutation with Calligraphy based diagonal scan, pixel permutation with Calligraphy based scan, and transformation process. For real time implementation, the sender and receiver must have the same calligraphy database. The volume of system memory utilized for maintaining the calligraphy database at their receptive terminal is very small. The various stages are discussed in the following sub sections with illustration.

3.1 Pre-processing

In the pre-processing stage, the characters of the secret keyword are embedded on the image such that each character will occupies b×b pixels of the original image matrix. If the length of the secret keyword is not sufficient to cover the blocks of the entire image then the characters of the keyword will get repeated. The pixels which overlap with the character segment is considered as hit pixels and the left over pixels are considered as un-hit pixels. For example, in Fig. 4(a) the pixel at the location (3, 2) is considered as hit pixel and the pixel at location (1, 2) is considered as un-hit pixel. The characters of the secret keyword should be chosen such that the number of hit pixels must be grater than un-hit pixels for better result. The unlimited number of calligraphy fonts can be considered for secret keyword by excluding the simple characters like dot (.), comma (,), vertical bar (|), and number 1 etc.

3.2 Pixel Permutation with Calligraphy based Diagonal Scan

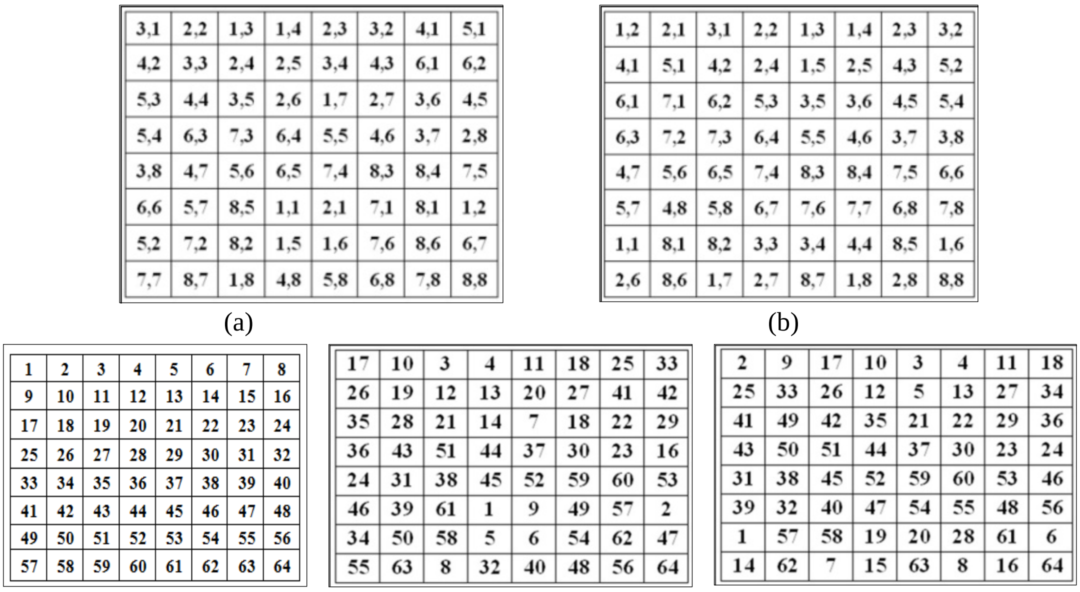
In this permutation stage, the Calligraphy scan is combined with the diagonal scan to permute the pixels. The calligraphy based diagonal scan is performed on the entire image to reorder the pixels hit by the characters of the keyword. Then, the un-hit pixels are read column wise and placed row wise in the scrambled image matrix. This scan is presented by assuming the first character of the keyword as the English letter 𝒲 (Edwardian Script ITC) and for the Tamil letter **T** (Appar1) in Fig. 4(a) and Fig. 4(b) respectively.



(a) English letter 𝒲 (b) Tamil letter T

Fig. 4. Illustration of Calligraphy based diagonal scan

The scan paths generated with the calligraphy based diagonal scan for the letters 𝒲 and T are shown as co-ordinates in **Fig. 5(a)** and **Fig. 5(b)**. The input image taken for encryption is shown **Fig. 5(c)** as a 8×8 matrix**.** The scrambled image matrix obtained by using the scan path generated with 𝒲 is shown in **Fig. 5(d).** The scrambled image matrix obtained by using the scan path generated with T is shown in **Fig. 5(e).** From the result it is seen that the given input image is scrambled for an acceptable level.



3,1	2,2	1,3	1,4	2,3	3,2	4,1	5,1
4,2	3,3	2,4	2,5	3,4	4,3	6,1	6,2
5,3	4,4	3,5	2,6	1,7	2,7	3,6	4,5
5,4	6,3	7,3	6,4	5,5	4,6	3,7	2,8
3,8	4,7	5,6	6,5	7,4	8,3	8,4	7,5
6,6	5,7	8,5	1,1	2,1	7,1	8,1	1,2
5,2	7,2	8,2	1,5	1,6	7,6	8,6	6,7
7,7	8,7	1,8	4,8	5,8	6,8	7,8	8,8

(a)

1,2	2,1	3,1	2,2	1,3	1,4	2,3	3,2
4,1	5,1	4,2	2,4	1,5	2,5	4,3	5,2
6,1	7,1	6,2	5,3	3,5	3,6	4,5	5,4
6,3	7,2	7,3	6,4	5,5	4,6	3,7	3,8
4,7	5,6	6,5	7,4	8,3	8,4	7,5	6,6
5,7	4,8	5,8	6,7	7,6	7,7	6,8	7,8
1,1	8,1	8,2	3,3	3,4	4,4	8,5	1,6
2,6	8,6	1,7	2,7	8,7	1,8	2,8	8,8

(b)

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

(c)

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

(d)

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

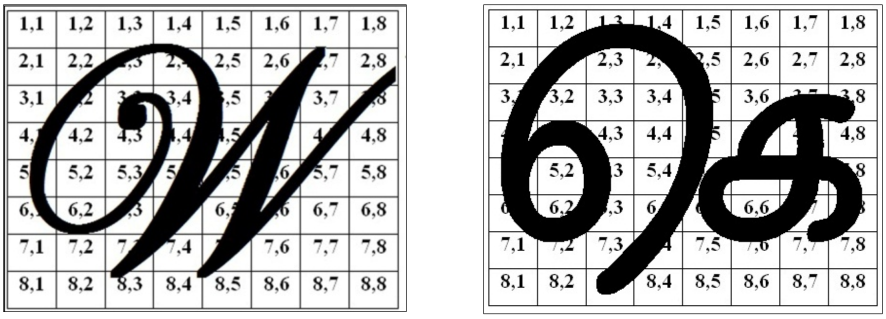
(e)

(a) Scan path obtained with 𝒲, (b) Scan path obtained with T, (c) Input image matrix, (d) Scrambled image obtained using scan path derived from 𝒲 and (e) Scrambled image obtained using scan path derived from T

Fig. 5. Result of Calligraphy based diagonal scan

3.3 Pixel Permutation with Calligraphy based Scan

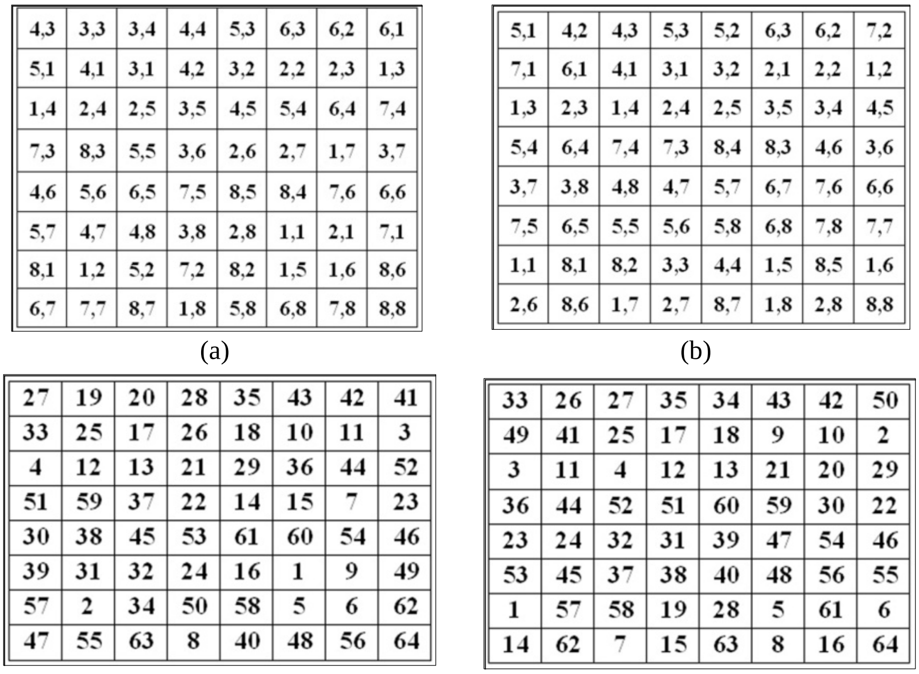
The novel calligraphy based scan pattern is used to permute the pixel positions by the way of writing a character by human. First, the hit-pixels are reordered and then the un-hit pixels are read column-wise from the input image and placed row-wise in the scrambled image. The pixel reordering based on calligraphy is shown for the English letter 𝒲 and the Tamil letter T in **Fig. 6(a)** and **Fig. 6(b)**.



(a) English letter $\mathcal{W}$ (b) Tamil letter **T**

Fig. 6. Illustration of Calligraphy based scan

The scan paths generated with calligraphy based method for the letters $\mathcal{W}$ and **T** are shown in **Fig. 7(a)** and **Fig. 7(b)**. The image matrix shown in **Fig. 5(c)** is taken as input for encryption. The resultant scrambled image obtained by using the scan path generated with $\mathcal{W}$ is shown in **Fig. 7(c)** and the scrambled image obtained by using the scan path generated with T is shown in **Fig. 7(d).** From the result it is confirmed that the proposed calligraphy based scan pattern is more suitable for pixel permutation.



4,3	3,3	3,4	4,4	5,3	6,3	6,2	6,1
5,1	4,1	3,1	4,2	3,2	2,2	2,3	1,3
1,4	2,4	2,5	3,5	4,5	5,4	6,4	7,4
7,3	8,3	5,5	3,6	2,6	2,7	1,7	3,7
4,6	5,6	6,5	7,5	8,5	8,4	7,6	6,6
5,7	4,7	4,8	3,8	2,8	1,1	2,1	7,1
8,1	1,2	5,2	7,2	8,2	1,5	1,6	8,6
6,7	7,7	8,7	1,8	5,8	6,8	7,8	8,8

(a)

5,1	4,2	4,3	5,3	5,2	6,3	6,2	7,2
7,1	6,1	4,1	3,1	3,2	2,1	2,2	1,2
1,3	2,3	1,4	2,4	2,5	3,5	3,4	4,5
5,4	6,4	7,4	7,3	8,4	8,3	4,6	3,6
3,7	3,8	4,8	4,7	5,7	6,7	7,6	6,6
7,5	6,5	5,5	5,6	5,8	6,8	7,8	7,7
1,1	8,1	8,2	3,3	4,4	1,5	8,5	1,6
2,6	8,6	1,7	2,7	8,7	1,8	2,8	8,8

(b)

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

(c)

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

(d)

(a) Scan path obtained with the letter $\mathcal{W}$, (b) Scan path obtained with the letter **T** (c) Scrambled image obtained by using scan path of $\mathcal{W}$ (d) Scrambled image obtained by using scan path of **T**

Fig. 7. Result of Calligraphy based scan

3.4 Transformation Process

In transformation process, the pixel values of the scrambled image are altered bitwise by using XOR operation to obtain the cipher image. The Blum Blum Shub (BBS) pseudorandom number generator is used to generate the random number. The BBS generator produces a sequence of bits according to the following algorithm [2].

```
$X_0 = S^2 \bmod n$
for $i = 1$ to $\infty$
    $X_i = (X_{i-1})^2 \bmod n$
    $B_i = X_i \bmod 2$
```

Where, *S* is the seed value and *n* is the product of two prime numbers (*p* and *q*). Both *p* and *q* have a remainder of 3 when divided by 4 and *S* is relatively prime to *n*.

3.5 Encryption Algorithm

In this section, the sequence of steps required for the proposed encryption method to convert the original image into cipher image is presented.

Input: Original image, Secret keyword, Block size, and Seed values for BBS
Output: Cipher image

The following are the sequence of steps:

Step 1: Input the original image and the secret keyword.
Step 2: Input the seed value (*S*) and two prime numbers (*p* and *q*).
Step 3: Embed the characters of the secret keyword such that each character occupies b×b pixels of the original image.
Step 4: Perform pixel permutation with calligraphy based diagonal scan on the entire image.
Step 5: Perform pixel permutation with calligraphy based scan on each block.
Step 6: Generate random number by using the BBS generator.
Step 7: Obtain the cipher image by XORing the scrambled image obtained in step 5 and the random number generated in step 6.
Step 8: Store the cipher image.

In the encryption algorithm, the steps 4 and 5 produce the scrambled image and step 7 produces the cipher image. For ex1perimental purpose, *n* is chosen as 256 and *b* as 16 and thus the required length of the secret keyword is 256 characters. The characters of the secret keyword can be repeated if the input keyword contains less number of characters.

3.6 Decryption Algorithm

In this section, the sequence of steps required for the decryption to retrieve the original image from the cipher image is presented. The decryption process is the inverse of the encryption process.

Input: Cipher image, Secret keyword and Seed values for BBS
Output: Decrypted image

The following are the sequence of steps:

Step 1: Input the cipher image and the secret keyword.
Step 2: Input the seed value (*S*) and two prime numbers (*p* and *q*).
Step 3: Select the scan paths corresponding to the characters of the secret keyword.

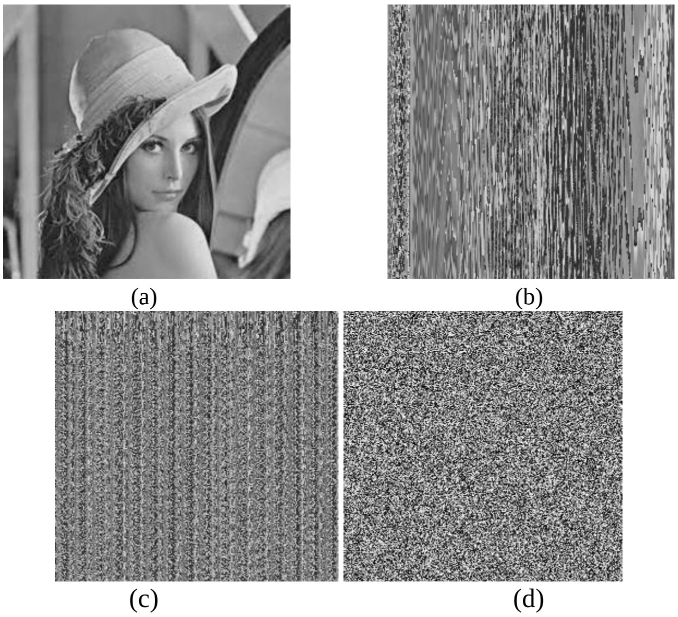
Step 4: Perform inverse pixel permutation with calligraphy based diagonal scan on th entire image.
Step 5: Perform inverse pixel permutation with calligraphy based scan on each block.
Step 6: Generate random number by using BBS generator.
Step 7: Perform bitwise XOR operation between the random numbers and the output obtained in step 5 to get the decrypted image.
Step 8: Store the decrypted image.

In the above algorithm, steps 4 and 5 perform the inverse pixel permuation of the encryption process and step 7 produces the decrypted image.

4. Experimental Results and Analysis

To confirm the effectiveness of the proposed encryption method the evaluation metrics are measured and analyzed with standard test images of size 256×256 pixels and the results are presented by using the Lena, Baboon, Cameraman, and Peppers images. The experiment is implemented in Matlab 2010a with Intel Core i3 Duo Processor, 2 GB RAM, 160 GB Hard Disk Drives, Clock Speed is 2 GHz, and Windows 7 Operating System.

The obtained step-by-step result of the proposed image encryption method is presented for Lena image using the font name Edwardian Script ITC and secret keyword **“**ABQ@#$&WR6**”** which consists of alphabets, numbers and special characters. The input Lena image is shown in **Fig. 8(a)**. The initial scrambled image obtained after applying the secret keyword based scan is shown in **Fig. 8(b)**. The highly scrambled image obtained with the novel calligraphy based scan is shown in **Fig. 8(c)**. The resultant cipher image obtained by XORing the scrambled image with the random number is shown in **Fig. 8(d)**.



(a) Input Lena image (b) Scrambled image by using Calligraphy based diagonal scan
(c) Scrambled image after Calligraphy based scan (d) Encrypted Lena image

Fig. 8. Result of proposed image encryption method

The decryption process is carried out and the obtained correlation between the original Lena image and the decrypted Lena image is 0.9997. Also the test images Baboon, Cameraman, and Peppers with the same secret keyword are tested and observed encouraging results.

4.1 Visual Testing

The perceptual relationship between the original image and the corresponding encrypted image should be reduced after the encryption process. That is, the encrypted image should be completely different from its original version. To quantify this requirement, the evaluation parameters such as Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) should be determined and analyzed [8].

4.1.1 Number of Pixel Change Rate (NPCR)

The NPCR indicates the percentage of difference in pixels between two images. For the original image $I_o(i, j)$ and the encrypted image $I_{enc}(i, j)$, the mathematical formula to compute the NPCR value is given in equation (1) [23].

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{1}$$

Where, W and H are the width and height of the images, $I_o(i, j)$ is the pixel at ith row and jth column of the original image, and $I_{enc}(i, j)$ is the pixel at ith row and jth column of the encrypted image. If $I_o(i, j)$ is equal to $I_{enc}(i, j)$, then $D(i, j) = 0$; else $D(i, j) = 1$. The algorithm is considered as better when obtained NPCR value is greater than 99.5% [24]. The NPCR value obtained by the proposed method and few existing image encryption methods are given in **Table 1**.

Table 1. Comparison of NPCR value

Encryption Method	NPCR Value (in %)
Proposed	Lena: 99.6277 Cman: 99.6460
Khaled Koukhaoukha et al. [8]	99.5850
C.K. Huang et al. [10]	99.5400
Adrian Viorel Diaconu et al. [12]	99.6120
Kamlesh Gupta et al. [28]	99.6300

From **Table 1**, it is observed that the NPCR value obtained by the proposed method is optimal, better than the methods in [8, 10, 12] and very close to the method [28].

4.1.2 Unified Average Changing Intensity (UACI)

The UACI measure is used to identify the average intensity difference in pixels between two images. For the plain image $I_o(i, j)$ and encrypted image $I_{enc}(i, j)$ the equation (2) gives the mathematical formula to compute the UACI value [23].

$$\text{UACI} = \frac{1}{W \times H} \left[\sum_{i,j} \frac{Io(i,j) - Ienc(i,j)}{255}\right] \times 100\% \tag{2}$$

Where, W and H are the width and height of the images, $I_o(i, j)$ is the pixel at ith row and jth column of the original image, and $I_{enc}(i, j)$ is the pixel at ith row and jth column of the encrypted image. The encryption algorithm is better when obtained UACI value is around 33% [24]. The UACI value obtained by the proposed method and the existing image encryption methods are given in **Table 2**.

Table 2. Comparison of UACI value

Encryption Method	**UACI Value (in %)**
Proposed	Lena : 28.7294 Cman: 31.3903
Khaled Koukhaoukha et al. [8]	28.6201
C.K. Huang et al. [10]	28.2700
Adrian Viorel Diaconu et al. [12]	30.5997
Kamlesh Gupta et al. [28]	28.8700

From **Table 2**, it is found that the UACI value obtained by the proposed method is acceptable and matches with those methods in [8, 10, 12, 28]. Both NPCR and UACI results confirms that the proposed method resists the differential attacks for an acceptable level.

4.2 Key Sensibility Analysis

A small change in the original image or key should cause significant change in the encrypted image. In order to confirm this property, the proposed method is tested with small change in the secret keyword and the obtained output is given in **Table 3**.

Table 3. Sensibility of secret keyword

Original Image	**Between Scrambled Images**		**Between Encrypted Images**	
	NPCR (in %) C_1**Vs** C_2	**UACI (in %)** C_1**Vs** C_2	**NPCR (in %)** C_1**Vs** C_2	**UACI (in %)** C_1**Vs** C_2
Lena	99.1531	19.5670	99.1333	29.3731
Cameraman	98.7579	22.2598	98.8693	25.8879
Baboon	99.2477	18.4956	99.2950	30.0912

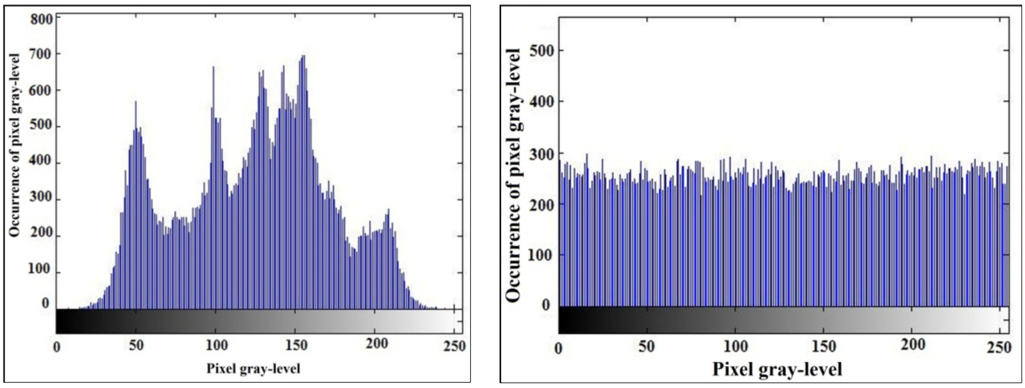
Where, C_1 is the cipher image encrypted using the secret keyword "ABQ@#$&WR6" and C_2 is the cipher image encrypted using the secret keyword "ABQ@#WR6". The specific bits difference between the secret keywords is 19. From the result, it is confirmed that the proposed method has significant key sensibility with respect to the secret keyword.

4.3 Statistical Analysis

It is possible to break the image encryption methods by statistical analysis. This is done by analyzing the histogram and the correlation between the adjacent pixels of the encrypted image. The evaluation parameters such as histogram and correlation are examined to confirm the resistance of the proposed method against statistical attacks.

4.3.1 Histogram Analysis

It is important to ensure that the encrypted and the original images do not have any statistical similarities. The histogram analysis reveals how the pixel values of an image is distributed before and after the encryption process. The histogram of an original image contains great rises followed by sharp declines but the histogram of the encrypted image should be flat. The histogram of the original and the corresponding encrypted Lena image is shown in **Fig. 9(a)** and **Fig. 9(b)**.



(a) Original Lena image (b) Encrypted Lena image

Fig. 9. Histogram of original and encrypted images

The histogram of the encrypted image is flat and the gray-scale values are uniformly distributed over the entire cipher image. Thus, the proposed method resists the statistical attacks based on analysis of histogram of an encrypted image.

4.3.2 Correlation coefficient

The correlation coefficient is a useful measure to judge the security level of any image cryptosystem. It is used to find the degree of similarity between the original and the corresponding encrypted images and between adjacent pixels of the encrypted image. An arbitrarily chosen pixel in an original image is strongly correlated with adjacent pixels, in horizontal, vertical and diagonal directions. A secure image encryption algorithm must produce an encrypted image having minimum correlation between adjacent pixels in all the directions. The correlation co-efficient is computed by using the equations (3) to (6).

$$\boldsymbol{\gamma}_{\mathbf{xy}} = \frac{\boldsymbol{Cov(x,y)}}{\sqrt{\boldsymbol{D(x)}}\sqrt{\boldsymbol{D(y)}}} \tag{3}$$

$$\mathbf{Cov(x,y)}= \frac{\mathbf{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}}\big(\boldsymbol{x_i} - \boldsymbol{E(x)}\big)(\boldsymbol{y_i} - \boldsymbol{E(y)}) \tag{4}$$

$$\boldsymbol{D(x)} = \frac{\mathbf{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}}(\boldsymbol{x_i} - \boldsymbol{E(x)})\,\ddot{\boldsymbol{\imath}} \tag{5}$$

$$\boldsymbol{E(x)} = \frac{\mathbf{1}}{\boldsymbol{N}}\sum_{\boldsymbol{i=1}}^{\boldsymbol{N}}\boldsymbol{x_i} \tag{6}$$

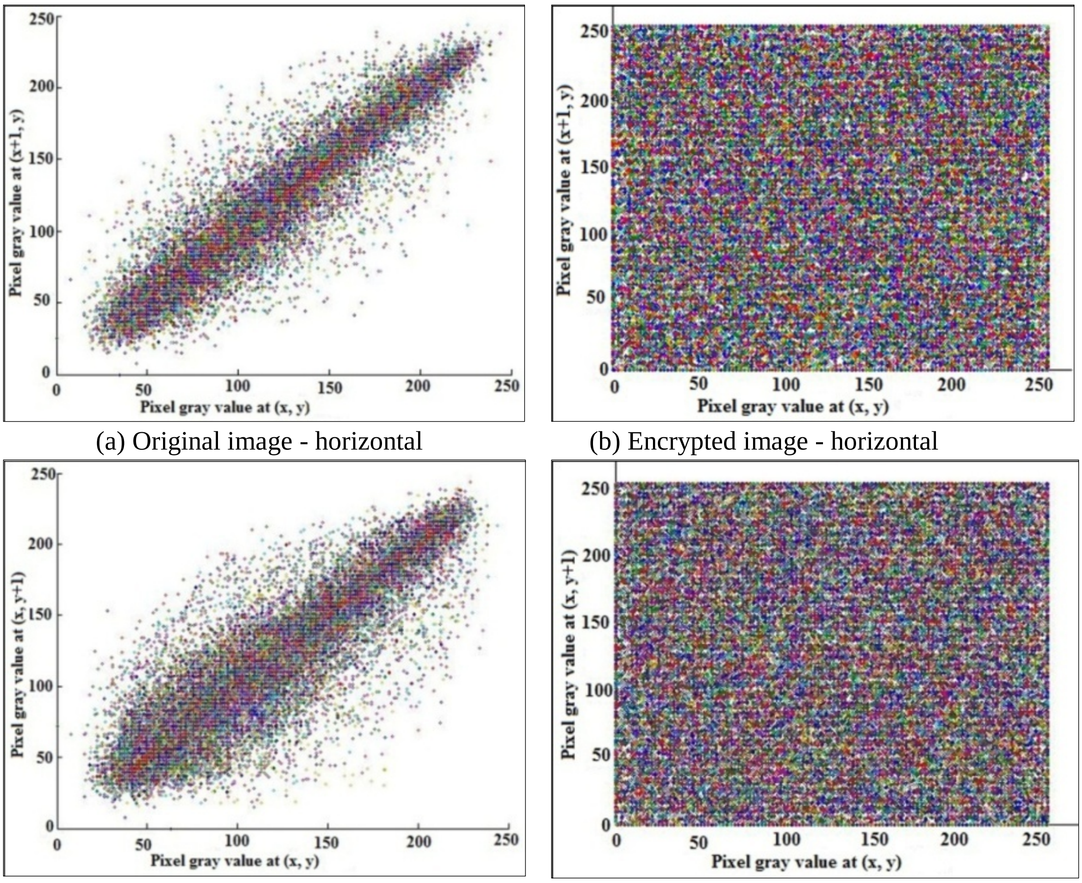
Where, Cov(*x*,*y*) is the covariance between *x* and *y*; *N* is the number of pixel pairs (x_i, y_i), and E(*x*) and D(*x*) are the mean and standard deviation of the pixel values of x_i and y_i respectively. The comparison of adjacent pixel correlation obtained by the proposed image encryption method and the existing methods are given in **Table 4**.

Table 4. Comparison of adjacent pixel correlation value

Encryption Methods	Directions		
	Horizontal	**Vertical**	**Diagonal**
Proposed	0.0101	0.0044	0.0006
Qiang Zhang et al. [4]	0.1366	0.0166	0.0021
Liang Zhao et al. [5]	0.0199	0.0431	-0.0034
KhaledKoukhaoukha et al. [8]	0.0068	0.0091	0.0063
Reza Moradi Rad et al. [11]	-0.0009	-0.0101	-0.0023
Adrian Viorel Diaconu et al. [12]	0.0002	0.0006	0.0043
C. K. Huang et al. [15]	0.01776	0.04912	0.00348
P. Vidhya Saraswathi et al. [16]	0.01776	0.04912	0.00348
Kamlesh Gupta et al. [28]	0.0010	0.0060	0.0910
Rasul Enayatifar et al. [29]	-0.0051	0.0078	-0.0009
Haojiang Gao et al. [30]	-0.01589	-0.06538	-0.03231

The correlation between the adjacent pixels of the encrypted images optimal and is close to zero. It is found that the obtained values are better than the methods in [4, 5, 15, 16] and comparable with those methods in [8, 11, 12, 28, 29, 30].

The graphical view of relationship between the adjacent pixels in horizontal, vertical, and diagonal directions in the original and encrypted Lena images are shown in **Fig. 10(a) to Fig. 10(f)**.

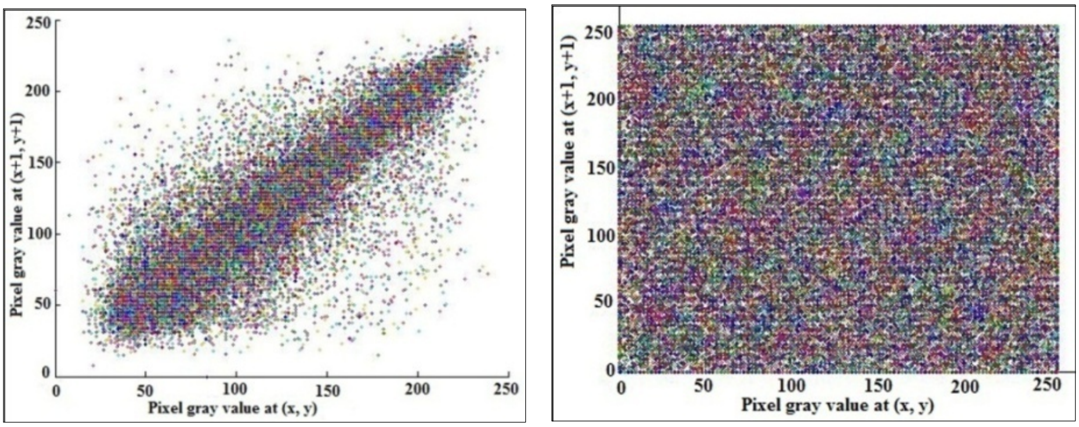


(a) Original image - horizontal

(b) Encrypted image - horizontal

(c) Original image - vertical

(d) Encrypted image - vertical



(e) Original image - diagonal (f) Encrypted image - diagonal

Fig. 10. Distribution of adjacent pixel correlation

From the graph, it is observed that the correlation between adjacent pixels in the encrypted image is reduced and hence the proposed method resists the statistical attacks.

The correlation between the original and encrypted images is given in **Table 5**. The cross correlation value shows that there is no relationship between the original image and the corresponding encrypted image. The obtained cross correlation value is comparable with the methods in [13, 31].

Table 5. Comparison of cross correlation value

Encryption Method	Correlation Value
Proposed	0.0040
H.T Panduranga et al. [13]	-0.0073
G.A Sathishkumar et al. [31] (A-I)	-0.0535
G.A Sathishkumar et al. [31] (A-I & A-II)	0.0074

4.4 Entropy Analysis

The entropy of a message source is a measure of the amount of information that the source has. For any source emitting 2^8 symbols with the equal probability, when the entropy is expressed in bits, the dela result is 8 corresponding to a truly random source [5]. The measure is a function of the probability distribution over the set of all possible messages the sources may produce [32, 33]. The entropy of gray-scale images is theoretically equal to 8 Sh, if each level of gray is assumed to be equiprobable. In image encryption, the encrypted image should provide an equiprobable gray level [8]. If the entropy values of the encrypted image is close to 8 Sh (Shannon) then the encryption algorithm is highly robust against entropy attacks. The entropy of the information is computed by using the mathematical expression given in equation (7).

$$\boldsymbol{H(m) = \sum_{i=0}^{m-1} p(mi) log \left({}^{1}/_{p(mi)}\right)} \tag{7}$$

Where, m is the total number of symbols in $m_i \in m$; $p(m_i)$ represents the probability of occurrence of the symbol m_i and log denotes the base 2 logarithm. The obtained entropy value of the proposed method and existing methods are given in **Table 6**.

Table 6. Comparison of entropy value

Encryption Method	Entropy Value (Sh)
Proposed	Lena: 7.9970 Cman: 7.9946
Qiang Zhang et al. [4]	7.9975
Liang Zhao et al. [5]	7.9719
Khaled Loukhaoukha et al. [8]	7.9968
Reza Moradi Rad et al. [11]	7.9971
Adrian Viorel Diaconu et al. [12]	7.9992
G.A. Sathishkumar et al. [14]	7.8101
Z. Lin et al. [22]	7.9890
Kamlesh Gupta et al. [28]	7.9981
Rasul Enayatifar et al. [29]	7.9931

It is observed that the result obtained by the proposed method is acceptable and better than those methods in [5, 14, 22, 29]. Also, the obtained result is comparable with the existing method in [4, 8, 11] and slightly lower than the methods in [12, 28].

4.5 Noise Attack Analysis

The attackers may introduce cropping and additive noise attacks on the encrypted image while transit. These attacks destroy the information condition so that the authorized person couldn’t use the image after successful decryption.

4.5.1 Additive Noise Attack

An additive noise attack consists in adding random noise to the intercepted encrypted image [12]. The additive noise attack is introduced on the encrypted image using salt and pepper noise and speckle noise to test the resistance of proposed image encrypted method against this attack. The obtained result of additive noise attack test using the encrypted Lena image is presented in **Fig. 11(a)**, **(b)**, **(c)** and **(d)** with density 0.05 and 0.1 for salt and pepper noise and variance 0.01 and 0.02 for speckle noise respectively.

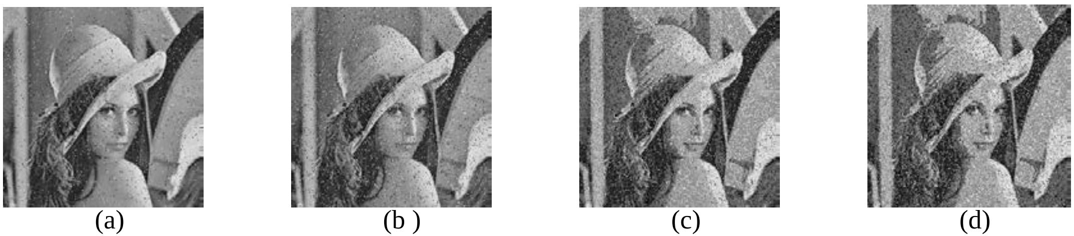

(a) (b) (c) (d)

Fig. 11. Results of additive noise attack

From the results, it is found that the proposed method has good resistance against additive noise attacks and better result is obtained when compared with the method in [12] for high density and variance of salt and pepper and speckle noises.

4.5.1 Cropping Attacks

The cropping attacks consist of modifying the intercepted cipher image by destroying few regions [12]. The cropping attack is tested using the encrypted Lena image after removing 16 regions, each of size 10×10 pixels and one center region of 50×50 pixels as shown in **Fig. 12(a)** and **Fig. 12(b)** respectively. The corresponding decrypted images are shown in **Fig. 12(c)** and **Fig. 12(d)**. The decrypted images are distorted but it could be recognized as a Lena image.

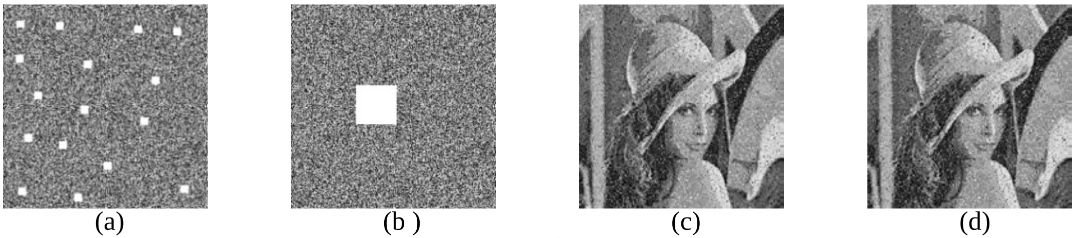

(a) (b) (c) (d)

Fig. 12. Results of cropping attack

From the results, it is observed that the proposed method has acceptable resistance against cropping attacks and better result is obtained when compared with the method suggested in [12].

4.6 Key Space Analysis

The key space size is the number of encryption/decryption key pairs that are available in the cipher system. A necessary condition for an encryption scheme to be secure is that the key space should be large enough to preclude the exhaustive key search attack [33]. The cryptosystem which uses 26 characters as key supports 26! = 4×10^{26} number of keys. If the speed of the system is one decryption/µs, then the time required for exhaustive key search attack is 6.4×10^{12} years [2]. The key space supported by the propsoed method and the existing methods are given in **Table 7**. The calligraphy based scan is suitable for all the characters of the Unicode character set. Therefore, the proposed method has a total of 65,536 characters (simple characters may be excluded) as key space to resist the exhaustive key search attack. In the proposed method the time consumed for one encryption/decryption is 0.39 s. For a keyword with 16 characters the estimated time for brute-force attack is 77 years. Hence, it is observed that the proposed method has required resistance for brute-force attack.

Table 7. Comparison of key space

Encryption Method	**Key Space**
Proposed	65,536 characters
Qiang Zhang et al. [4]	10^{84} (Approx. 2^{279})
Liang Zhao et al. [5]	10^{56}
S.S.Maniccam et al. [6, 7]	10^{19000}
Adrian Viorel Diaconu et al. [12]	10^{88}
Kamlesh Gupta et al. [28]	2^{148}
Rasul Enayatifar et al. [29]	2^{80} (Approx. 1.20893×10^{24})

4.7 Cryptanalysis

Cryptanalysis is an analysis of possible attacks on a cryptosystem and its difficulty level. When cryptanalyzing a cryptosystem the purpose is to recover the secret key which is used in encryption/decryption. Based on the Kerckhoffs's principle, there are four possible attacks to deduce the keys. These types attacks rely on development and working of the algorithm. The known knowledge about plaintext, ciphertext, and sample plaintext-ciphertext pairs are utilized in these attacks. In the analysis, it is assumed that the adversary know everything about the cryptosystem except the secret key [2, 33].

In the proposed method, the secret key used is highly unpredictable since it is based on the large volume of key space and is of 65,536 characters. Hence, the secret key used for the encryption cannot be exploited easily. Also in the development of encryption algorithm two unique scan patterns generated based on Calligraphy are used. It is infeasible to extract the permutation sequence and unique seed values to the random number generator. So the adversary would not be able to succeed easily with known-plaintext attack.

In the case of chosen-ciphertext attack, the adversary selects the ciphertext and study the plaintext by decrypting them. To mount this attack the adversary gains access to the equipment used for decryption but not the decryption key. The objective is to deduce the key from the plaintext derived from the ciphertext. In the proposed method, the encryption/decryption system used for this purpose is highly secure.

In the proposed method, large volume of key space, unconventional scan pattern generation procedure and compatible random number generator are used for the encryption/decryption. The overall security attained by this method is clearly demonstrated by the results obtained in the experimental analysis. In addition, the system setup used for this purpose is highly secure. Hence, the proposed encryption method would have significant resistance to all possible attacks.

4.8 Execution Time

The real time usage of any image cryptosystem is typically relies on the execution time taken by encryption process. Thus, the amount of time consumed by the proposed method is measured and compared with the existing methods and the results are tabulated in Table 8. The time taken to insert characters of the secret keyword and to identify the hit and un-bit pixels for scan key generation is one time process and usually this is not considered as part of the encryption time.

Table 8. Comparison of encryption time

Encryption Method	Time	Image Size	System Configuration
Proposed	0.39 s	256×256	Matlab 2010a, Intel Core i3 Duo Processor, 2 GHz, 2 GB RAM, 160 GB HDD, and Windows 7.
Conventional Algorithms	> 30 s (DES) > 37 s (AES) > 80 s (IDEA)	256×256	
Liang Zhao et al. [5]	1.3912 s	256×256	Not reported
KhaledLoukhaoukha et al. [8]	0.12 s	256×256	Matlab, PC with an AMD Athlon Processor with 2.70 GHz, 1 GB RAM and 160 GB hard-disk.
Reza Moradi Rad et al. [11]	0.1022 s	256×256	Windows 7, Intel(R) Core (TM) 2 Duo CPU, 2.53 GHz, 4 GB RAM.
Adrian Viorel Diaconu et al.[12]	0.1826 s	512×512	Matlab 7.3.0, Intel Pentium Dual CPU T3200 @ 2.00 GHz PC.
Kamlesh Gupta et al. [28]	0.521 s	256×256	Matlab 7.0, Intel Core 2 Duo 2 GHz, 2 GB RAM and Windows XP.
Haojiang Gao et al. [30]	<0.5 s	256×256	P-IV, 1.5 GHz, 512 MB RAM, 40 GB HDD.

The execution time of proposed method is better than the conventional encryption algorithm and the image encryption methods suggested in [5, 28, 30]. Also, the result is comparable with the methods in [8, 11, 12].

The efficiency of the encryption/decryption process mainly depends on the available key space, the type and randomness of the scan pattern, and the source for random numbers. In the proposed method, Calligraphy is used to generate scan patterns which depends on the chosen characters of the language. The generated scan pattern depends on the selected secret keyword and the way of writing the character of the keyword. The basic scan patterns such as raster, diagonal, orthogonal, spiral and Rubik's cube are based on well defined set of rules. But the Calligraphy based scan pattern generation is not based on set of rules as above so it is highly random.

In the experimental results and analysis, the evaluation metrics which are necessary for assuring the security of the proposed encryption method is performed. The metrics such as histogram, correlation, NPCR, UACI, entropy, noise attack test, key space, cryptanalytics, and execution time are determined and compared with the standard values. The main objective of the analysis is to demonstrate the efficiency of the proposed method by considering only the necessary metrics. A single iteration is done for comparing the performance of the proposed method with the existing methods. The security of the proposed encryption method can be further improved for practical applications by increasing the number of iterations for encryption and by using distinct secret keyword for each iteration.

5. Conclusion

In this paper, a novel image encryption method is presented with calligraphy based scan patterns and random number. It is found that the encrypted image is completely different from the original image by high pixel shuffling rate. The obtained NPCR values are greater than 99.5% and the UACI values are approximately close to 30%. The correlation between adjacent pixels of the encrypted image and the correlation between the original image and the corresponding encrypted image are almost zero. The histogram of the encrypted image is much flat. Thus, the proposed method resists the differential and statistical attacks. The obtained entropy value is close to 8 Sh which makes the entropy attack infeasible. The proposed method has good resistance against additive-noise and cropping attacks and has sufficient key space to resist the exhaustive key search attack.

References

[1] Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen, "A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software*, vol. 58, no. 2, pp. 83-91, 2001. Article (CrossRef Link)

[2] William Stalling, *Cryptography and Network Security-Principles and Practices*, 5th Edition, Pearson Education, 2013.

[3] Hongjun Liu, Xingyuan Wang, and Abdurahman kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing*, vol. 12, no. 5, pp. 1457-1466, 2012. Article (CrossRef Link)

[4] Qiang Zhang, Xianglian Xue, and Xiaopeng Wei, "A novel image encryption algorithm based on DNA subsequence operation," *The Scientific World Journal*, vol. 2012, pp. 1-10, 2012. http://hindawi.com/journals/tswj/2012/286741/ref

[5] Liang Zhao, Avishek Adhikari, Di Xiao, and Kouichi Sakurai, "On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation

encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 8, pp. 3303-3327, 2012. Article (CrossRef Link)

[6] SS Maniccam and NG Bourbakis, "Lossless image compression and encryption using scan," *Pattern Recognition*, vol. 34, no. 6, pp. 1229-1245, 2001. Article (CrossRef Link)

[7] SS Maniccam and NG Bourbakis, "Image and video encryption using scan patterns," *Pattern Recognition Society*, vol. 37, no. 4, pp. 725-737, 2004. Article (CrossRef Link)

[8] Khaled Loukhaoukha, Jean-Yves Chouinard and Abdellah Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1-13, 2012. http://hindawi.com/journals/jece/2012/173931

[9] Avi Dixit, Pratik Dhruve and Dahale Bhagwan "Image encryption using permutation and rotational XOR technique," *Computer Science & Information Technology*, vol. 2, no. 3, pp. 01-09, 2012. Article(CrossRef Link)

[10] CK Huang, CW Liao, SL Hsu and YC Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommunication Systems*, vol. 52, no. 2, pp 563-571, 2013. http://link.springer.com/article/10.1007%2Fs11235-011-9461-0

[11] 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, pp. 275-290, 2013. Article (CrossRef Link).

[12] Adrian Viorel Diaconu and Khaled Loukhaoukha, "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher," *Mathematical Problems in Engineering*, vol. 2013, pp. 1-10, 2013. http://downloads.hindawi.com/journals/mpe/2013/848392.pdf

[13] HT Panduranga and SK Naveen Kumar, "Hybrid approach for image encryption using scan patterns and carrier images," *International Journal on Computer Science and Engineering*, vol. 2, no. 2, pp. 297-300, 2010. http://arxiv.org/pdf/1003.1239

[14] GA Sathishkumar and K Bhoopathy Bagan, "A novel image encryption algorithm using pixel shuffling and Base-64 encoding based chaotic block cipher," *WSEAS Transactions on Computers*, vol. 10, no. 6, pp. 169-178, 2011. http://dl.acm.org/citation.cfm?id=2001193

[15] CK Huang and HH Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, vol. 282, no. 11, pp. 2123-2127, 2009. Article (CrossRef Link)

[16] P Vidhya Saraswathi and M Venkatesulu, "A block cipher algorithm for multimedia content protection with random substitution using binary tree traversal," *Journal of Computer Science*, vol.8, no. 9, pp. 1541-1546, 2012. Article (CrossRef Link)

[17] Han Shuihua and Yang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation," *ECTI Transactions on Computer and Information Technology*, vol. 1, no. 2, pp. 126-133, November 2005. http://ecti-thailand.org/assets/papers/95_pub_3.pdf

[18] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption using Block-Based Transformation Algorithm," *IAENG International Journal of Computer Science*, vol. 35, no. 1, pp.15-23, 2008. http://iaeng.org/IJCS/issues_v35/issue_1/IJCS_35_1_03.pdf

[19] Chinmaya Kumar Nayak, Anuja Kumar Acharya, and Satyabrata Das, "Image Encryption Using an Enhanced Block Based Transformation Algorithm," *International Journal of Research and Reviews in Computer Science*, vol. 2, no. 2, pp. 275- 279, 2011. http://connection.ebscohost.com/c/articles/82589786

[20] A Mitra, YV Subba Rao, and SRM Prasanna, "A new image encryption approach using combinational permutation techniques," *International Journal of Electrical and Computer Engineering*, vol.01, no.02, pp. 127-131, 2006. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.360.989&rep=rep1&type=pdf

[21] Tzung-Her Chen and Kuang-Che Li, "Multi-image encryption by circular random grids," *Information Sciences*, vol. 189, pp. 255-265, 2012. http://dl.acm.org/citation.cfm?id=2109630

[22] Z Lin and H Wang, "Efficient image encryption using a chaos-based PWL memristor," *IETE Technical Review*, vol. 27, no. 4, pp. 318–325, 2010. Article (CrossRef Link)

[23] Jawad Ahmad and Fawad Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *International Journal of Video & Image Processing and Network Security*, vol. 12, no. 04, 2012, pp. 18-31. http://ijens.org/Vol_12_I_04/1213104-9696-IJVIPNS-IJENS.pdf

[24] Yue Wu, Joseph P Noonan, and Sos Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications* , pp. 31-38, 2011. http://ijcaonline.org/archives/volume103/number12/18126-9198

[25] Chen W and Chen X, "Optical image encryption using multilevel Arnold transform and noninterferometric imaging," *Optical Engineering*, vol. 50, no. 11, 117001, 2011. Article (CrossRef Link).

[26] Chen W, and Chen X, "Security-enhanced interference-based optical image encryption," *Optics Communications*, vol. 286, pp. 123-129, 2013. Article (CrossRef Link)

[27] Chen W, Javidi B and Chen X, "Advances in optical security systems," *Advances in Optics and Photonics*, vol. 6, no. 2, pp. 120-155, 2014. Article (CrossRef Link)

[28] Kamlesh Gupta and Sanjay Silakari, "New approach for fast color image encryption using chaotic map," *Journal of Information Security*, vol. 2, pp. 139-150, 2011. Article (CrossRef Link)

[29] Rasul Enayatifar, "Image encryption via logistic map function and heap tree," *International Journal of the Physical Sciences*, vol. 6, no. 2, pp. 221-228, 2011. http://academicjournals.org/journal/IJPS/article-abstract/57AFB2319623

[30] Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li, "A new chaotic algorithm for image encryption," *Elsevier Science Direct*, vol. 29, no. 2, pp. 393-399, 2006. Article (CrossRef Link)

[31] GA Sathishkumar, K Bhoopathy and R Sriraam, "Image encryption based on diffusion and multiple chaotic maps," *International Journal of Network Security & its Applications*, vol. 3, no. 2, pp. 181-194, 2011. http://arxiv.org/pdf/1103.3792

[32] CE Shannon, "A mathematical theory of communications," *Bell Systems Technical Journal*, vol. 27, no. 3, pp. 379-423, 1948. Article (CrossRef Link)

[33] Alfred J.Menezes, Paul C.van Oorschot, and Scott A.Vanstone, *Handbook of Applied Cryptography*, CRC Press, New York, 2010.

T.Sivakumar received his B.Sc degree in Mathematics from the Manonmaniam Sundaranar University, and M.C.A degree from the Bharathidasan University, India. He received his second master degree M.E in Computer Science and Engineering from Anna University of Technology, Coimbatore, India. He is currently working as an Assistant Professor (Senior Grade) in the Information Technology Department, PSG College of Technology, Coimbatore, Tamilnadu-641004, India. and pursuing Ph.D in image encryption techniques.

R.Venkatesan received his B.E (Hons) degree from Madras University in 1980. He completed his Masters degree in Industrial Engineering from Madras University in 1982. He obtained his second Masters degree MS in Computer and Information Science from University of Michigan, USA in 1999. He was awarded with Ph.D from Anna University, Chennai in 2007. He is currently Professor and Head in the Department of Computer Science and Engineering at PSG College of Technology, Coimbatore, India. His research interests are in Simulation and Modelling, Software Engineering, and Algorithm Design. He has several International and National publications to his credit.