



Knight's Tour Application in Digital Image Encryption

Narendra K Pareek

University Computer Centre, Vigyan Bhawan
M L Sukhadia University, Udaipur, India

Abstract— *Use of rule sets of popular games, especially in design of image encryption algorithm, leads to a new paradigm in the field of cryptography. The paper aims to study a newly designed digital grey image encryption scheme that uses knight moving rules (game of chess) in conjunction with an external secret key of 128-bits size. In the propose scheme, image is divided into several squared sub-images and knight tour is used to scramble the pixels of sub-image. The starting position of knight on a board (sub-image) as well as pixel substitution depends on the secret key used in the algorithm. The propose encryption scheme has total fifteen rounds and each round has four different processes. Performance analysis shows that the proposed scheme has good statistical character, key sensitivity and can resist attack efficiently.*

Keywords— *Knight tour, Grey image encryption, Secret key, Image cipher, Pixel scrambling, Image security.*

I. INTRODUCTION

With the advances in information technology, a huge amount of digital data is being exchanged over various types of networks. Major part of transmitted digital data, which is either confidential or private, demands for security mechanisms to provide required protection. Therefore, security has become an important issue during the storing and transmission of digital data. Security of images is an application layer technology to guard the transmitted information against unwanted disclosure as well as to protect the data from modification while they are in transit. Three different ways to protect digital data from unauthorized eavesdropping are cryptography, steganography and watermarking. Among them, cryptography has become one of the major tools to provide high level of security. Cryptography deals with the development of techniques for converting information between intelligible and unintelligible forms. It deals with the content confidentiality and access control. The conventional encryption algorithms, like AES, DES, IDEA etc, are not preferred for image encryption for two reasons [1]. The first one is that the image size is always large as compared to the simple text size therefore the conventional text cryptosystems take longer time to encrypt the image data. The second is that image data has high correlation among adjacent pixels. It is difficult for these cryptosystems to shuffle and diffuse image data effectively.

In order to transmit images securely over unsecured public channels, a variety of encryption algorithms have been suggested. These algorithms can be classified into three major categories: position permutation, substitution transformation and permutation-substitution transformations. All these image encryption algorithms are based on principle of chaos[2-3], cellular automata[4-5], spatial transform [6-7], matrix decomposition[8] etc. Besides these, a few new designs based on rule sets of the popular games e.g. Sudoku puzzle based [9-10], Chinese knight tour based [11-12], Rubik's cube principle based [13-14] and Poker shuffling based [15]) are also found secured.

The aim of this article is to contribute a new encryption scheme for grey images based on knight's moving rules in conjunction with an external key of 128-bits size. The proposed encryption scheme uses both pixel substitution as well as pixel scrambling process. The pixel substitution is achieved with the help of secret key used in the algorithm whereas knight tour is used for pixel scrambling. In the proposed scheme, there are fifteen rounds and each round have four different processes. In each process, image is divided into squared sub-images and further, these sub-images passes through pixel scrambling process. The rest of this paper is organized as follows. In Section II, overview of knight tour is presented. In Section III, we discuss the detail of proposed algorithm and in Section IV, performance and security analysis of the proposed algorithm are discussed. Finally, Section V concludes the work carried out.

II. KNIGHT TOUR

Knight tour problem is an interesting puzzle among the domain of chess problems. Number of different solutions to the knight tour problem becomes larger and more intractable as N , the dimension of the board, increases. When dimension of board is 5×5 , there are 304 solutions only. On increasing board size to 6×6 , there are 524,486 solutions. For $N=8$, the number of solutions grows incredibly large, with 33,439,123,484,294 possible tours [16]. The original knight tour problem can be stated as follow. Place a knight on an arbitrary square of the chess board and visit every other square exactly once by performing knight moves until all 64 squares have been visited. The problem can be extended to $N \times N$ board, completing a tour when all $N \times N$ squares have been visited. Knight's moving rules, unlike to all other pieces, follow an 'elbow' shape i.e. in form of English letter L. In other words, a horizontal displacement of two squares, followed by a vertical displacement of one square or a vertical displacement of two squares, followed by a horizontal displacement of one square, in either direction. Thus, as shown in Fig. 1(a), one can define a set of eight possible moves.

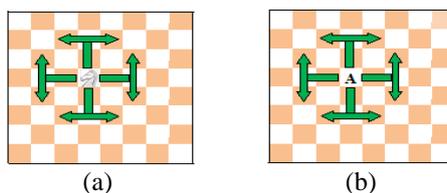


Fig. 1 Knight's possible moves (a) Knight movement (b) Data movement.

In the propose scheme, the image is divided into several squared sub-images and each sub-images are considered as chess board. The knight' path on a board is used to scramble the pixels of a sub-image within itself. The starting position of the knight on the board is chosen from the used external secret key i.e. k_x, k_y . In the Fig. 2(a), we have shown an image of 8x8 size and their pixel values are denoted with 1,2,3... so on. Starting position of the knight is chosen from secret key used and assume it is (5,5). On completion of tour on board, the path of the knight is shown in Fig. 2(b). This Fig. 2(b) is used to scramble the pixels of image within itself. When dimension of the board is 8x8, the minimum number of unique knight tour sets is 64. For $N = 18$, the number of unique tour sets grows with 324.

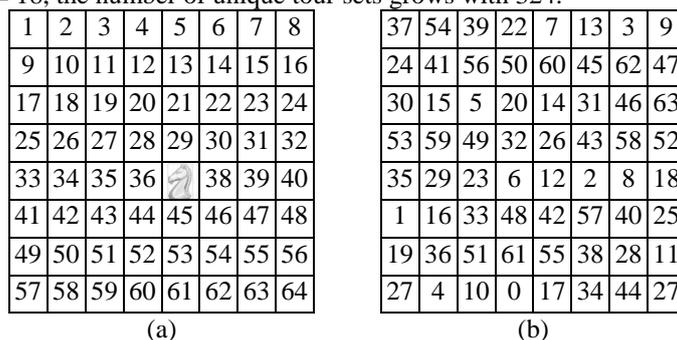


Fig. 2 (a) Chess board of dimension 8x8 (b) Path of Knight on chess board.

III. PROPOSED ALGORITHM

Detail of the proposed encryption algorithm is as follows.

- Proposed encryption algorithm uses a secret key of 128-bits size. The key is divided into blocks of 8-bits each referred as session keys.

$$k = k_1 k_2 k_3 \dots k_{32} \text{ (in hexadecimal),}$$

$$K = K_1 K_2 K_3 \dots K_{16} \text{ (in ASCII),}$$

here, k_i 's (referred as sub-keys) are hexadecimal digits (0-9 and A-F) and K_i 's represent session keys.

- Set M =Number of columns in the image, N =Number of rows in the image
Set $index=0$, $Bsize=18$
- For Step = 0 : 15 do
- For R = 1 : N do
For C = 1 : M do { Image[R][C] = Image[R][C] \oplus K[index%16+1];
index = index + 1; }
- Endfor
- Endfor
- Divide the resultant image into squared sub-images of sizes of $Bsize \times Bsize$ as follow-
 - If (Step mod 4=0) Take entire image and divide it into non-overlapping square sub-images. The partially encrypted image is shown in Fig 3(a).
 - If (Step mod 4=1) Take part of partially encrypted image (Fig 3(a)), leaving first 9 pixels of each column, as shown in Fig 3(b) (dark shed) and divide it into non-overlapping sub-images.
 - If (Step mod 4=2) Take part of partially encrypted image (Fig 3(b)), leaving first 9 pixels of each row, as shown in Fig 3(c) (darken shed) and divide it into non-overlapping sub-images.
 - If (Step mod 4=3) Take part of partially encrypted image (Fig 3(c)), leaving first 9 pixels of each column and row, as shown in Fig 3(d) (darken shed) and divide it into non-overlapping sub-images.
- Set NBlock= Number of square sub-images in the image, index=1
- For i = 1 : NBlock do
- Set $x=k_{index}$, $y=k_{index+1}$
- Take i^{th} sub-image and consider it as chessboard of the size of $Bsize \times Bsize$.
- Record pixels order of knight tour route on chessboard starting from pixel location (x,y) in i^{th} sub-image.
- Scramble the pixels of i^{th} sub-image according to the pixels order of knight tour route.
- Set $index=(index + 2)$ to choose next pair of sub-key.
- If ($index > 32$) Set $index=1$.
- Endfor { Step 7 }
- Endfor { Step 3 }
- Resultant encrypted blocks are written in a file.

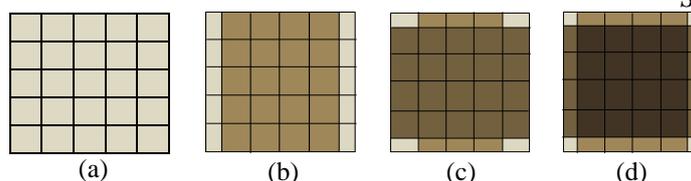


Fig. 3 Squared sub-images used in four different processes.

IV. PERFORMANCE AND SECURITY ANALYSIS

In this section, we discuss the security analysis of the proposed image encryption scheme through statistical analysis, key space analysis, sensitivity analysis etc. to prove the robustness of the proposed algorithm against most common attacks. To illustrate the robustness of proposed scheme, size of squared sub-image was taken as 18x18 pixels. We implemented the proposed image encryption technique in C programming language and analysis of image have been done using MATLAB application tool.

A. Distribution of Pixels

Histogram analysis depicts pixels' distribution within an image by representing their number relative to each intensity level [3]. We have analyzed the histograms of several encrypted images and their corresponding plain images having widely different contents. Two examples of such histograms analysis are shown in Fig. 4. In Frames (a), we have shown an image and its corresponding encrypted image produced using the key 'E5DA750B4C1F78D328EA25E6B15CF9E4' is shown in Frame (b). In Frames (c) and (d) respectively, histograms of the image (Frame (a)) and its encrypted image (Frame (b)) are shown. From both histograms, it is clear that most of pixels are scattered in the range 50 to 180 (Fig. 4(c)) in the original image whereas pixels are almost uniformly distributed (Fig. 4(d)) in the encrypted image. Plain image and its corresponding encrypted image produced using the key 'E5DA750B4C1F78D328EA25E6B15CF9E4' are shown in Frames (e) and (f) respectively. This histograms of these images are shown in Frames (g) and (h) respectively. From both histograms, it is again evident that pixels are scattered in the range 10 to 180 (Fig. 4(g)) in the original image whereas pixels are almost uniformly distributed (Fig. 4(h)) in the encrypted image. The encrypted images histograms (Fig. 4(d) and Fig. 4(h)), approximated by a uniform distribution, are significantly different from images histograms.

Uniform distribution of pixels of encrypted image points out good quality of the encryption method. Therefore, the encrypted image does not provide any clue to employ any statistical attack on the proposed image encryption scheme, which makes statistical attacks difficult [3].

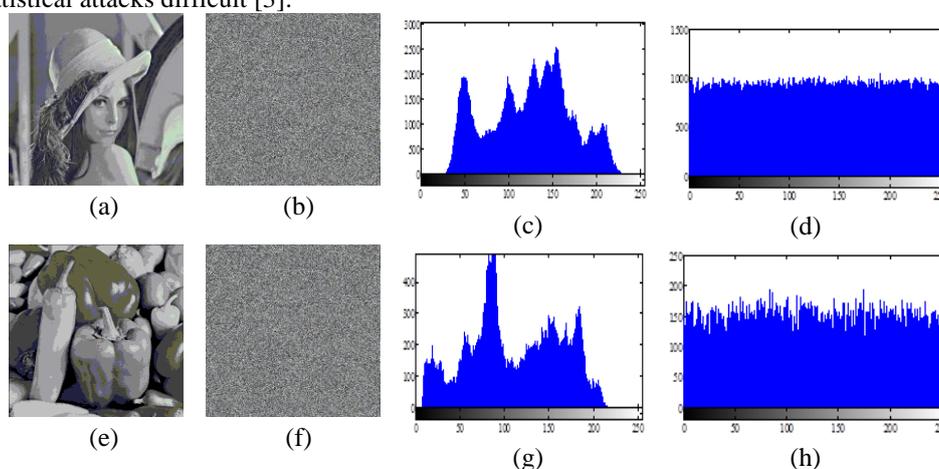


Fig. 4 Histograms of images and their corresponding encrypted images.

B. Correlation between images and their encrypted images

We have also done extensive study of the correlation between pairs of original and its corresponding encrypted image produced using the proposed image encryption algorithm by computing the correlation coefficients. Results of a few images of various sizes and contents are given in Table 1. In the last row of Table 1, we have given the results for the average value of the correlation coefficients between over 50 gray images of various sizes and having widely different contents i.e. a heterogeneous collection and their corresponding cipher images produced using the proposed encryption algorithm. It is evident from Table 1 that correlation coefficients between images and their corresponding encrypted images, for all the test cases, are negligible and around zero, which shows that the original images are nearly independent from the encrypted images.

Table I Correlation coefficient between various sizes of plain and cipher images

Image	Size	Correlation
512x512	256 KB	0.0132
128x128	17 KB	0.0209

256x256	64 KB	-0.0183
512x480	241 KB	0.0169
400x376	147 KB	0.0167
Average for a heterogeneous collection of images		0.108

C. Correlation analysis of adjacent pixels

In addition to the correlation analysis of images, we have also analyzed the correlation between horizontally and vertically adjacent pixels in several images and their corresponding encrypted images. In Fig. 5, we have shown the distribution of horizontally and vertically adjacent pixels in images (Fig. 4(a) and 4(e)) and their corresponding encrypted image (Fig. 4(b) and 4(f)). Particularly, in Frames (a) and (c) respectively, we have depicted the distributions of two horizontally and vertically adjacent pixels in image however in Frames (b) and (d) respectively, the distributions of horizontally and vertically adjacent pixels in the encrypted image have been depicted. We observe from the pixel distributions shown in Fig. 5 that there is a negligible correlation between the adjacent pixels in the encrypted image. However, the adjacent pixels in the original image are highly correlated.

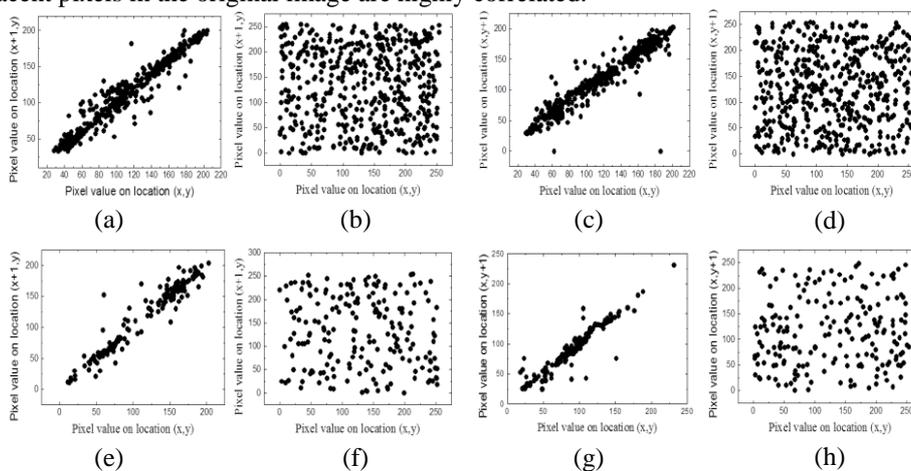


Fig. 5 Horizontal and vertical adjacent pixels plot of original and encrypted images.

D. Key sensitivity analysis

An ideal image cipher should be extremely sensitive with respect to the secret key. Even flipping of a single bit in the key should produce a widely different encrypted image. To test the sensitivity of the proposed image cipher with respect to the key, encrypted image corresponding to image is decrypted with a slightly different key than the original one. One such example is discussed below.

- 1) The encrypted image (Fig. 4(b)) is decrypted by making a slight modification in the original key 'D5DA750B4C1F78D328EA25E6B15CF9E4' and resultant image is shown in Fig. 6(a).
- 2) The encrypted image (Fig. 4(b)) is decrypted by making a slight modification in the original key 'E5DA750B4C1F78D328EA25E6B15CF9E3' and resultant image is shown in Fig. 6(b).
- 3) The encrypted image (Fig. 4(b)) is decrypted by making a slight modification in the original key 'E5DA750B4C1F78D338EA25E6B15CF9E4' and resultant image is shown in Fig. 6(c).

With a slight change in the key, one is unable to find any clue about the original image from the decrypted image. We can conclude that one cannot find any clue about the image even if there is a little change in the key. Having the right pair of secret key is an important part while decrypting the image, as a slight change in the secret key will not retrieve the exact original image. Above example shows that the decryption of the encrypted image with the wrong secret key will not reveal any information about the original image hence shows the effectiveness of the proposed technique.

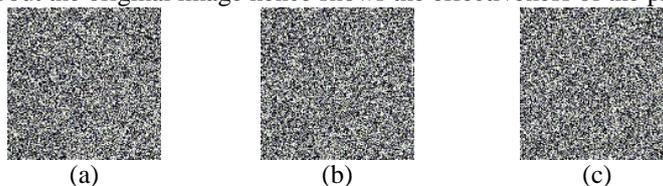


Fig. 6 Encrypted images with slightly modified secret keys.

E. Information entropy

To quantifying the uniformity of pixel distribution, we also computed the information entropy. It quantifies the amount of information contained in data, usually in bits or bits/symbol. The following expression is used for the calculation of information entropy [17].

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \log_2 \frac{1}{P(s_i)} \quad (1)$$

where N is the number of bits used to specify the grey pixel value in the image and $P(s_i)$ shows the probability of i^{th} grey level. If every symbol has an equal probability, i.e., $s = \{s_0, s_1, s_2, \dots, s_{2^8-1}\}$ and $P(s_i) = 1/2^8$ ($i=0,1,\dots,255$), then the entropy is $H(s)=8$ which corresponds to an ideal case. To design a good image encryption scheme, the entropy of encrypted image close to the ideal case is expected. We have computed entropy of several encrypted images of different nature and found to be very close to the ideal value. This means information leakage in the proposed encryption process is negligible. Hence, proposed algorithm is secured upon the entropy attack.

Table II Entropy of images

Entropy	Original image	Encrypted image
Lena	7.4469	7.9993
Chilli	7.5162	7.9945

F. Key space analysis

Along with the sensitivity on secret key, any good encryption scheme should possess a large enough key space to make brute-force attacks infeasible. The secret key used in the encryption/decryption should be neither too long nor too short. In the proposed encryption algorithm, size of secret key is 128-bits. Thus, it has 2^{128} different combinations (3.40×10^{38}). An image encryption algorithm with such a large key space is sufficient for resisting against any brute-force attacks.

G. Encryption speed

Apart from the security consideration, encryption/ decryption rate of the algorithm is also an important aspect for a good encryption scheme. We have also measured time taken by the proposed scheme to encrypt/decrypt various different sizes images. The time analysis has been done on a personal computer with Intel core i5 2.9 GHz processor and 4 GB RAM. The average encryption rate of proposed scheme is 210 KB/second.

V. CONCLUSION

In this paper, rule sets of knight' movement was used to design a digital image encryption scheme for grey scale image in conjunction with an external secret key of 128-bits size. The proposed scheme is based on scrambling as well as substitution process. Results obtained from the rigorous security analysis prove the robustness of the proposed method and indicate that the proposed scheme has high order of security and thus can be used for real-time transmission of digital grey scale images.

REFERENCES

- [1] Hongxing Yao, and Meng Li, "An approach of image hiding and encryption based on a new hyperchaotic system," *International Journal of Nonlinear Science*, vol. 7, pp. 379-384, 2009.
- [2] Chong, Meng Fu, Wei-hong Zhan, Yong-feng Zhu, Zhi-liang Francis, C.M. Lau., Tse Chi K., and Ma Hong-feng, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43(8), pp.1000-1010, 2013.
- [3] V. Patidar, N.K. Pareek, G. Purohit, and K.K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics communications*, vol. 284(19), pp. 4331-4339, 2011.
- [4] R. Ye, and H. Li, "A novel image scrambling and watermarking scheme based on cellular automata," in *Proc of International Symposium on Electronic Commerce and Security*, August 2008, p. 938-941, Guangzhou, China.
- [5] A.L.A. Dalhoum, B.A. Mahafzah, A.A. Awwad, I. Aldamari, A. Ortega, and M. Alfonseca, "Digital image scrambling using 2D cellular automata," *IEEE Transactions on Multimedia*, vol. 19(4), pp. 28-36, 2012.
- [6] G. Ye, X. Huang, and C. Zhu, "Image encryption algorithm of double scrambling based on ASCII code of matrix element," In *Proc of the International Conference on Computational Intelligence and Security (CIS '07)*, p. 843-847, December 2007.
- [7] K.T. Lin, "Hybrid encoding method by assembling the magic matrix scrambling method and the binary encoding method in image hiding," *Optics Communications*, vol. 284(7), pp. 1778-1784, 2011.
- [8] D. Van de Ville, W. Philips, R. Van de Walle, and I. Lemahieu, "Image scrambling without bandwidth expansion," *IEEE Trans on Circuits and Sys for Video Tech*, vol. 14(6), pp. 892-897, 2004.
- [9] Y. Zou, X. Tian, S. Xia, and Y. Song, "A novel image scrambling algorithm based on Sudoku puzzle," In *Proc of the 4th International Congress on Image and Signal Processing (CISP '11)*, vol. 2, p. 737-740, Shanghai, China, October 2011.
- [10] Y.Y. Wang, D. Wan, and H.Y. Sheng, "An encryption algorithm by scrambling image with sudoku grids matrix," *Advanced Materials Research*, vol. 433, pp. 4645-4650, 2012.
- [11] J. Delei, B. Sen, and D. Wenming, "An image encryption algorithm based on Knight's tour and slip encryption filter," In *Proc of the International Conference on Science and Software Engineering*, vol. 1, p. 251-255, Wuhan, China, December 2008.

- [12] Z.K. Lei, Q.Y. Sun, and X.X. Ning, "Image scrambling algorithms based on knight-tour transform and its applications," *Journal of Chinese Computer Systems*, vol. 5, Article 044, 2010.
- [13] K. Loukhaoukha, J.-Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *Journal of Electrical & Computer Engineering*, Article ID173931, 2012.
- [14] A.-V Diaconu,, and K. Loukhaoukha, "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher," *Mathematical Problems in Engineering*, Article ID 848392, 2013.
- [15] X. Wang, J. Zhang, "An image scrambling encryption using chaos-controlled Poker shuffle operation," *In Proc of the IEEE International Symposium on Biometrics and Security Technologies (ISBAST '08)*, p. 1-6, Islamabad, Pakistan, April 2008.
- [16] Luis Paris, "Heuristic strategies for the knight tour problem," *In proc of the International Conference on Artificial Intelligence, IC-AI* , vol 2, p. 1121-1125, June 21-24, 2004.
- [17] C.E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, pp. 656-715 ,1949.