SN Computer Science (2021) 2:139
https://doi.org/10.1007/s42979-021-00542-7

ORIGINAL RESEARCH

Minimal Block Knight's Tour and Edge with LSB Pixel Replacement Based Encrypted Image Steganography

B. S. Shashikiran[1] · **K. Shaila**[1] · **K. R. Venugopal**[2]

Received: 12 December 2020 / Accepted: 23 February 2021 / Published online: 13 March 2021

Abstract

The data security of an information is predominant in the digital world and gaining lot of importance. Cryptography and steganography are widely used in providing security to an information. In the proposed algorithm, the image encryption and steganography are performed using Knight's move in the game of chess called Knight's Tour Algorithm. Minimum block or square required for a knight's tour to reach all the squares is 5×5 block. The 5×5 blocks' pattern generated is used for image encryption. The encrypted image is then embedded into another image and block shuffling is performed to obtain a crypto-stego image. Proposed algorithm is robust and provides high data security with a good PSNR and SSIM.

Keywords Cryptography · Crypto-Stego · Knight's tour · PSNR · SSIM · Steganography

Introduction

The incessant development and popularization of digital technology has changed the processing of secret images. The entire world is moving towards smart era driven by digital technology and all information is accessible at finger tips. Every second, more than a million information is exchanged across the internet in different formats, such as text, audio, image or video. Information in the image is sparkling and visually attractive than text information. Sensitive, personal information or defense information related to a country or medical information or documents related to an organization need to be protected from trespassers when it is distributed and shared over internet.

The recursive root cause analysis is carried out on trapping and attack of information by trespassers and data protective techniques are improved with new security algorithms. There are many effective techniques that are available to protect the data from unauthorized access like cryptography and steganography. Image files are extensively used nowadays due to its high capacity and easy accessibility and protecting these image files are the top priority. Many cryptography, steganography and crypto-steganography algorithms are developed.

Chess is a game of adaptive strategy and intelligence. Each move of pieces in the chess ends with some pattern by the end of game. The pattern of each pieces has encouraged many combinatorial puzzles. The most interesting and popular patterns are obtained from Knight's Tour and Eight Queen puzzle.

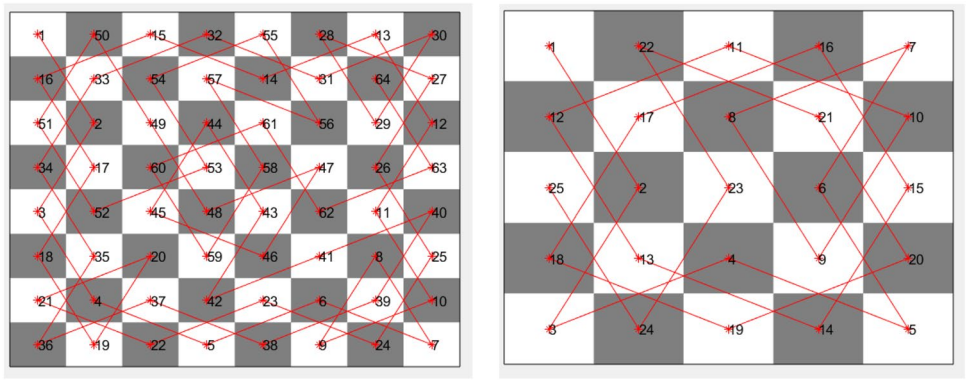
Knight's tour [1–3] is an arrangement of moves of a knight on a chess board such that knight visits each square just once. If the knight tops on a same square where it started, then it is called closed tour, otherwise it is open. The knight's tour problem has become the mathematical puzzle and motivated open thoughts for many image processing and pattern-based research work. The moves of knight in chess game are very tactical to end the game with possible win. Knight's tour is not restricted only for a chess board size 8×8, but it can be extended for any size $M \times N$. To obtain a solution for Knight's tour, minimum size of the board should be 5×5. Figure 1a shows one of the patterns generated by knight's tour on 8×8 board and Fig. 1b shows one of the patterns generated by knight's tour on 5×5 board.

This article is part of the topical collection "Cyber Security and Privacy in Communication Networks" guest edited by Rajiv Misra, R. K. Shyamsunder, Alexiei Dingli, Natalie Denk, Omer Rana, Alexander Pfeiffer, Ashok Patel and Nishtha Kesswani.

✉ B. S. Shashikiran
shashikiran.bisileri@gmail.com

[1] Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru, Karnataka, India

[2] Bangalore University, Bengaluru, Karnataka, India



(a) Knight's tour on 8 X 8 square (b) Knight's tour on 5 x 5

Fig. 1 **a** Knight's tour on 8×8 square, **b** Knight's tour on 5×5

Steganography [4] is a technique of hiding information such that it does not attract the attention of unauthorized persons. Steganography means protected writing and is originated [5] from two Greek words 'Steganos' means protected and 'graphia' means writing. Types of steganography methods [6] used for embedding information are text, image, video and audio steganography. Nevertheless, all types of steganography can be combined together to protect the secret information [7]. Image steganography is a widespread digital steganography used in most of the application.

Cryptography [8] is a technique used for protected communication between authorized persons in the presence of unauthorized person. Cryptography [9] is categorized into two types: symmetric-key cryptography in which same key is used for encryption and decryption; when different keys are used, it is called asymmetric-key cryptography. With the increase use of image for information sharing, image encryption [10] gained lot of demand in the digital era. Different algorithms are used for image encryption ranging from mathematical operations on individual pixels to blocks of pixels.

This work is focused towards encrypting an image using minimal knight's tour algorithm and embedding the encrypted image in other image using steganography. Minimal knight's tour is open tour knight's move on a 5×5 block. Knight's tour does not exist below 5×5 block which visits all the locations in a block and also for an odd size of blocks, there exists no closed knight's tour.

The proposed algorithm is applicable in vast field like confidential communication, protection of data modification, database systems in an organization and other applications.

Motivation

The development of technology and interest of people to have the information at finger tips has encountered in information security issues. During COVID-19 pandemic, most of the physical things changed to virtual things, viz online classes, meetings, shopping, etc. Some organizations inevitably need to share the information virtually. Few of which are making a way for trespassers to hack the information. The main idea is to secure the information in an image by embedding encrypted image using minimal knight's tour algorithm.

Contribution

The information in the image needs to be protected from the intruders. Various encryption and steganography algorithms exist to secure the secret information in an image. With the drastic development in the technology, new algorithms are required for securing the information in an image. In this work, smallest knight's tour algorithm is used for image scrambling to get crypto-image. This crypto-image is then embedded into other image using edge-based and LSB pixel replacement which is applied with block shuffling to get crypto-stego image.

Organization

Related work and problem definition are discussed in Sect. 2 and 3, respectively. Embedding and decryption process with implementation algorithm is described in Sect. 4. Performance results are discussed in Sect. 5.

Related Work

Steganography and cryptography are the techniques that provide security to digital information with the development of digital technology; enormous research at present is in the field of data security. Knight's move in game of chess is different compared to other games and is used in image processing applications. Image encryption and steganography can be achieved using the knight's tour algorithm and

a minimal open knight's tour algorithm is proposed in the work.

Manpreet et al., [11] proposed image encryption algorithm by scrambling the image using standard chessboard knight's tour approach with Euler's solution. Jiang et al., [12] proposed an encryption algorithm using Knight's tour matrix and slip filter convolution approach by altering filter template matrix.

Kanchan et al., [13] proposed knight's tour matrix algorithm in which, image is divided into m x n block size. Knight's tour matrix neighborhood addition modulo encryption is performed to get the encrypted image in two phases. Said et al., [14] proposed image encryption and steganography technique using DNA encoding Choquet's integral sequences. Four coded images are produced using the DNA bases and integral sequences are generated, Choquet's approach used to get four random sequences that are encoded. Wavelet fusion algorithm is used to generate encrypted image.

Chaotic Lorenz system-based information hiding technique is proposed in [15]. Encryption parameters are derived from Lorenz differential equation and using this equation, secret image is encrypted and standard LSB technique is applied on RGB planes separately to embed the encrypted image into Cover image. DCT-based image steganography algorithm is proposed in [16]. Two-dimensional DCT is applied on a non-overlapping 8×8 block image and a quantization of image is performed with quality factor of 50. Non-zero coefficients of $K \times K$ blocks are unaltered and other blocks are embedded with secret image pixels to get the stego image.

Histogram-oriented gradient and intensity gradient are used to get the block of interest with a size of 2×2 for embedding secret image, on the BOI (block of interest) pixel value differencing algorithm is performed in [17]. The process of compressing the secret image is embedded into cover image is discussed in [18]. Coefficient adjustment scheme is employed to slightly modify the cover image based on stego image. Hiding process is performed based on the quality factor.

Graph signal processing (GSP)-based image steganography is discussed in [19]. Arnold cap transformation is used on secret image to scrambled image and then graph wavelets are performed on both cover image and secret image. Alpha bending is performed and then embedding process is carried out to get stego image. Quotient value differencing and LSB substitution-based image steganography and discussed in [20]. 3×3 non-overlapping pixel blocks are considered and QVD is identified. There exists a gradient substation of pixels at higher bits and standard LSB replacement is performed to get stego image.

Problem Definition

Problem Statement

Digital information in the form of image is widely used with the progress of technology. It is observed that trespassers attack the image to retrieve information. Securing the information hidden in an image when it is personal and sensitive is a challenging task. So, crypto-steganography algorithm is developed to embed secret information.

Objectives

The objective of our work is to:

(i) To develop algorithm to maintain integrity and confidentiality of the information.
(ii) To embed secret image using a cover image with knight's tour.

Assumptions

Few of the assumptions in developing algorithm are:

(i) Size of the cover image is $M \times M$ i.e., square image.
(ii) Size of the QR code image is less than $M/2 \times M/2$ of cover image.

Implementation

The method proposed is to apply LSB technique and minimal knight's tour algorithm on secret image and cover image to obtain stego image such that only lawful person has access to hidden information. In this work, a knight tour-based pixel replacement algorithm is developed to encrypt the secret image, making it difficult to trace the original information. The encrypted image is embedded at the edges of blocks and last two-bit planes of cover image using LSB Replacement technique. The obtained image is again applied block shuffling for replacement of blocks.

To recover the secret image from stego image, Knight's tour backtracking algorithm is applied on blocks of stego image and reverse LSB technique is performed to get the encrypted image. The decryption of image is performed using backtracking of knight's tour algorithm. The block diagram of proposed algorithm is represented is Fig. 2. Metrices, such as MSE and PSNR, are calculated to validate the quality of the obtained image and SSIM is calculated to find the structural similarity of cover image and stego image. The key for encryption and decryption is optional and patterns generated using knight's tour should be same for encryption and decryption for the integrity of data. Change in the

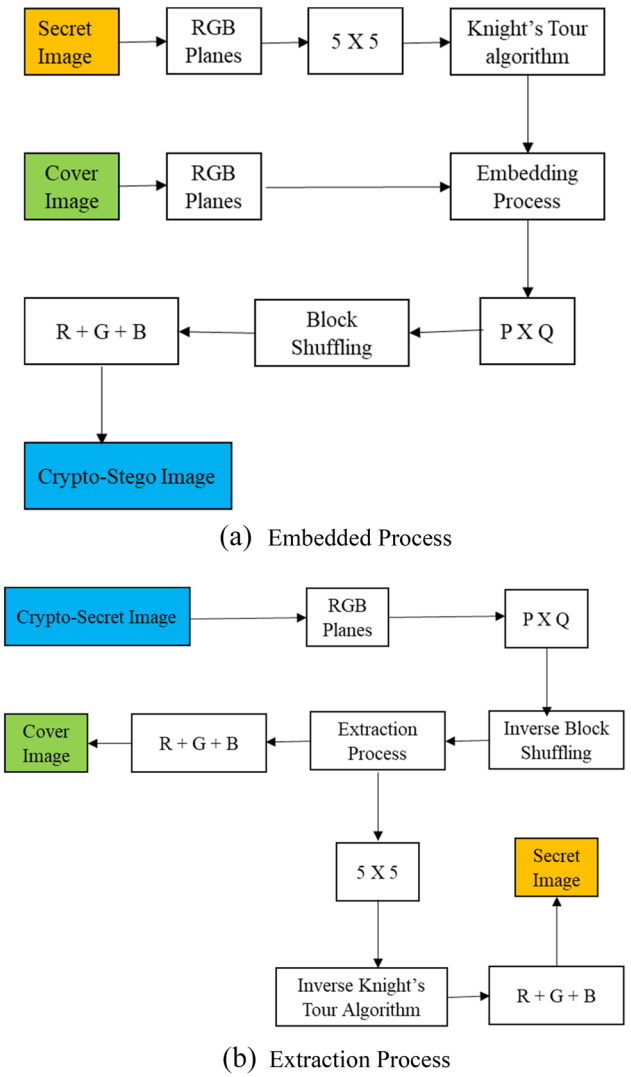


Fig. 2 Embedding and extraction process

pattern for encryption and decryption results in redundant information of the image.

Embedding Process

For embedding secret image in cover image, it is assumed that the ratio in size of the images should be 1:2, respectively. For a minimal knight's tour algorithm, the size of block should be 5×5 and an algorithm is developed on 5×5 matrix. The numbers generated on 5×5 matrix using knight's tour algorithm are converted to a single column. The secret image is divided into 5×5 pixel blocks and converted to a single column in a sequential order. Numbers generated using algorithm are now mapped to pixels positions and replaced based on the encryption block of pixels. The process of encryption is extended all over the image with 5×5 pixel blocks. The cover image is also divided into P x Q pixel blocks. Encrypted secret image is embedded at the last two-bit planes of cover image and extreme corner pixels. Once the pixel replacements is completed, block shuffling is performed and minimal knight's tour algorithm is performed to obtain Crypto-Stego image.

The cover image is represented by:

$$A(i,j) = \begin{bmatrix} A(0,0) & A(0,1) \cdots\cdots & A(0,N-1) \\ A(1,0) & X(1.1) \cdots\cdots & A(1,N-1) \\ \vdots & \vdots & \vdots \\ A(M,0) & A(M,1) \cdots\cdots & A(M-1,N-1) \end{bmatrix}$$

where $M = N$.

Secret image is represented by:

$$B(m,n) = \begin{bmatrix} B(0,0) & B(0,1) \cdots\cdots & B(0,K-1) \\ B(1,0) & B(1.1) \cdots\cdots & B(1,K-1) \\ \vdots & \vdots & \vdots \\ B(L,0) & B(L,1) \cdots\cdots & B(L-1,K-1) \end{bmatrix}$$

where $K = L = M/2$.

Secret image $B(m,n)$ is divided into 5×5 pixel blocks first block is represented by:

$$B_1(m,n) = \begin{bmatrix} B(0,0) & B(0,1) \cdots\cdots & B(0,4) \\ B(1,0) & B(1.1) \cdots\cdots & B(1,4) \\ \vdots & \vdots & \vdots \\ B(4,0) & B(4,1) \cdots\cdots & B(4,4) \end{bmatrix}$$

Knight's tour algorithm is produced based on the L-shape knight's move in chess based on its current position. Few of the moves are represented in the Fig. 3. Once the Knight visits a position, it is grayed out or marked as full and not allowing knight to visit the same position again (Figs. 4, 5). A Knight can have a maximum option to have one among 8 positions to move when it is placed at the center and a minimum of 2 positions to move when it is placed at the corner. Based on the present position of knight, number of possible positions available for next move is decided by:

$$\{(x+2,y+1),\ (x+2,y-1),(x-2,y-1),(x-2,y+1),$$
$$(x-2,y-1),(x-2,y+2),(x+1,y-2)(x+1,y+2)\}.$$

This encrypted image is embedded into 7th and 8th bit planes of cover image using LSB-based steganography to obtain the stego image and a block shuffling is performed using block flip operation to get crypto-stego image represented by:

$$S(i,j) = \begin{bmatrix} S(0,0) & S(0,1) \cdots\cdots & S(0,N-1) \\ S(1,0) & S(1.1) \cdots\cdots & S(1,N-1) \\ \vdots & \vdots & \vdots \\ S(M,0) & S(M,1) \cdots\cdots & S(M-1,N-1) \end{bmatrix}$$

where $M = N$.

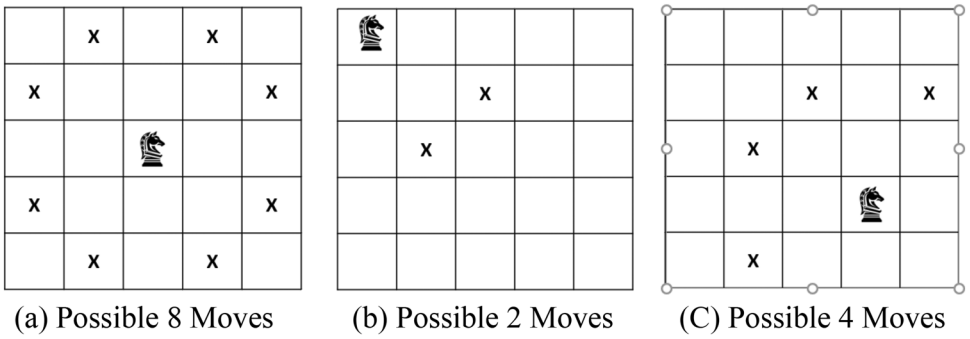


Fig. 3 **a** Possible 8 moves, **b** possible 2 moves, **c** possible 4 moves

158	200	94	255	158
15	176	35	45	221
180	44	196	100	0
113	25	64	88	234
200	185	96	4	33

→

94	221	200	113	158
234	0	255	180	185
45	200	33	15	25
100	88	35	96	44
158	4	196	64	176

Fig. 4 Secret image block of 5×5 before and after applying Knight's Tour algorithm

B11	B12	B13	B14
B21	B22	B23	B24
B31	B32	B33	B34
B41	B42	B43	B44

→

B44	B43	B42	B41
B34	B33	B32	B31
B24	B23	B22	B21
B14	B13	B12	B11

Fig. 5 Before and after block shuffling using flip method

Decryption Process

Decrypting the secret image from crypto-stego image is exactly reverse of embedding process. The crypto-stego image is divided into $P \times Q$ pixel blocks and inverse block shuffling algorithm is applied to get stego image from the 7th and 8th bit planes of stego image-encrypted secret image is extracted.

The encrypted secret image is divided into 5×5 pixel blocks and converted to a single column in a sequential order. Knight's tour algorithm performed on 5×5 block to generate the numbers is mapped with the encrypted image to get the secret image information. The representation of image and mathematical calculations is same as embedding process.

Algorithm for Embedding and Decrypting Secret Image

Algorithm 1: Embedding Secret Images

Step 1: Read Cover-Image and Secret-Image of size *N* x *N* and *N/2* x *N/2* respectively
Step 2: Convert Cover-Image into its RGB components.
Step 3: Convert Secret-Image into its RGB components.
Step 4: Divide Secret-Image '*R*' component into 5 x 5 pixel blocks and convert it to a single column.
Step 5: Perform knight's tour on 5 x 5 matrix and convert it to a single column.
Step 6: Perform pixel replacement based on the numbers generated using Knight's tour to get crypto image.
Step 7: Embed the encrypted '*R*' component Secret-Image in Cover-Image using LSB replacement technique and extreme edges.
Step 8: Divide '*R*' component of Cover-Image into *P* x *Q* pixel blocks and perform block shuffling to get the '*R*' component Stego-Image
Step 9: Repeat the steps for '*G*' and '*B*' components
Step10: Combine RGB Component to get stego image

Algorithm 2: Extracting Secret Images

Step 1: Read Stego-Image.
Step 2: Convert Stego-Image into its RGB components.
Step 3: Divide R component of Stego-Image in to *P* x *Q* pixel and perform inverse block shuffling.
Step 4: Extract the encrypted Secret-Image '*R*' component using LSB bit replacement and from extreme edges.
Step 5: Divide the extracted image into 5 x 5 pixel bloks and convert to a single column.
Step 6: Decrypt the Secret-Image using Knight's tour algorithm.
Step 7: Repeat the steps for G and B components.
Step 8: Combine RGB planes separately to get key images.

Block shuffling using flip is performed by

```
for i = 1: PBlock+1
        for j = 1: QBlock+1
                S(i,j) = R(PBlock+1-i, QBlock+1-j)
        end
end
```

Pseudocodes of Algorithm

Inserting secret image bits into LSB of cover image *A(i,j)*

Inserting secret image bits into LSB of cover Image *A(i,j)*

```
for i = 1:RowLength
        for j = 1:ColumnLength
                if MSBofA(i,j)==1
                        m= m+1;
                else
                        n= n+1;
                end
        end
        if (m>n and (MSBofA(i,j)==1)
                LSBofA(I,j) = MSBofB(i,j  )          ; %where MSBofA(i,j) =1
        elseif (m<n and (MSBofA(i,j)==0)
                LSBofA(i,j) = MSBofB(i,j)            ; %where MSBofA(i,j) =0
        else
                LSBofA(i,j) = LSBofA(i,j);
        end
end
```

Extracting secret image bits from LSB of secret image *S(i,j)*

```
for i = 1:RowLength
        for j = 1:ColumnLength
                if MSBofS(i,j)==1
                        m= m+1;
                else
                        n= n+1;
                end
        end
        if (m>n and (MSBofS(i,j)==1)
                MSBofB(i,j) = MSBofS(i,j) ;          %where MSBofS(i,j) =1
        elseif (m<n and (MSBofA(I,j)==0)
                MSBofB(i,j) = MSBofS(i,j) ;          %where MSBofS(i,j) =0
        else
                LSBofS(i,j) = LSBofA(S,j);
        end
end
```

Performance Evaluation

Performance Metrices

Mean square error (MSE) MSE is defined as the square of error between cover image and stego image and is given by:

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{1,j=1}^{M,N} (X(i,j) - Y(i,j))^2$$

Peak signal-to-noise ratio (PSNR) PSNR is defined as the peak signal-to-noise ratio, it is used to regulate the excellence of the image before and after crypto-steganography. The suitable value of PNSR for a typical 8-bit image is 30 to 50 dB and PSNR is calculated as:

$$\mathrm{PSNR} = 20.\log_{10}\left(\mathrm{Max}_{\mathrm{I}}\right) - 10.\log_{10}(\mathrm{MSE})$$

Structural similarity index measure (SSIM) It is a method for visualizing the apparent quality of an image by determining the similarity between two images. SSIM is based on three evaluation measurements between the input and output images given by luminance (l), contrast (c) and structure (s) mathematically represented by:

$$l(x,y) = \frac{2\mu_x\mu_y + c_1}{\mu_x^2 + \mu_y^2 + c_1} c(x,y) = \frac{2\sigma_x\sigma_y + c_2}{\sigma_x^2 + \sigma_y^2 + c_2} s(x,y) = \frac{\sigma_{xy} + c_3}{\sigma_x\sigma_y + c_3}$$

$$\mathrm{SSIM}(x,y) = [l(x,y)^{\alpha} + c(x,y)^{\beta} + s(x,y)^{\gamma}]$$

where μ_x is the average of x, μ_y is theaverage of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y, σ_{xy} is the covariance of x and y.

Performance Analysis

To measure the performance analysis, standard image data sets are used and results are calculated based on the performance metrices. PSNR and SSIM are calculated and tabulated in the results. PSNR is calculated before block shuffling. SSIM is calculated before and after block shuffling to find the structural similarity of the images. Though multiple levels of operations are performed, block shuffling and encryption operations are lossless process as it only changes the positions of pixels without modifying pixel value. The loss of redundant information encountered only during embedding process. Some images used in the proposed algorithm and its crypto-stego images are shown in Fig. 6.

The algorithm proposes a new way of securing the information in an image by encrypting and embedding in another image using minimal Knight's tour algorithm. The algorithm is implemented using m-script and is on standard set of images. PSNR and SSIM are calculated and tabulated in Table 1. Proposed algorithm is compared with existing algorithms and tabulated in Table 2. The existing algorithms are well suited for steganography but it does not involve the image encryption process. In the proposed algorithm, security is provided at multiple levels with the involvement of encryption and hiding process followed by block shuffling.

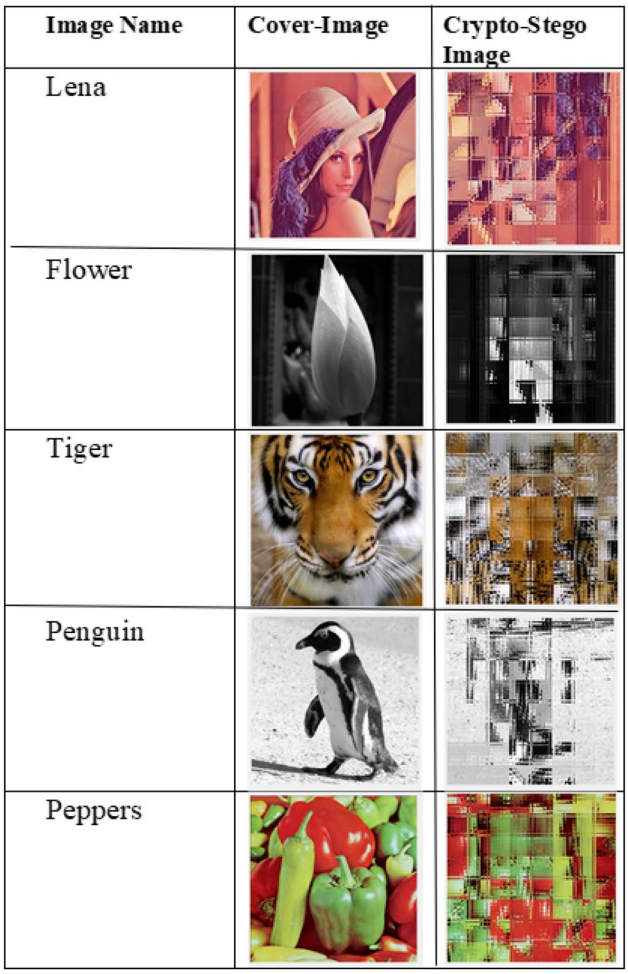


Fig. 6 Cover image and resultant crypto-stego image

Table 1 PSNR and SSIM obtained for different images

Image	PSNR	SSIM	
		Before block shuffling	After block shuffling
Lena	52.1980	0.9999	0.6644
Flower	52.0799	0.9927	0.2906
Tiger	52.2003	0.9992	0.2661
Penguin	52.0821	0.9931	0.1611
Peppers	52.2612	0.9998	0.5371

Table 2 Comparison of proposed algorithm with other methods

	Reversible data hiding method	DWT-LSB method	QR code steganography method	Multiple image steganography	DES encrypted steganography	Proposed algorithm
Encryption	No	No	Yes	No	Yes	Double encryption
MSE	1.5563	0.3716	0.6153	5.7161	0.2219	0.3909
PSNR (in dB)	46.21	52.43	50.24	40.56	54.67	52.21

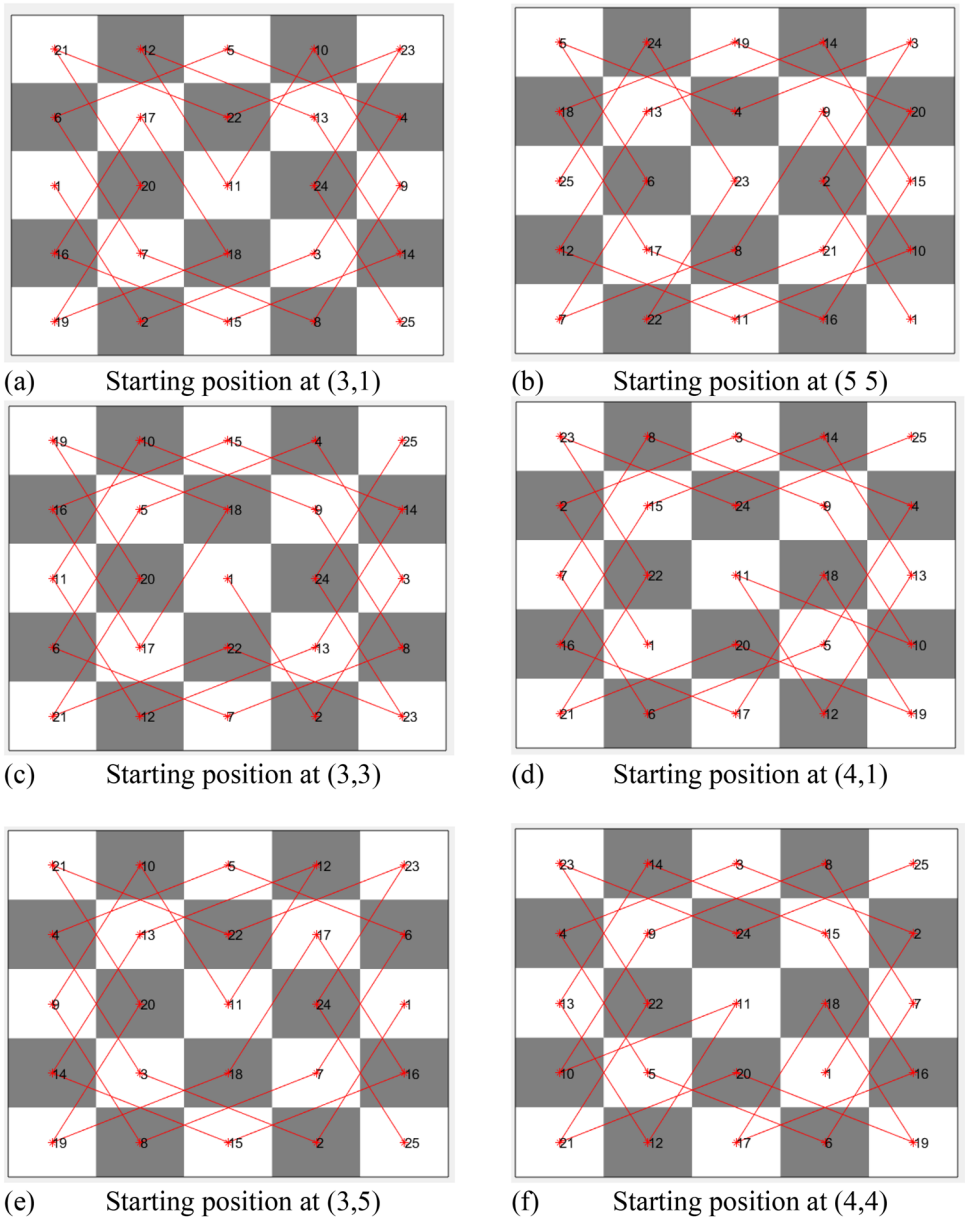


Fig. 7 Starting position of Knight's Tour at different positions

Some of the encryption pattern generated using a 5×5 Knight's tour algorithm starting with different positions are shown in Fig. 7a–f.

Conclusion

The image encryption and steganography performed using Knight's tour algorithm shows better results with

compromised PSNR and better SSIM. The pattern generated using the algorithm makes the encryption stronger with different starting positions. Same pattern is used for encryption and decryption, thus providing the integrity to data. The encrypted image is a result of lossless encryption process which involves only replacement of pixels without any modification to its value. The encrypted image is embedded into a cover image which is then shuffled using block shuffling or Knight's tour to obtain a crypto-stego image resulting in further security and confidentiality to information in an image with acceptable PSNR and better SSIM. The proposed algorithm provides security to an image resulting in encryption of secret image and is embedded in another image such that it is not visible to eavesdropper.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Ghosh D, Bhaduri U (2017) A simple recursive backtracking algorithm for knight's tours puzzle on standard 8×8 chessboard. In: 2017 international conference on advances in computing, communications and informatics (ICACCI), Udupi, pp 1195–1200
2. Bai S, Zhu G, Huang J (2013) An intelligent algorithm for the (1,2,2)-generalized Knight's tour problem. In: 2013 ninth international conference on computational intelligence and security, Leshan, pp 583–588
3. Younus ZS, Younus GT. Video steganography using Knight tour algorithm and LSB method for encrypted data. J Intell Syst. 2019;29(1):1–10.
4. Guo L, Ni J, Shi Y. Uniform embedding for efficient JPEG steganography. IEEE Trans Inf Forensics Secur. 2014;9(5):814–25.
5. Sedighi V, Cogranne R, Fridrich J. Content-adaptive steganography by minimizing statistical detectability. IEEE Trans Inf Forensics Secur. 2016;11(2):221–34.
6. Sadek M, Khalifa A, Mostafa M. Video steganography: a comprehensive review. Multimed Tools Appl. 2015;74(17):7063–94.
7. Sharma R, Sharma N (2016) A more private & secure e-mail system using image steganography (EPS) and data mining. In: International conference on advances in information communication technology and computing, Article no 104, pp 1–5
8. Suguna S, Dhanakoti V, Manjupriya R. A study on symmetric and asymmetric key encryption algorithms. Int Res J Eng Technol (IRJET). 2016;3(4):27–31.
9. Alexandre B, Richard D, Nuno A, Nuno L, Marco V. Understanding how to use static analysis tool for detecting cryptography misuse in software. IEEE Trans Relaib. 2019;68(4):1384–403.
10. Li T, Du B, Liang X. Image encryption algorithm based on logistic and two-dimensional Lorenz. IEEE Access. 2020;8:13792–805.
11. Singh M, Kakkar A, Singh M. Image encryption scheme based on Knight's Tour problem. Proc Comput Sci. 2015;70:245–50.
12. Delei J, Sen B, Wenming D (2008) An image encryption algorithm based on knight's tour and slip encryption-filter. In: International conference on computer science and software engineering, IEEE Computer Society, Hubei, pp 251–255
13. Bisht K, Deshmukh M (2020) Encryption algorithm based on knight's tour and n-neighbourhood addition. In: 2020 7th international conference on signal processing and integrated networks (SPIN), Noida, pp 31–36
14. El-Khamy SE, Korany NO, Mohamed AG. A new fuzzy-DNA image encryption and steganography technique. IEEE Access. 2020;8:148935–51.
15. Sharma N, Sauni I, Yadav AK, Singh P (2017) Phase-image encryption based on 3D-lorenz chaotic system and double random phase encoding. In: 3D Research 8, Springer, Article 39, pp 1–17
16. Zhang X, Peng F, Long M. Robust coverless image steganography based on DCT and LDA topic classification. IEEE Trans Multimed. 2018;20(12):3223–38.
17. Hameed MA, Hassaballah M, Aly S, Awad AI. An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. IEEE Access. 2019;7:185189–204.
18. Pal AK, Naik K, Agawal R. A steganography scheme on JPEG compressed cover image with high embedding capacity. Int Arab J Inf Technol. 2019;16(1):116–24.
19. Sharma VK, Srivastava DK, Mathur P. Efficient image steganography using graph signal processing. IET Image Process J. 2018;12(6):1065–71.
20. Horng J, Chang C, Li G. Steganography using quotient value differencing and LSB substitution for AMBTC compressed images. IEEE Access. 2020;8:129347–58.