# Rudrata's path based Image Encryption 

By

Arush Gupta
Student of Bhaskaracharya Pratishthan

## 1. Introduction

In ATMs, security of the transaction is of utmost importance, one weakness can affect thousands of people. Generally, no one can steal your money because your pin is encrypted. Encryption is what secures pretty much every virtual thing you own, from ATM password to cryptocurrency or even helping our country be one step ahead than our enemies. Hackers constantly try to break this encryption by a method of decryption. This is possible only if you know the encryption method which is known (mostly) by the amazing, truthful, loyal computers. For Example, encrypting the text "Hello Everyone" by a common encrypting method called hashing looks somewhat like
"044f2adcf0b76999bf209c9cef322acc83cc44e50deda1dc2f252051".
Even one small change like changing the "Hello" to "hello" would change the entire hash to
"73c6c1344b56fd197bac048aa0b489361fe4e1814b0b3a12adb37cbd".
The above encryption is done using "sha224" hashing algorithm. Like text encryption, Image Encryption is used in variety of places like keeping private photos safe on the cloud. There are various image encryption techniques which is used for different requirements, have its pros and cons. Here are some well-known techniques:

- Image Encryption using prime numbers and pseudo random generator
- Gaussian Elimination
- Image Encryption using DNA coding and Chaotic Maps

Some of the image encryption algorithms use grayscale images to encrypt that removes all color information, leaving only the luminance of each pixel. This paper will talk about image encryption using a Knight's tour.

## Knight and Knight's Tour

In the game of chess, a knight is a piece which moves in an $L$ shape shown as below. The arrow head represents the places the knight can go in one "L" move.


Figure 1: Knight's Moves

Using many such moves we can make "tour" in which our knight visits every square on the chess board only once. Knight tour comes under a broader topic of Hamiltonian path (a path that visits each "vertex" exactly once), which again comes under an even broader topic of Graph Theory (study of "graphs" used
to model relationships between objects. A "graph" is made up of vertices which are then connected by edges).

There are 2 types of knight tours, closed and open. Closed knight tours are the knight tours in which the first and the last squares of the knight tour can be connected by a knight move, while an open tour is when the first and the last squares cannot be connected via a knight tour. There are exactly $26,534,728,821,064$ closed knight tours in an $8 \times 8$ chessboard. Guess how many open tours there are on an $8 \times 8$ chessboard? Well, we do not know, there are truly a lot of them.

Here are some pictures were the knight tour of an $8 \times 8$ chessboard is represented by lines. As you can see, in Fig 2, the first knight tour is an open tour, while the rest of the knight tours are closed.


Figure 2: Knight's Tour on $8 \times 8$ represented by lines
Here the knight tour ( $8 \times 8$ ) are represented by numbers, where 1 corresponds to the first square the Knight lands (Starting square) and 2 corresponds to the $2^{\text {nd }}$ square the knight lands and so on. In Fig 3, the second knight tour is a closed one.

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


| 35 | 40 | 47 | 44 | 61 | 08 | 15 | 12 |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 46 | 43 | 36 | 41 | 14 | 11 | 62 | 09 |
| 39 | 34 | 45 | 48 | 07 | 60 | 13 | 16 |
| 50 | 55 | 42 | 37 | 22 | 17 | 10 | 63 |
| 33 | 38 | 49 | 54 | 59 | 06 | 23 | 18 |
| 56 | 51 | 28 | 31 | 26 | 21 | 4 | 09 |
| 29 | 32 | 53 | 58 | 05 | 02 | 1 | 24 |
| 52 | 57 | 30 | 27 | 20 | 25 | 04 | 07 |

Figure 3:Knight's tour represented by numbers
Here are some of the $8 \times 8$ knight tours which I found using the Diamond Square Method. This method envolves cutting the $8 \times 8$ chessboard into 4 equal quadrants then marking all of the squares as Diamond Left, Diamond Right, Square Left, or Square Right according to the pattern shown below


Figure 4:Dimond Square Method
Each quadrant can be filled using the following pattern. After choosing a starting square, let's take the bottom left square on the chessboard, we need to find which pattern does this square lie in. In our example the starting square starts in the Right Diamond system. Our plan will be to fill on of the squares in the right diamond system, in all the quadrants. Then we will switch to the Left/Right square system. Once again, we will fill all the squares in the system, in all of the quadrants. Then we will switch to the Left diamond system. Again, we will fill all the squares in the Left diamond system, in all of the quadrants. Then we can fill the rest of the squares easily.

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

Figure 5:The Knight's tours which I found
There are cases when a knight tour is not possible, such as on a $3 \times 5$ chessboard. Schwenk proved that for any $m \times n$ board where $m \leq n$, a knight tour is possible unless one or more of these conditions are meet.

- $m$ and $n$ are both odd
- $m=1,2,3,4$
- $m=3$ and $n=4,6$ or 8

And Cull et al and Conrad et al proved that for any rectangular board whose smaller dimension is at least 5 , there is a knight's tour.

## 2. History of Knight Tour

Some people credit Euler for the first solution of the knight tour, some people credit Rudrata, there is a constant fight on who solved the first knight tour. So what really happend?

9th century: Rudrata, Ratnakara, al-Adli

## Rudrata

Knight tours can be dated back to the $9^{\text {th }}$ century first made by a Kashmiri poet known by the name of Rudrata (Satananda). He is known for his great poetic work in Kavyalankara. Below is the shloka, given in his book Kavyalankara Chapter 5, Number 15 that gives the knight's tour of $4 \times 8$.

## सेना लीलीलीना नाली लीनाना नानालीलीली। नलीनालीले नालीना लीलीली नानानानाली || ३५ \|

His shloka shows the knight tour of $4 \times 8$. Here is his knight tour:

| 1 | 30 | 9 | 20 | 3 | 24 | 11 | 26 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 16 | 19 | 2 | 29 | 10 | 27 | 4 | 23 |
| 31 | 8 | 17 | 14 | 21 | 6 | 25 | 12 |
| 18 | 15 | 32 | 7 | 28 | 13 | 22 | 5 |

Figure 6:Rudrata's Knight's tour ( $4 \times 8$ )
This is a special shloka because when you read it in a knight tour of a $4 \times 8$ chess board given above, you get the same verse as you do when you read it normally.

से ना ली ली ली ना ना ली
ली ना ना ना ना ली ली ली
न ली ना ली ले ना ली ना
ली ली ली ना ना ना ना ली

This is when read in the Knight tour and when read normally.

By the way this shloka talks about military leadership.

## Ratnakara

After 15 years, a knight tour was presented in the book Haravijava. The author of this book was Ratnakara. He was also a well-known Kashmiri poet. Here is his knight tour.

| 26 | 11 | 24 | 5 | 20 | 9 | 30 | 7 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 23 | 4 | 27 | 10 | 29 | 6 | 19 | 16 |
| 12 | 25 | 2 | 21 | 14 | 17 | 8 | 31 |
| 3 | 22 | 13 | 28 | 1 | 32 | 15 | 18 |

Figure 7:Ratnakara's knight's tour

This is a special knight tour because it can be flipped and rotated 180 deg and combined with the original knight tour to get an $8 \times 8$ chessboard's closed knight tour. This is shown below.

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

Figure 8:Ratanakara's $8 \times 8$ knight's tour
As you can see, the part of the knight tour which is in the green box is the same as the knight tour in Fig 6. The part of the knight tour which in the orange box is just the mirror image, 180 deg rotation and addition of 32 from Fig $6.1+32=33$ shown diagonal to 1 , and so on.
al-‘Adli

Another 12 years past when al-'Adli (Persian world champion in chess) published his book about chess, namely Kitab ash-shatranj. What was written in his complete book has remained a mystery, but we know from a subsequent treatise from Abu Zakarya Yahya ibn Ibrahim al-Hakim that al-'Adli had mentioned a closed knight tour of a $8 \times 8$ chess board and also an open knight tour which he credits to Ibn Mani.

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

Figure 9:Left to Right, Ibu Mani's Knight tour and Al-adli's Knight tour
$14^{\text {th }}$ century: Sri Vedanta Desika
Sri Vedanta Desika

Fast forward to $14^{\text {th }}$ century when Sri Vedanta Desika shared what he had to say. He was a poet, devotee, philosopher, logician. He is also considered as an avatar of Venkateswar of Tirumalai. He belongs to the

Vishwamitra gotra. He wrote a poem consisting of 1008 verses praising footwear of Lord Ranganatha. Out of that one of them follows a knight tour. His knight tour is the same as Rudrata's. Here is the verse:

## स्थिरागसां सदाराध्या विहताकततामता ।

सत्पाढुके सरसा मा रङ्गराजपदं नय ॥

Reading the 929 verse in the knight tour will give you the 930 verse of his book.

| $\begin{gathered} \text { स्थि } \\ 1 \end{gathered}$ | $\begin{aligned} & \text { रा } \\ & 30 \end{aligned}$ | $\begin{aligned} & \hline \pi \\ & 9 \end{aligned}$ | $\begin{aligned} & \text { सां } \\ & \mathbf{2 0} \end{aligned}$ | $\begin{aligned} & \text { स } \\ & 3 \end{aligned}$ | $\begin{aligned} & \text { दा } \\ & 24 \end{aligned}$ | $\begin{gathered} \text { रा } \\ 11 \end{gathered}$ | $\begin{aligned} & \text { ध्या } \\ & 26 \end{aligned}$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $\begin{aligned} & \hline \text { वि } \\ & 16 \end{aligned}$ | $19$ | $\begin{aligned} & \text { ता } \\ & 2 \\ & 2 \end{aligned}$ | 29 | त | ता 27 | $\begin{aligned} & \text { म } \\ & \mathbf{4} \end{aligned}$ | ता |
| $\begin{gathered} \hline \text { स } \\ 31 \end{gathered}$ | $\begin{aligned} & \text { त्पा } \\ & \text { 8 } \\ & \hline \end{aligned}$ | $\begin{gathered} \hline \text { दु } \\ 17 \end{gathered}$ | के | स | $\begin{gathered} \text { रा } \\ \cdots \\ \mathbf{6} \\ \hline \end{gathered}$ | सा | मा |
| $18$ | - 15 | 32 |  | 28 | 13 | 22 | 5 |

Figure 10:Knight tour used by Sri Vedanta Desika

## $18^{\text {th }}$ century: Leonhard Euler

Leonhard Euler

Finally, we arrive at the famous mathematician, Leonhard Euler ( $18^{\text {th }}$ century). He was a swiss mathematician who made some important discoveries in many branches of math including knight's tour. Here is his first solution.

This is an open knight tour. This is not very different from the previous ones from Ibu Mani or al-Adli.

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

Figure 11: Leonhard Euler's Knight's tour

[^0]William Beverley

Also, in the $19^{\text {th }}$ century William Beverley shared his knight tour with the rest of the world. Here is the knight tour.


Figure 12:William Beverley's Magical knight's tour
This is also a very special knight tour, it is called a semi magical square because all the rows, columns add up to 260 , each of the quadrants add up to 520 , each of the rows and columns in the quadrant add up to 130 , each of the $2 \times 2$ squares sum up to 130 . Unfortunately, the diagonals do not add up to the required 260. So, this is a semi magical knight tour. But mathematicians found 140 different semi-magical squares.

## Krishnaraja Wodeyar III

Back to India, in 1852, Krishnaraja Wodeyar III, King of Mysore and a writer, was third to compose a semi magical knight tour on $8 \times 8$ chessboard which he then had printed on a silk panel. His knight tour is shown here.

As you can see, this is a closed semi magical knight tour, in which too, the columns and the rows, add up to 260 , the quadrants also add up to 520 , but the rows and columns of the quadrant do not always add up to 130 though, the $2 \times 2$ squares also do not add up to 130 .

| 11 | 46 | 21 | 52 | 13 | 44 | 19 | 54 |  |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 22 | 49 | 12 | 45 | 20 | 53 | 16 | 43 |  |
| 47 | 10 | 51 | 24 | 41 | 14 | 55 | 18 |  |
| 50 | 23 | 48 | 9 | 56 | 17 | 42 | 15 | 260 |
| 35 | 8 | 25 | 64 | 29 | 40 | 57 | 2 |  |
| 26 | 63 | 36 | 5 | 60 | 1 | 30 | 29 |  |
| 7 | 24 | 61 | 28 | 37 | 32 | 3 | 58 |  |
| 62 | 27 | 6 | 33 | 4 | 59 | 38 | 31 |  |

Figure 13: Krishnaraja Wodeyar III's Magical Knight's tour

## 3. KnightCryption Algorithm

Here are KnightCryption algorithm's results from encrypting an image using the knight tour. I have used Python programming language on an 8GB laptop to get these results in $\sim 90$ secs for the entire operation. (Encrypting and decrypting).

This is the test image with size $640 \times 480$.


Figure 14:Original Image

This is the encrypted image, achieved by arranging parts of an image according to the knight's tour. This is done twice, $1^{\text {st }}$ level and $2^{\text {nd }}$ level. More about that later. The size of this encrypted image is 1600 x 1600.


Figure 15:Encrypted Image

This is what I get after decrypting the encrypted image. I rearrange the squares according to the levels to get back a copy of the original image. The size of this image is also $1600 \times 1600$. This is why the GSLV looks a bit thinner In this image.


Figure 16:Decrypted Image

## Explaining KnightCryption

So, how did I achieve these results? Here is the flowchart.

*Note I am using the solution of a $16 \times 16$ chessboard's knight tour. Image stands for the input image, the image to encrypt. This image is then passed to the "CHOPPER". The chopper chops the image into $16 \times 16$ smaller images, which I store in a list. This list is passed into the square arrange method. This method is where the story revolves. Let's see how this method works. I have the solution of the knight tour, and the chopped images stored in a list, we will label each image starting from 1 to 256 . Our knight tour solution should look like this:
[
[1, 126, 191, 196, 5, 122, 187, 200, 9, 120, 183, 202, 11, 118, 181, 204],
$[192,195,2,125,188,199,6,121,184,1201,10,119,182$, 203, 12, 117],
...
]
You see, have the same numbers we used to label the images, in a different format, what is left is to arrange the chopped images according to the knight tour. So, arrange square method, just creates a new
list, in which the chopped images are rearranged, then it combines all the images to reform the real image. This image should look like a puzzle put in a wrong fashion. This looks like this, I have numbered the squares to help you understand the knight tour arrangement.


Figure 17: Image after Square arrange 1
But we want more distortion. For that we repeat this process but in a smaller scale. "Chopper small" breaks the given image again to $16 \times 16$ small images, then it chops every small square into $16 \times 16$ very small images and appends them to a list. This list is then passed into the square arrange method again. So, it rearranges the very small squares to recreate the small squares. After all small squares have been rearranged, the small squares are combined again to for the semi-final encrypted image.

The semi-final encrypted image could be where we can stop, but let's just change the colors so that nobody can relate our GSLV real image from our encrypted image. The semi-final encrypted image is passed into the Color Changer. This method takes in an image, flips it's colors (white to black and black to white) and returns the flipped image.

For Decryption we go through a reversal process and achieve the decrypted image. The various tests on the images show satisfactory results on encryption and decryption.
*Note that the knight tour solution and the "values" in the Color changer should be known in both sides of the communication.

## Conclusion

Knight Tour is part of recreational mathematics. The Knight tour were invented through verses of Rudrata and Ratnakar. Rudrata path is also called Hamiltonian path now a days, so the origin of Hamiltonian path can be traced in Rudrata work from Ancient India. Surprisingly in today modern world it has great application, picture or image cryptography by dividing the picture in squares and using the Knight tour to encrypt is practically used and the decryption depends on knowledge of tour solution and the values in color change. In general, due to vast number, enormous number of possible Knight tour it is very difficult to obtain the decryption key for any unauthorized person.

## 4. References

1. https://pdfs.semanticscholar.org/7b2b/db1447a8b23a257675462c304c3e0ae7be9f.pdf
2. http://ijarcsse.com/Before August 2017/docs/papers/Volume 6/8 August2016/V6I6-0334.pdf
3. https://en.wikipedia.org/wiki/Rudrata
4. https://sreenivasaraos.com/tag/knights-tour-problem/
5. https://www.youtube.com/watch?v=ab dY3dZFHM
6. https://www.youtube.com/watch?v=9fSFCOOZKPg
7. https://www.youtube.com/watch?v=8tBP6uFWQv4
8. https://www.youtube.com/watch?v=6XZE67N IuQ
9. https://www.youtube.com/watch?v=Ma1C6wcROJg
10. https://en.wikipedia.org/wiki/Knight\'s tour
11. https://opencv-python-tutroals.readthedocs.io/en/latest/
12. https://www.youtube.com/watch?v=DjZB9HvddQk\&list=WL\&index=14
13. https://en.wikipedia.org/wiki/Rudrata https://en.wikipedia.org/wiki/Hamiltonian path
14. https://archive.org/details/KavyamalaVol02KavyalankaraOfRudrata1886 201803
15. https://www.geeksforgeeks.org/warnsdorffs-algorithm-knights-tour-problem/
16. https://en.wikipedia.org/wiki/Knight\'s tour
17. https://www.techiedelight.com/print-possible-knights-tours-chessboard/
18. https://support.sas.com/resources/papers/proceedings15/3060-2015.pdf
19. https://math.stackexchange.com/questions/2013656/knights-tour-on-4x4-and-8x8-chess-board
20. https://www.mayhematics.com/
21. http://eulerarchive.maa.org/hedi/HEDI-2006-04.pdf
22. https://www.johndcook.com/blog/magic knight/
23. https://fr.wikipedia.org/wiki/Al-Adli
24. https://www.ibiblio.org/sripedia/ebooks/vdesikan/rps/knight.html
25. https://www.youtube.com/watch?v=oPxxhzl1dF0
26. https://blog.storagecraft.com/5-common-encryption-algorithms/
27. https://www.wisdomlib.org/definition/rudrata
28. http://math.oregonstate.edu/~math reu/proceedings/REU Proceedings/Proceedings2002/200 2AL McGown.pdf

[^0]:    19 ${ }^{\text {th }}$ century: William Beverley, Krishnaraja Wodeyar III

