BIOMETRIC STEGANOGRAPHY USING MID POSITION VALUE TECHNIQUE

A. LAKSHMI KEERTHI, K. RAMBABU

1.PG STUDENT, D.N.R. COLLEGE, P.G. COURSES (AUTONOMOUS), BHIMAVARAM-534202.

Emailid: alapatilakshmikeerthi123@gamil.com

1. Assistant Professor in DEPARTMENT OF MASTER OF COMPUTER SCIENCE, BHIMAVARAM-534202.

Email:kattarambabudnr@gamil.com

ABSTRACT

Biometric data, is prone to attacks and threats from cyber criminals to conduct identity theft, and its economic value makes it a product that can be traded in underground marketplaces such as the dark web. Securing it is the need of the hour. Sensitive data is subsequently in danger throughout a biometric identification system, and therefore the security measures implemented to guard this data must cover all contingencies. A steganographic approach is proposed as a solution to this. Biometrics are hidden inside other biometrics for safe storage and secure transmission. Steganography is a process of hiding data in a transmission medium. The main objectives while hiding data are its undetectability, robustness against image processing and other attacks, which steganography can easily achieve.

This project focuses on a process of hiding an image in another image by using mid position value(mpv) technique. Here we have to choose the secret biometric on which Arnold transform will be applied resulting in a scrambled version of the secret biometric. This will be embedded into the cover image resulting in a stego image. Lastly, the hidden secret biometric will be decoded from this stego image, which will first result in a scrambled secret biometric. Inverse Arnold Transform will be applied on this to finally result in the decoded secret biometric.`

1. INTRODUCTION

The majority of present-day authentication and verification systems are dependent on things like user's memory power and traits, which requires users to remember multiple passwords or to possess tokens that, for example, generate one-time pin (OTP) numbers. However, these passwords and pins are often forgotten by the users or can become risky if they are written down. Sometimes, tokens can be lost, and the access to the required services is not possible until and unless the token is found or replaced. An individual's behavioral, as well as physiological attributes, can identify a specific person uniquely, using their personal features so that there is no need to remember passwords or carry a note. The advantage with using biometrics is that these biometric characteristics do not need to be remembered. They do not get lost easily. While this biometric user-authentication and verification is convenient to use, it does make the safety of the digitised biometric data a critical matter. If this data is accessed by any hacker, it is often wont to conduct attacks by various means. Identification of persons by way of biometric features is an emerging phenomenon. Over the years, biometric recognition has received much attention due to its need for security. Amongst the many existing biometrics, fingerprints are considered to be one of the most practical ones. Techniques such as watermarking and steganography have been used in attempt to improve security of biometric data. Watermarking is the process of embedding information into a carrier file for the protection of ownership/copyright of music, video or image files, whilst steganography is the art of hiding information.

2. LITERATURE SURVEY AND RELATED WORK

This section surveys the existing biometric based authentication systems developed to achieve security. Venkatraman and Geetha [8] focused on hiding images by specialized steganographic image authentication (SSIA) method in cluster based cloud systems. The SSIA technique is employed for virtual elastic clusters in the public cloud environment. Now, the SSIA method embeds the image data by genetic operator and blowfish technique. At first, the blowfish approach is employed on the image and later the genetic operator is employed to reencrypt the image data. The presented method gives enhanced security compared to traditional blowfish method in a cluster based cloud scheme. Khudher [9] designed a Steganography Biometric Imaging System (SBIS). This scheme obtains RGB foot tip image and pre-process it to get foot templates. Later, chain code is demonstrated for individual data with the foot template image by Least Significant Bit (LSB). The precise identification process is executed by artificial bee colony optimization (ABC).

Sudhakar and Gavrilova [10] proposed a cancellable biometric architecture depending upon deep learning (DL) method on the cloud. They determine that cloud is a better resolution for biometric system whereas quick response times, intensive computation, and higher accurateness is needed. In Banerjee et al. [11], a novel security method was determined by creating the scheme more secure using steganography together with biometric security. domain of an image.

Das et al. [12] presented an effective and secured lip biometric architecture. Different from the conventional biometric architecture, which emphasis on the identification accurateness only, but they concentrate on both detection rate together with secured template stored in the biometric scheme. It involves preprocessing to improve the local feature of the lip image. The local interest point is identified by Scale Invariant Feature Transform (SIFT) that is utilized to extract the lip feature. AL-Kateeb and AL-Bazaz [13] proposed a method for hiding private data in colourful images depending upon the features of engineering dimension of the human hand as all kinds of biometrics; they extract several features and process them to create a matrix which states the mapping of distribution of private data in the cover image. The presented technique was employed for several images to hide a group of private messages and visual quality of the cover image wasn't influenced afterward the concealment. The real-world result explains the performance of this technique that was measured base on relation among the original image after and before concealments.

Kayode et al. [14] proposed a method for securing eye retina template by steganography. The research analysis was performed on matrix laboratory (MATLABR2015A) platform. The segmented eye retina region was standardized to reduce the dimension variations among eye retina regions using Hough transform (HT). The feature of the eye retina has been encoded by convolving the standardized eye retina region with 1D Log Gabor filters to create a bitwise biometric template. Later, LSB was utilized for securing the eye retina template. The Hamming distance was selected as a matching metric that provides the measure of several bits disagreed among the templates of eye retina. Abikoye et al. [15] integrate Cryptography (Two fish and Triple data decryption (3DES)) method and Steganography LSB for solving the challenge of hacking/attacking biometric template for a malicious act that becomes a major challenge in the eye retina detection scheme. In this study, HT, Log Gabor filter, and Daugman rubber sheet model have been utilized to normalization feature extraction, and eye retina image segmentation as well as the eye retina template created was encrypted by Two fish and 3DES methods. The cipher image is later embedded into a cover image for producing stego image by LSB. Atighehchi et al. [16] proposed a transformation based biometric template protection system as an enhancement of BioHashing method whereas the projection matrix is made by integrating the biometric and secret data. Study outcomes on 3 biometric modules like hands vein images, digital fingerprint, and finger knuckle print display the advantage of the presented technique faces to an attack when maintaining a better performance.

3. EXISTING SYSTEM

Image Steganography is a process of hiding images or text in other images. This method is implemented in many areas. There are two main domains in Image Steganography, they are Spatial Domain Methods, which consist of techniques like least significant bit, pixel value differencing, Pixel mapping method, MSB bit difference method, Mid value position Technique (MPV). The other Method is Transform Domain method, which consists of techniques like discrete cosine transformation technique (DCT), Discrete Fourier transform (DFT), Discrete wavelet transform (DWT). These methods are implemented for Image in Image Steganography, and Text in image steganography, for general information.

However, securing biometric images is superior to hiding normal images, as it will aid in data security and privacy.Compared to all the techniques which are used for performing the image steganography, mpv has the most similarity index with the cover image.

Similarity index is a measure to compare the similar-ness of the stego-image with the cover image. The need to measure this is required to show that the stego-image does not give away any hints or clues with any distortion in the stego-image or disturbance in it, that there is an image hidden inside it. The stego-image should be very similar to the cover image, so that nobody will know that there is an image hidden inside it.

The below graph shows that, when compared to other techniques, the value of the mpv is very close to 1. It proves that the quality of the image is well maintained, i.e. the cover image and the stego-image are highly similar.

4. PROPOSED SYSTEM

The proposed algorithm is the technique called Mid Position Value(MPV) Technique. In this technique, a secret biometric image is hidden inside a chosen cover image, which is also a biometric image. This technique is basically a two-step process of Arnold transformation and embedding bits using mpv method. It is done by first scrambling the secret biometric image using Arnold transform and then embedding it inside the cover image, which results in a stego image. Finally the secret image is decoded from the stego image and Inverse Arnold Transform is applied to get the secret biometric image. The cover image is also a chosen biometric image, because, the basic idea of steganography is hiding of the information. So, the secret image is safe inside the other biometric image. The secret image is also scrambled and then embedded, since it will act as a double shield from threats and attacks.

5. IMPLEMENTATION

MODULES

DATASET

Sokoto Coventry Fingerprint Dataset (SOCOFing) is a biometric fingerprint dataset designed for academic research purposes. It is made up of 6000 fingerprint images from 600 African subjects.This dataset is used as the cover images for the project. The secret images can be chosen from the same dataset, or the user can upload his own fingerprints. SOCOFing contains unique attributes such as labels for gender, hand and finger name as well as synthetically altered versions with three different levels of alteration for obliteration, central rotation, and z-cut. The dataset is freely available for noncommercial research purposes

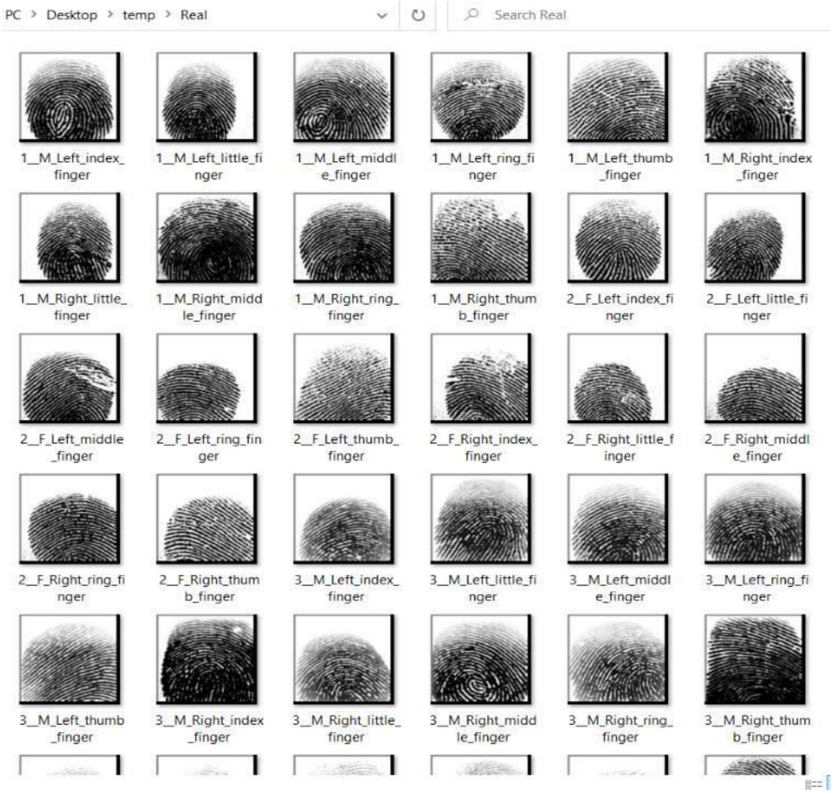


Fig 1- Dataset

ARNOLD TRANSFORMATION

Digital image scrambling can make an image into a completely different meaningless image during transformation, and it is a preprocessing during hiding information of the digital image, which also known as information disguise. Image scrambling technology depends on data hiding technology which provides non-password security algorithm for information hiding.

Data hiding technology led to a revolution in the warfare of network information, because it brought a series of new combat algorithms, and a lot of countries pay a lot of attentions on this area. Network information warfare is an important part of information warfare, and its core idea is to use public network for confidential data transmission. The image after scrambling encryption algorithms is chaotic, so attacker cannot decipher it. Some improved digital watermarking technology can apply scrambling method to change the distribution of the error bit in the image to improve the robustness of digital watermarking technology. Arnold scrambling algorithm has the feature of simplicity and periodicity, so it is used widely in the digital watermarking technology (Arnold transform is proposed by V. I. Arnold in the research of ergodic theory, it is also called catmapping, and then it is applied to digital image).

According to the periodicity of Arnold scrambling, the original image can be restored after several cycles. Because the periodicity of Arnold scrambling depends on the image size, it has to wait for a long time to restore an image. Generally, the cycle of Arnold transformation is not directly proportional to the image degree. Currently, Arnold scrambling algorithm is base on square digital image in most literature, and these images are mostly N×N pixels of the digital image. However, most of the digital images are non-square in the real world, so that we cannot use Arnold scrambling algorithm widely. To improve the Arnold scrambling algorithm, we will improve the original Arnold scrambling algorithm, so that we can apply Arnold scrambling algorithm to M×N non-square pixel digital image, it means the length and width of the image is not equal.

According to Arnold scrambling, the original image can be recovered after a certain number of iterations based on the size of the image. But the number of iterations will be different for different size of the images and the number of cycles does not follow any order. Currently, Arnold scrambling is applied to pixels only but it can be extended to blocks Alliance.

International Conference on Artificial Intelligence and Machine Learning (AICAAM), April2019 330 of the image also.

If the scrambling is performed on both pixels and blocks the robustness and security of the image can be improved. Arnold scrambling for pixels can be applied to any image of any size. But to apply Arnold scrambling to an image which is divided into blocks, the image size should be of order M×M. If the size of the image is not M×M, it can be made M×M by adding zeros to the image which is called as padding. Arnold transform is widely used in image stenography, authentication, tamper detection, self-recovery and image cryptography algorithms.

In all these cases, Arnold transform is used as a scrambling step in which the number of iterations is used as a key. Arnold transform for pixel scrambling is used in most of the applications and hence provides one key for the security. The coordinates of the pixels are scrambled first which is followed by the coordinates of the blocks and thus providing two levels of security for scrambling. If the first level descrambling is successful, then only the second level descrambling can be carried out. This increases the complexity of malicious and unauthorized descrambling of images. This scrambling proposes a two level image scrambling to increase the robustness of Arnold transform.

First, the plain image is divided into blocks and each block is assigned a coordinate. The block coordinates can be transformed through Arnold scrambling. Hence, each block of the image will get a new coordinate and gets scrambled. Once the blocks are scrambled and arranged as an image, pixel scrambling can be carried out to scramble all the pixels in the image. This two level can also be implemented by doing pixel scrambling first which is followed by block scrambling.

TWO LEVEL ARNOLD

First, the plain image is divided into blocks and each block is assigned a coordinate. The block coordinates can be transformed through Arnold scrambling. Hence, each block of the image will get a new coordinate and gets scrambled. Once the blocks are scrambled and arranged as an image, pixel scrambling can be carried out to scramble all the pixels in the image. This two level algorithm can also be implemented by doing pixel scrambling first which is followed by block scrambling.

A.BLOCK SCRAMBLING :

In block scrambling, image is divided into M×M blocks and each block is assigned a coordinate {m,n} according to their spatial orientation. For an image of size 512×512, image can be divided into 64×64 blocks. Hence, there are spatial coordinates in the set of {(1,1), (1,2),…,(1,8),…,(8,1),(8,2),…,(8,8)}. Arnold scrambling is applied to the coordinates of blocks and hence each coordinate is assigned a new coordinate as given by equation (2). This paper proposes a block scrambling method for the blocks with same spatial resolution. This is possible only when the input image I(x,y) is of spatial resolution 2n ×2n ; where n=1,2,3,…,N. Scrambling of blocks through Arnold transform is given as follows.

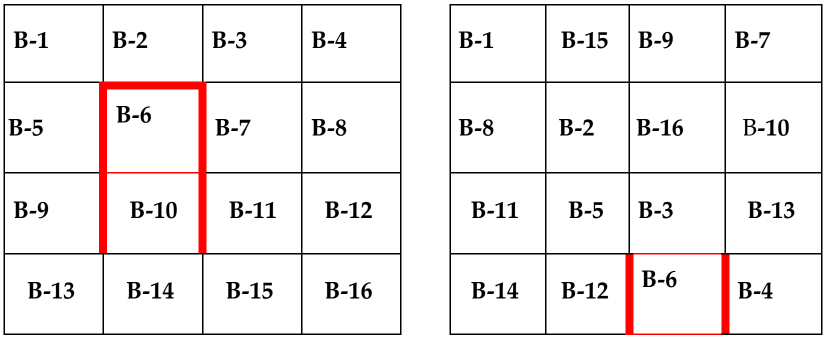
$[\ \{B(xi)\}\ \{B(yi)\}\ ] = [\ 1\ 1\ 1\ 2\ ][\ \{B(xi-1)\}\ \{B(yi-1)\}\ ]$

(mod M) (5) Where B(xi ,yi) is the coordinate of the block of an image. M is number of rows or number of columns of all the blocks.

B. ILLUSTRATION OF ARNOLD BLOCK SCRAMBLING:

First, the image is divided into blocks. For example, a 512 x 512 image is converted into blocks of size 128 x 128. Then the image will be divided into 16 blocks as shown in Fig.

When Arnold scrambling is applied to blocks then the positions of blocks will get shifted.



B-1	B-2	B-3	B-4
B-5	B-6	B-7	B-8
B-9	B-10	B-11	B-12
B-13	B-14	B-15	B-16

B-1	B-15	B-9	B-7
B-8	B-2	B-16	B-10
B-11	B-5	B-3	B-13
B-14	B-12	B-6	B-4

Fig 2 Illustration of Arnold block scrambling

Let us consider block6 whose original position is at (2, 2) but after scrambling the position of block6 is shifted to new position i.e., (4, 3) for one iteration. For further iterations the input will be the output of previous iteration.

C.SCRAMBLING PROCESS

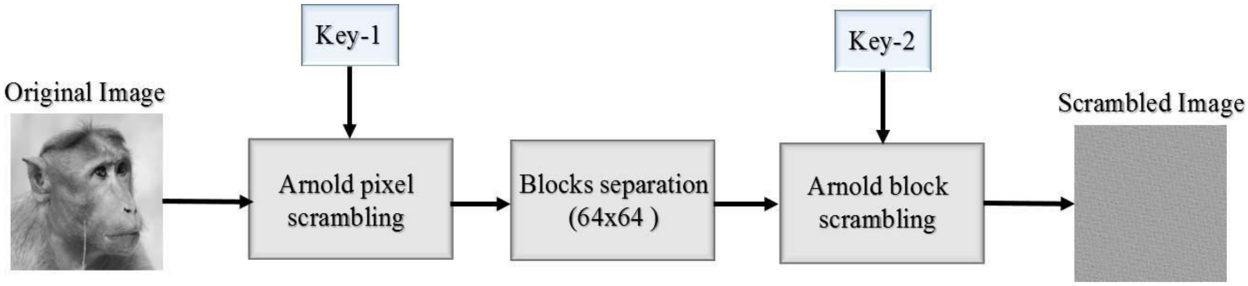


Fig 3 Scrambling process

In the scrambling process, the original image is scrambled in two levels as shown in Fig. 2. In the first level the image is subjected to pixel Arnold scrambling with a specific number of iterations. The information related to number of iterations of level1 will be in key1 (K1). The scrambled image is divided into 8 x 8 blocks. In the second level the divided image is subjected to block Arnold scrambling with other specified number of iterations. The information of number of iterations of second level scrambling will be in key2 (K2). The image obtained after the second level scrambling is the image that will be transmitted.

D. DESCRAMBLING PROCESS

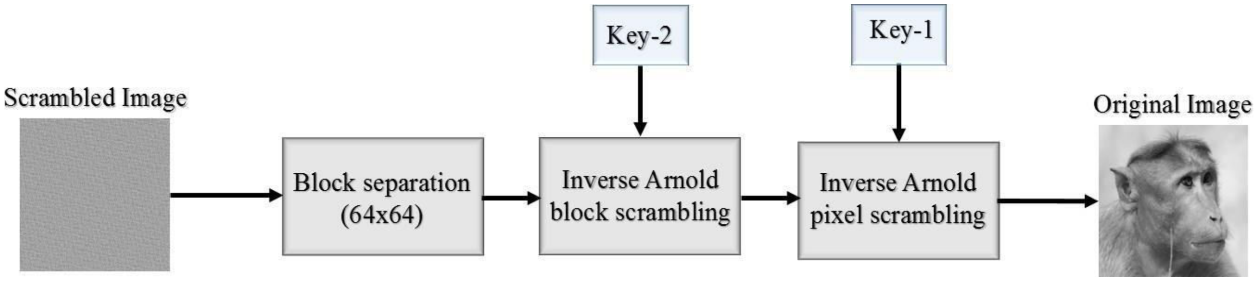


Fig 4 Descrambling Process

Same as scrambling, the original image will be extracted in two levels as shown in Fig 3. The scrambled image is divided into blocks and inverse block Arnold scrambling is applied based on key2. In the second level, the obtained image after the inverse block Arnold scrambling will be subjected to pixel level inverse Arnold scrambling based on key1. The obtained image after the second level is the original image.

Image scrambling technology depends on data hiding technology which provides nonpassword security algorithm for information hiding.

Data hiding technology led to a revolution in the warfare of network information, because it brought a series of new combat algorithms, and a lot of countries pay a lot of attentions on this area.

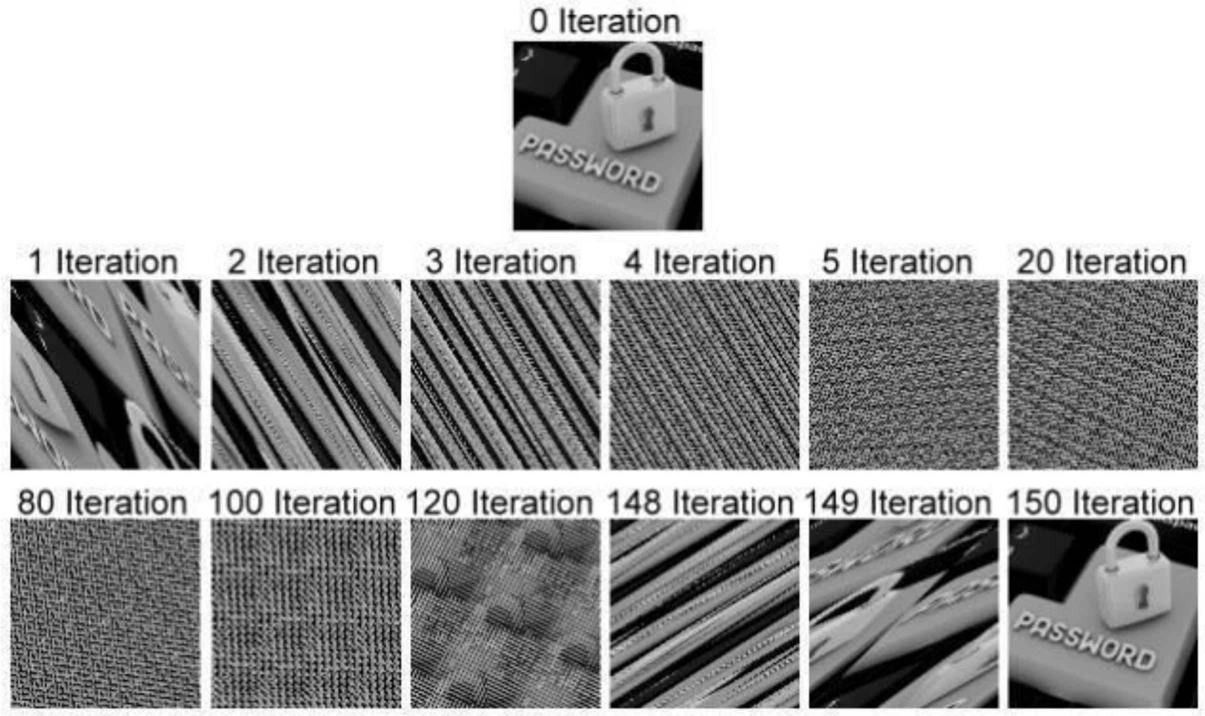
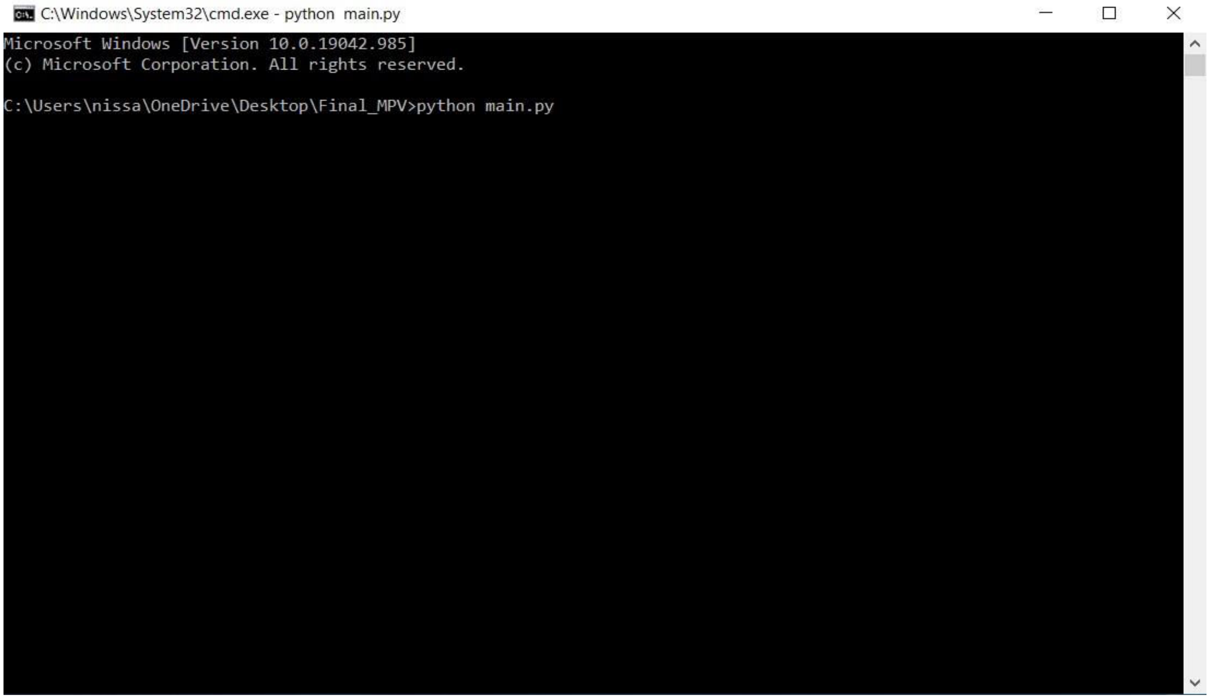


Fig 5 Sample Arnold Transformation

6. RESULTS AND DISCUSSION SCREEN SHOTS



```
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\nissa\OneDrive\Desktop\Final_MPV>python main.py
```

Fig 5 execution page

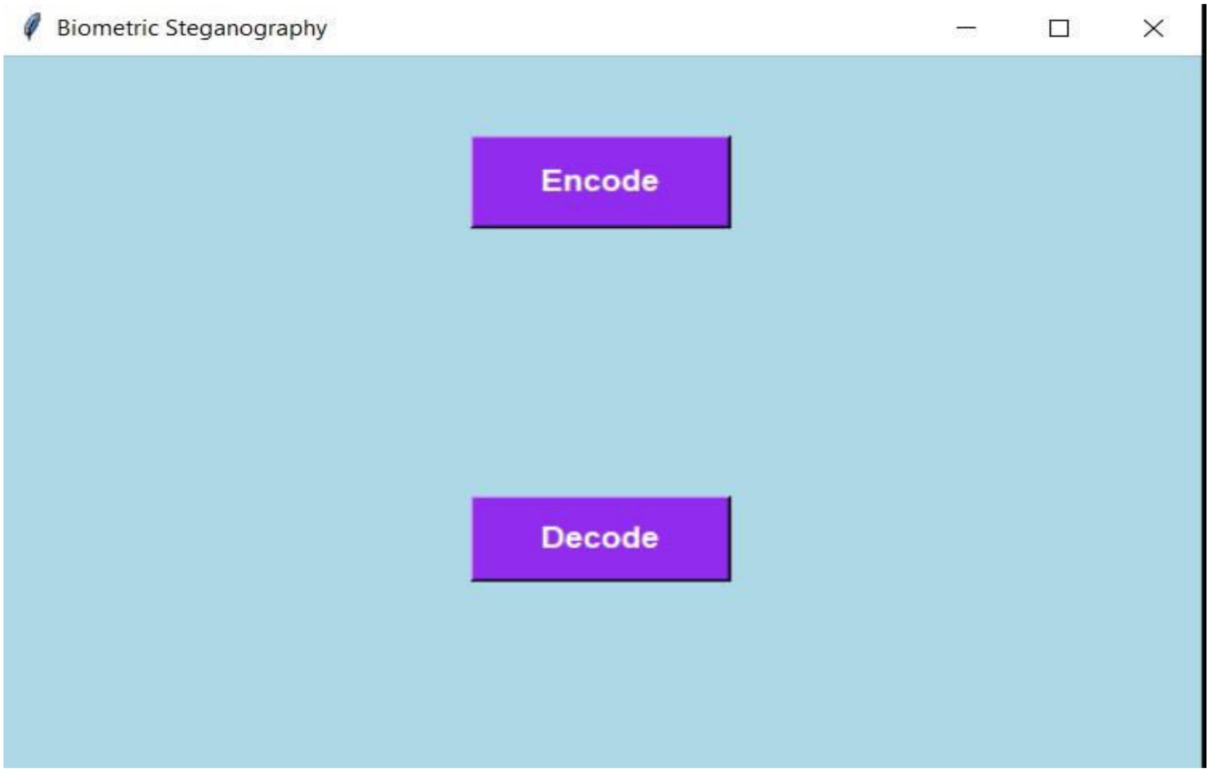
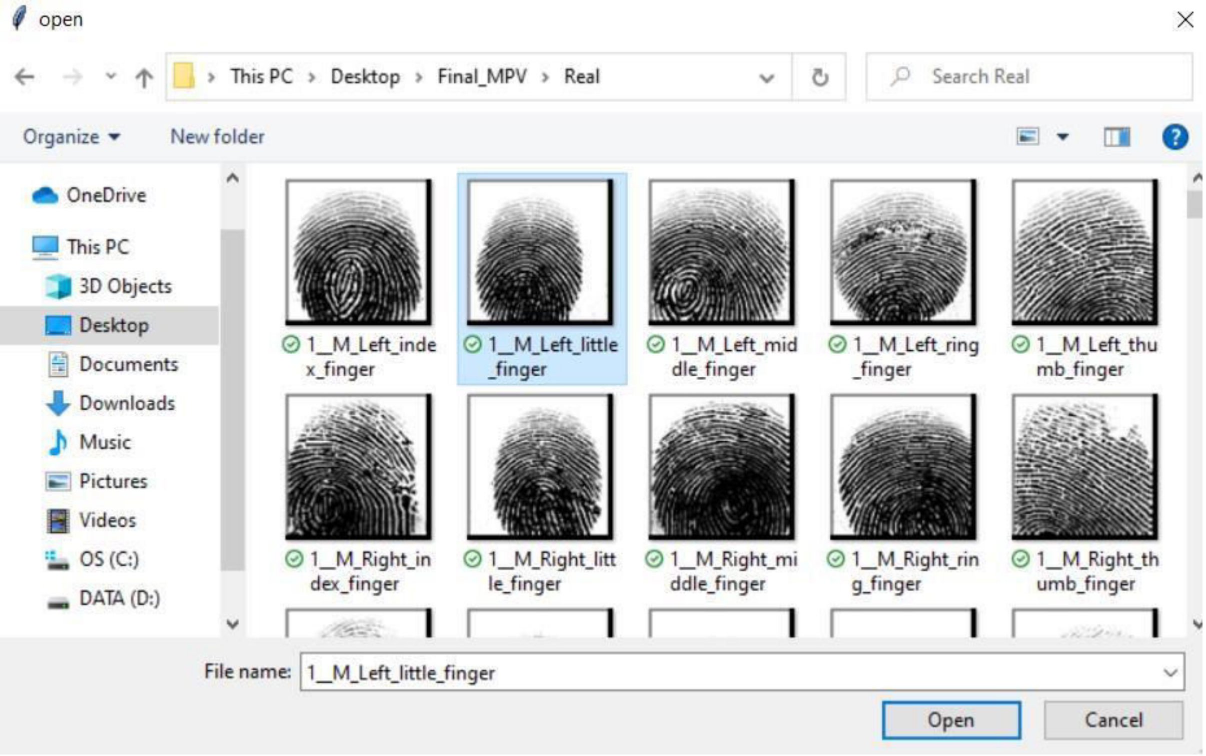


Fig 6 Student Dashboard



File name: 1_M_Left_little_finger

Fig 7 Selecting the secret image

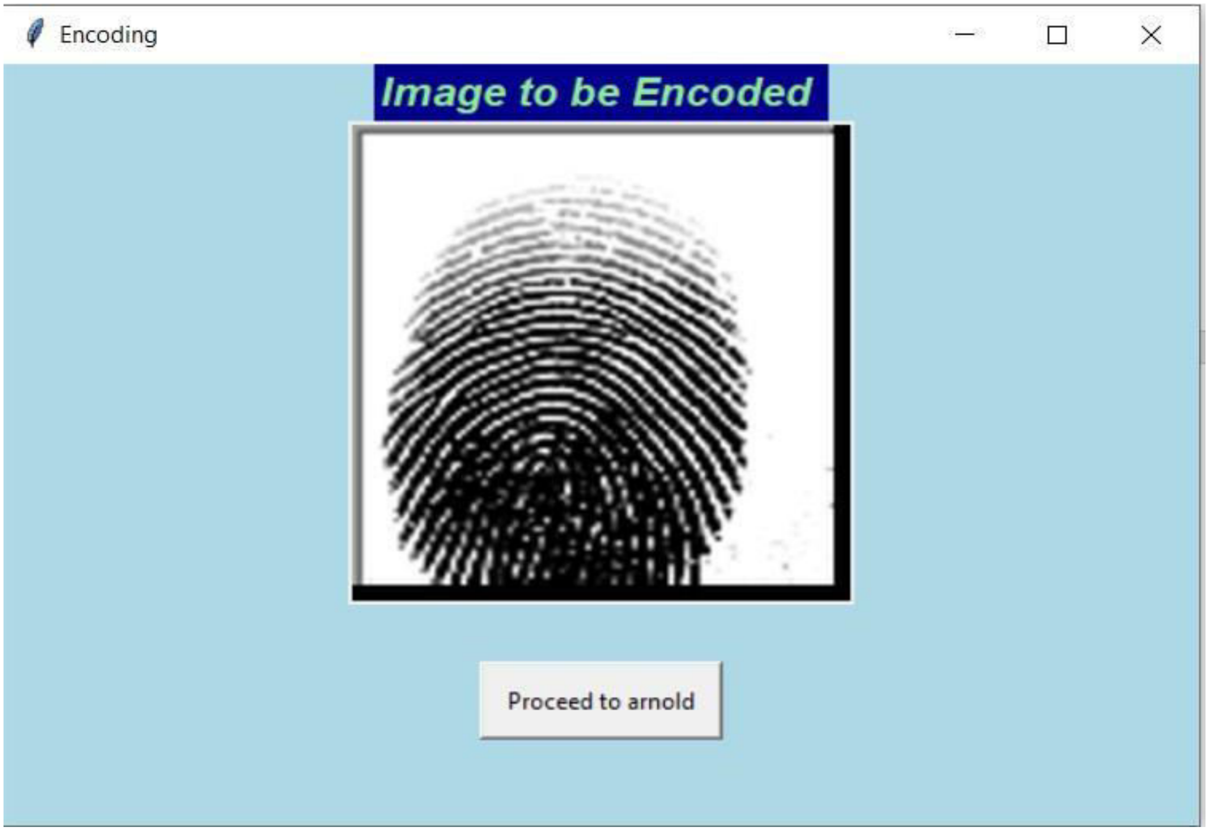


Fig 8 secret image

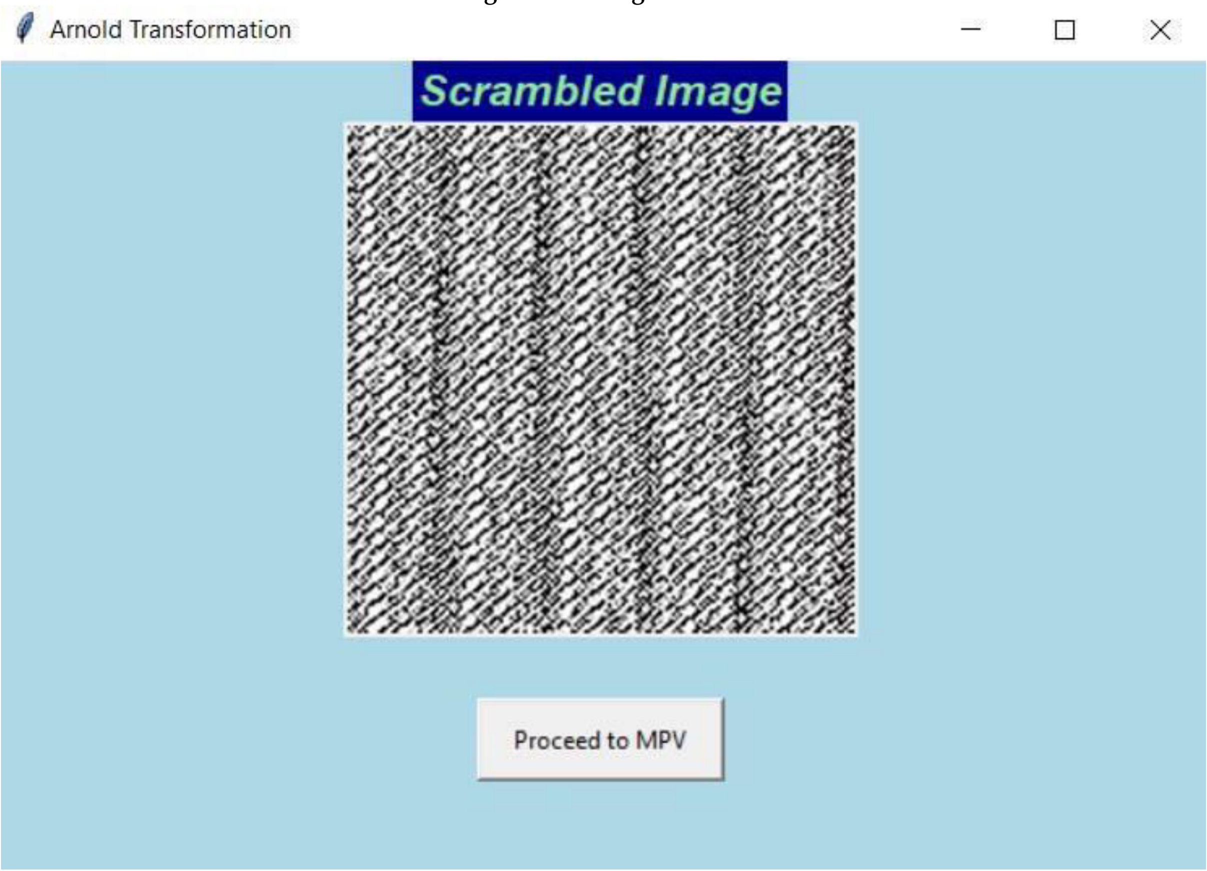


Fig 9 Scrambled image

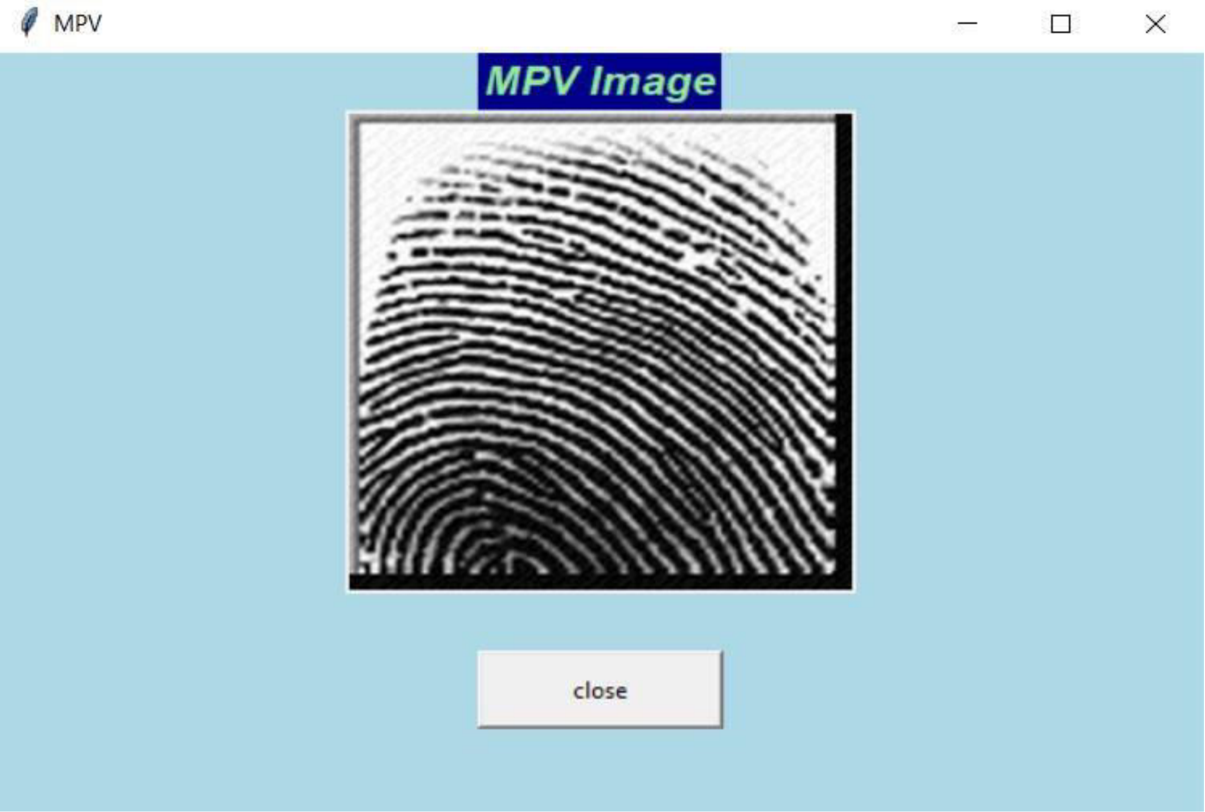
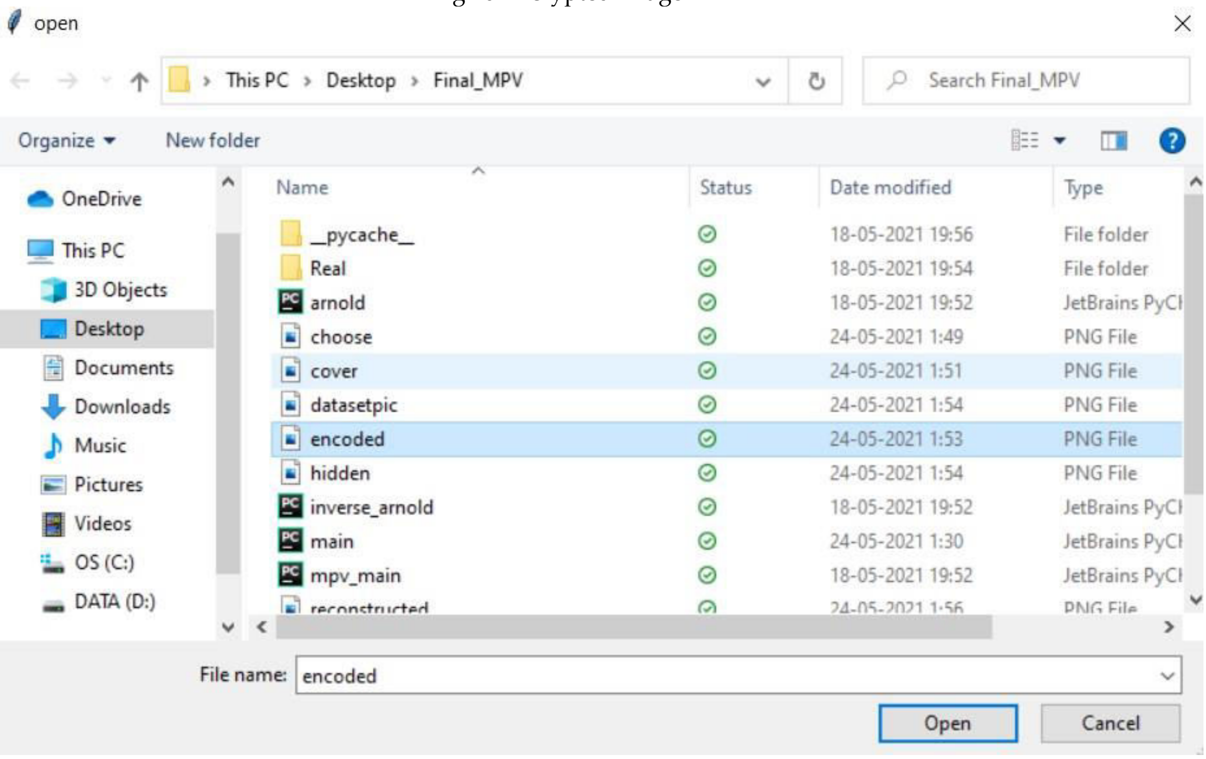


Fig 10 Encrypted image



Name	Status	Date modified	Type
__pycache__	✓	18-05-2021 19:56	File folder
Real	✓	18-05-2021 19:54	File folder
arnold	✓	18-05-2021 19:52	JetBrains PyCh
choose	✓	24-05-2021 1:49	PNG File
cover	✓	24-05-2021 1:51	PNG File
datasetpic	✓	24-05-2021 1:54	PNG File
encoded	✓	24-05-2021 1:53	PNG File
hidden	✓	24-05-2021 1:54	PNG File
inverse_arnold	✓	18-05-2021 19:52	JetBrains PyCh
main	✓	24-05-2021 1:30	JetBrains PyCh
mpv_main	✓	18-05-2021 19:52	JetBrains PyCh
reconstructed	✓	24-05-2021 1:56	PNG File

File name: encoded

Fig 11 Selecting the stego image

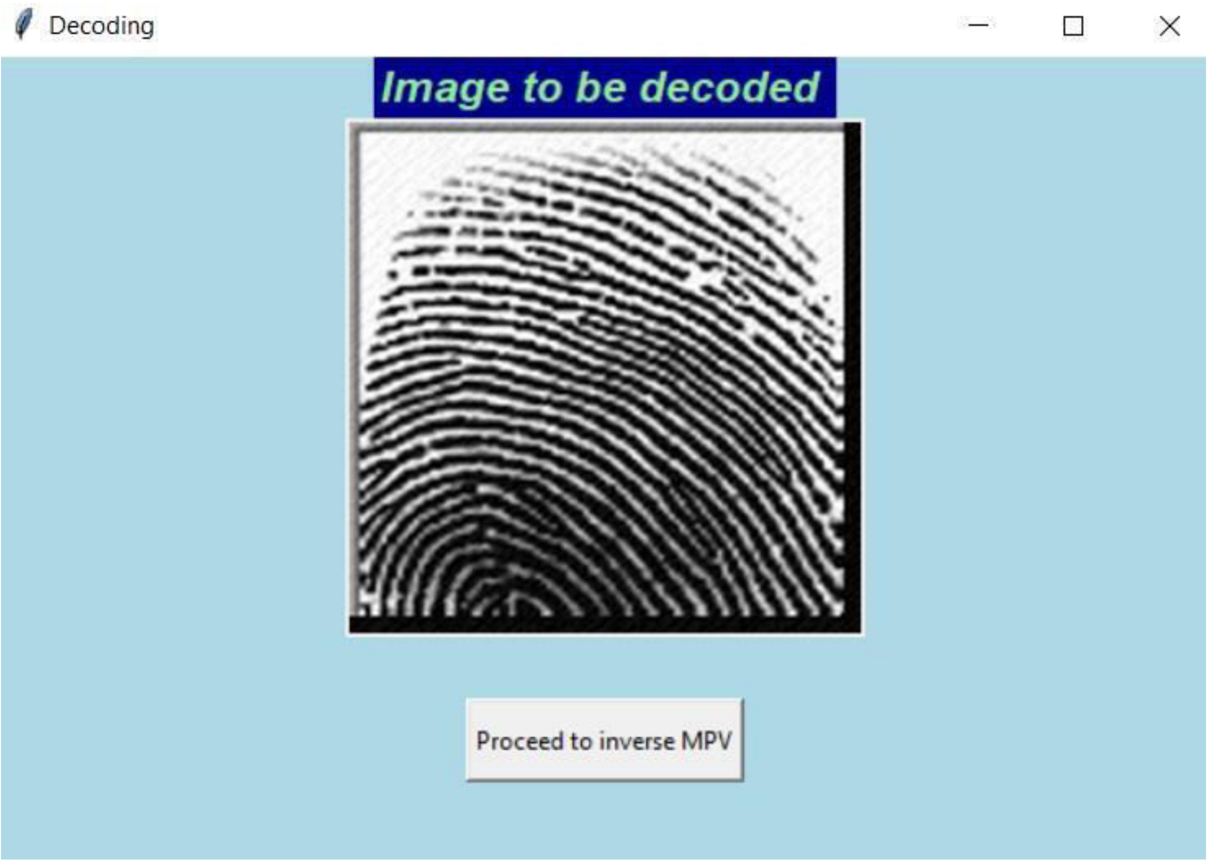


Fig 12 Stego Image

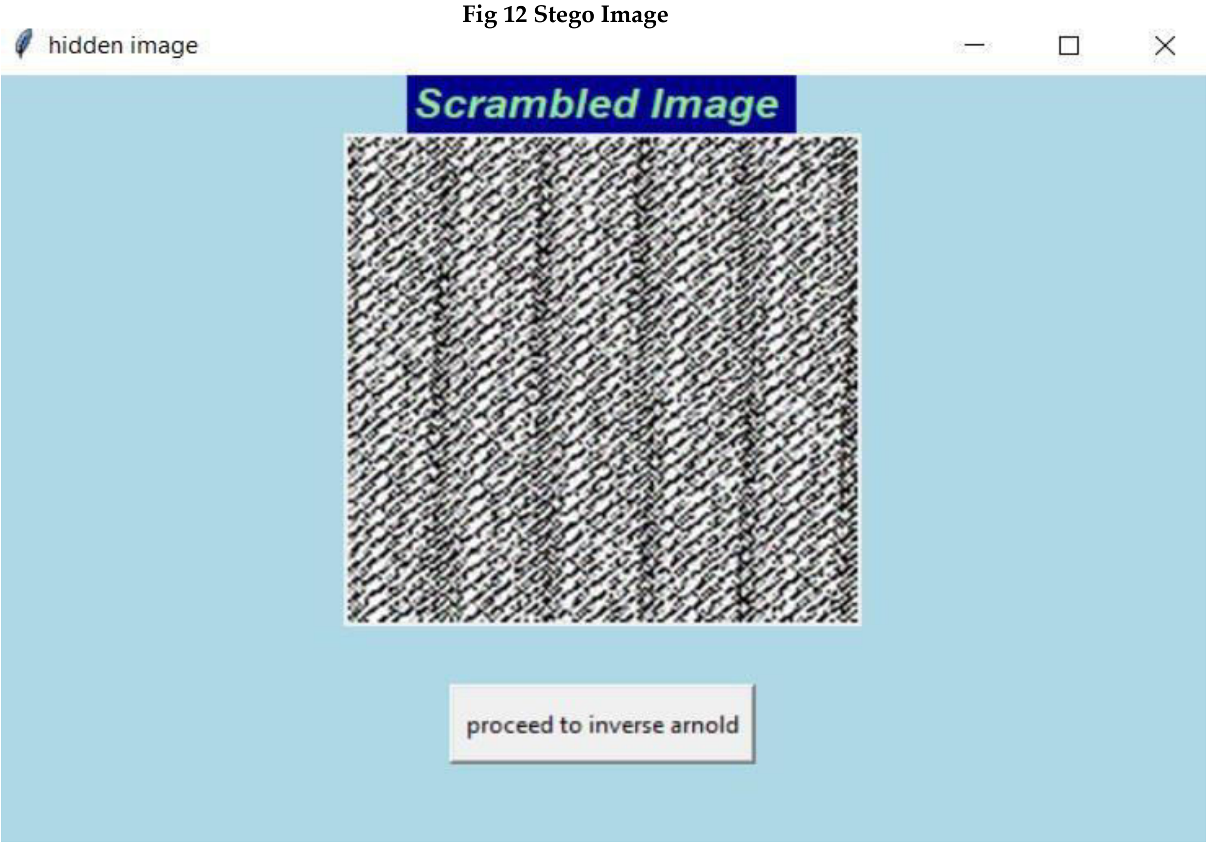


Fig 13 Applying Inverse Arnold

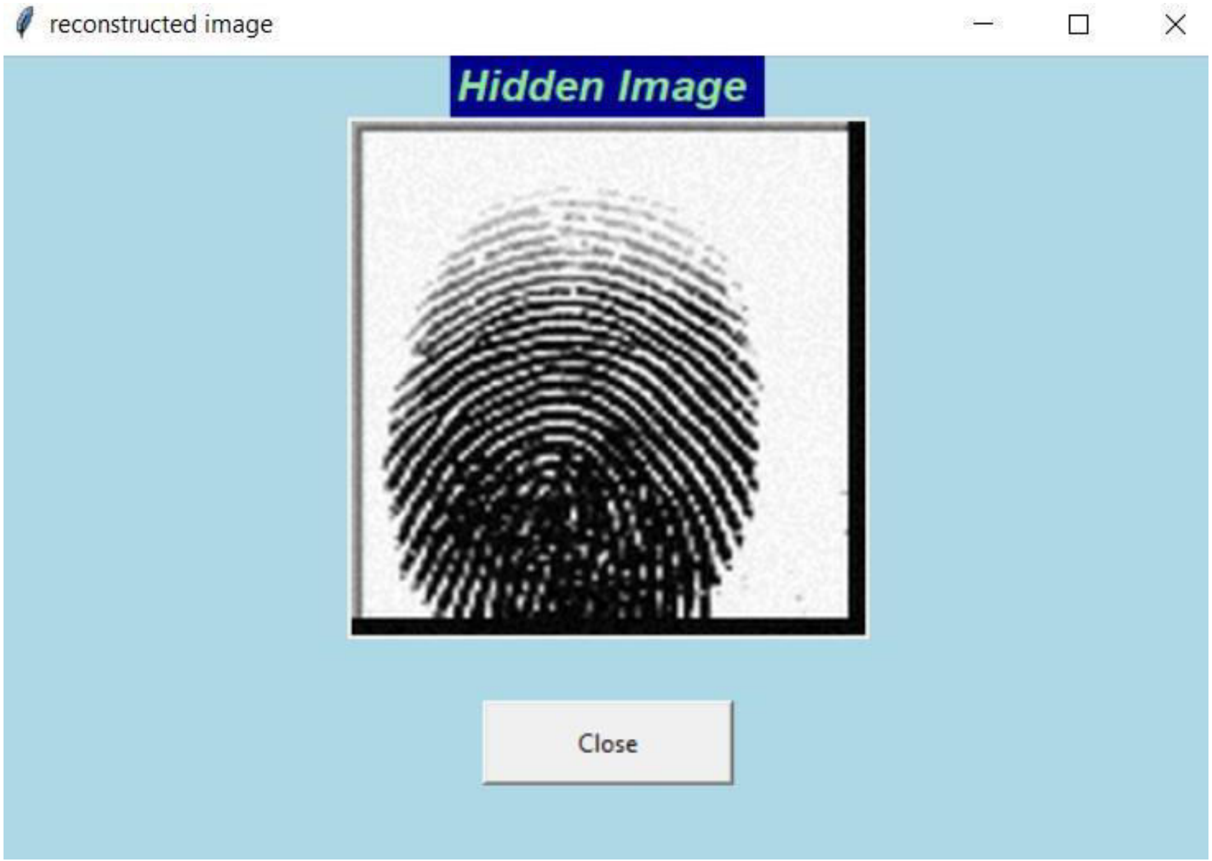


Fig 14 Decrypted Image

7. CONCLUSION AND SCOPE

Steganography is a technique which aids in security for several purposes during communication. In this paper, a steganographic approach is proposed for biometrics in image medium which masks the secret data bits that have to be transmitted without any third-party intervention. Application of Arnold Transform on the input image renders a level of security in the beginning of the process itself. The MPV technique follows a conditional strategy while embedding of secret data bits. The application of reverse mpv and inverse arnold transform does the decoding of the stego-image at the receiver end. The advantage of this method is that, the receiver does not need any extra key for decoding the secret image. The stego image itself gives a layer of security since it is also a biometric image. Thus, the overall security is endorsed. Hence, it doesn't attract the eye of unwanted sources.

This application provides a solution to those problems where there is security problem for biometrics. As we have seen a lot of issues regarding stealing or manipulating of biometrics this application makes the process easy and simple way for those who want to complete their communication securely. This also helps those who cannot remember their passwords etc., The future enhancement of this application is

- To increase the range from fingerprint to other biometrics.
- To implement with two level arnold.

7. REFERENCE

1. https://www.researchgate.net/publication/325657541_Image_Steganography_Using_Mid_Position_Value_Technique
2. https://www.academia.edu/10228724/FINGERPRINT_BASED_IMAGE_STEGANOGRAPHY_IN_TRANSFORM_DOMAIN
3. http://www.ijstr.org/final-print/dec2019/-Image-Steganography-Using-Lsb.pdf
4. https://www.researchgate.net/publication/333559334_Integration_of_Biometrics_and_Steganography_A_Comprehensive_Review
5. https://ijarcce.com/wp-content/uploads/2018/10/IJARCCE.2018.7910.pdf
6. https://www.hindawi.com/journals/jcnc/2018/9475142/