International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||06||Pages||5378-5385||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i6.04

Watermarking Using Bit Plane Complexity Segmentation and Artificial Neural Network

Rashmeet Kaur Chawla[1], Sunil Kumar Muttoo[2]

[1]Department of Computer Science,
University of Delhi
New Delhi
Rashmeet.mcs.du.2014@gmail.com
[2]Department of Computer Science,
University of Delhi
New Delhi
skmuttoo@cs.du.ac.in

Abstract: Digital Watermarking is the act of hiding a message related to an image within the image itself. Watermarking has many desirable properties like effectiveness, image fidelity and robustness.

Multilayer artificial neural network is used to achieve image compression. The input pixels are used as target values and the hidden layer output is the compressed image.

Our proposed technique uses an image as the vessel data and embeds secret information in the noise-like region of the bit-planes and watermark in the informative region of the bit-planes of the vessel image without deteriorating image quality. The secret image is first compressed by artificial neural network and then embedded in the vessel image. This technique makes use of the characteristics of the human vision system where a human eye cannot perceive any change in the information in a very complicated binary pattern.

Keywords:- Watermarking, Multilayer neural network, image compression, Vessel image.

1. INTRODUCTION

A digital watermark is visible information in the form of a text or image that has been added to the original image. Watermarking is the process that embeds data called watermark into a multimedia object. Some of its important applications include digital copyrights management and protection. [2]

Image compression has been an active area of research since the inception of digital image processing. Compression is achieved by exploiting the redundancy in an image. Artificial Neural Network have found increasing applications in this field due to their noise suppression and learning capabilities. [1]

In this paper we have proposed a technique for watermarking using bit plane complexity segmentation and artificial neural network.
Some of the concepts used are as follows:-

1.1 Back Propagation Neural Network

An Artificial Neural Network (ANN) is a computational model based on the structure and functions of biological neural networks. Back Propagation Neural Network is designed and trained using different learning algorithms. [4]

The neural network structure shown in Figure1 has three layers: one input layer, one output layer and one hidden layer. Both of input layer and output layer are fully connected to hidden layer. [3]

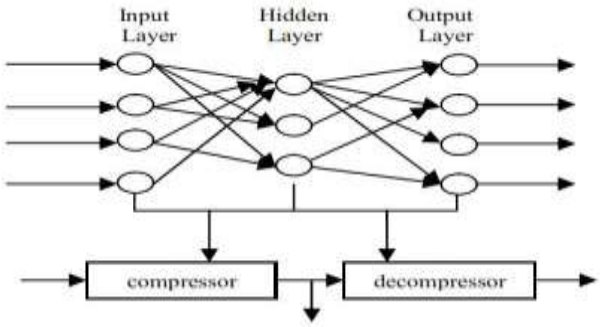


Figure 1

The connection weights in the network are gradually adjusted, working backwards from the output layer, to the input layer through the hidden layer, until correct output is produced. The general parameters deciding the performance of back propagation neural network algorithm includes mode of learning, target values, goal, epochs, learning rate and momentum factors. [3]

Compression is achieved by designing the value of the number of neurons at the hidden layer, less than that of neurons at both input and output layers. [3]

1.1.1 Network Training Algorithms

Training the network is an important step to get the optimal values of weights and biases after being initialized randomly

or with certain values. For training the network, the 128x128 pixels image has been employed. During training, the weights and biases of the network are iteratively adjusted to minimize the network performance function which is the mean square error for the feed forward networks. [1]

Training could be started by making target matrix equal to input matrix. Different training algorithms can be used, mainly classified as fast algorithms(example trainbfg, trainoss, trainlm, etc.) and slow algorithms (example traingd, traingda, etc.)

1.1.2 Simulation of Results

After training, we obtain a simulated network by the input matrix and the target matrix. In the simulation process two outputs are obtained, the hidden layer output and the output layer output. The hidden layer produces a matrix of 16x256, whereas the output layer produces a matrix of 64x256. [3]

Hidden layer output is the compressed image and the output layer matrix is the reconstructed image. In the hidden layer matrix, each column should be reshaped into 4x4 pixel blocks, while in the output layer matrix, each column should be reshaped into 8x8 pixel blocks to display both matrices as images. [1]

1.2 Watermarking

A watermark is data which consists of an identifying image or pattern. The watermark may not contain a relation to the multimedia object in which it is embedded. Watermarking is the process water mark in a cover.

Digital watermarks are used to verify the authenticity or integrity of the object or to show the identity of its owners. They are said to be robust if it resists a designated class of transformations. [5]. Watermarking is done in spatial domain and transform domain. Discrete Cosine Transform (DCT) is one of the transforms used for watermarking.

We have used DCT in our proposed technique.

1.2.1 HASHING

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values or hash codes.

The input (message, file etc.) is viewed as a sequence of n-bit blocks. The input is processed one block at a time in an iterative fashion to produce a 1-block hash function. [6]

1.2.2 ENCRYPTION

It is a process of scrambling the data to prevent third party from understanding the content. It also protects the content of the message in such a way that only authorized parties can read it. We have used **RSA (Rivest-Shamir-Adleman)** algorithm in our proposed technique.

1.3 Bit Plane Complexity Segmentation Technique:

The following are the steps used in the proposed technique:

- Canonical Grey Code

In BPC the substantial portions of the regions on the higher bit planes are relatively flat in color (mostly all 0s or all 1s). This is because of the "Hamming Cliffs" which occur with PBC wherein a small change in color affects many bits of the color value.

In binary:
127 = 01111111 & 128 = 10000000
In gray code:
127 = 01000000 & 128 = 11000000

In gray code the representation of adjacent gray levels will differ only in one bit (unlike binary format where all the bits can change). CGC images do not suffer from such Hamming Cliffs.

- ***Complexity of an image***

The complexity of an image (α) is defined by the following:-

α =k/The maximum possible B-W changes in the image,
where, k is the total length of black-and-white border in the image.
So, value of α ranges over $0 \leq \alpha \leq 1$.

- ***Conjugation of a binary image:-***

It is applied when the complexity of the vessel image block is less than the threshold and cannot be used for embedding the secret data.
$P^* = P \text{ XOR } W_c$,
where P* is a conjugated 8x8 block of vessel image, P is an informative (i.e. less complex) 8X8 block of vessel image,
W_c is a complex binary pattern.

After conjugation, complexity of the block of vessel image increases and thus can be used for embedding secret data.

$$A(P^*) = 1 - \alpha(P). \quad [6]$$

2. PROPOSED TECHNIQUE:-

Watermarking technique prevents unauthorised embedding as it solves the problem of authenticating the sender by either encrypting the message using asymmetric key cryptography or appending a cryptographic signature. Even if the adversary knows the embedding algorithm and watermark, the message cannot be encrypted correctly or a valid signature be created unless they know the encryption key.

With this proposed technique, we can also hide a larger size secret image into vessel image after compressing it using artificial neural network. This is extremely important for efficient storage and transmission of image data.

DOI: 10.18535/ijsrm/v5i6.04

In [5] the watermarking technique, in [1] the Image compression technique and in [6] the BPCS technique is described. The proposed technique is described in algorithm 1, 2 and 3.

Algorithm 1 for obtaining the cryptographic signature using the watermark:-

1. Construct a description of cover work based on lowest frequency components of vessel image. (Using dct)

2. Compute a **one way hash** of the watermark message concatenated with the description of cover work.

3. Encrypt the hash with a private key using **RSA algorithm**, thus obtaining a cryptographic signature.

4. Embed the watermark message along with the signature using Bit Plane Complexity Segmentation (BPCS) technique in the informative regions of the vessel image.

Algorithm 2 for the Image Compression:-

1. Take a 128x128 grey scale secret image. Divide it into 8x8 pixel blocks and reshape each one into 64x1 column vector.

2. Arrange the column vectors into a matrix of 64x256, which will be used as input matrix.

3. Let the target matrix equal to the input matrix obtained in step 2.

4. Choose a suitable learning algorithm such as traincgf and parameters like goal – 0.001 to start training the neural network using neural network toolbox of matlab.

5. Train and simulate the network with the given input matrix and the target matrix.

6. Obtain the output matrices of the hidden layer and the output layer.

7. Post-process them to obtain the compressed image and the reconstructed image respectively.

Algorithm 3 for the BPCS technique :-

1. Transform the vessel image from PBC to CGC system.

2. Divide our vessel image into a series of bit planes (1-8).

3. Segment each bit-plane of the vessel image into informative and noise-like regions by using a threshold value ($\alpha 0=0.3$).

4. Divide the watermark into a series of 8 X 8 blocks.

5. Embed watermark along with the signature into the informative regions of the bit-planes.

6. Divide the secret file into a series of 8 X 8 secret blocks.

7. If a block (P) is less complex than the threshold ($\alpha 0$), then conjugate it to make it a more complex block (P*). (Provided it is not used for embedding the watermark or the signature)

8. If the block is conjugated, then record this fact in a "conjugation map". Embed the conjugation map in the noise block with the highest entropy.

9. Embed each secret block into the noise-like regions of the bit-planes (or replace all the noise-like regions with a series of secret blocks).

10. Generate a new stego image using modified bit planes.

11. Convert the stego image from CGC back to PBC.

3. EXPERIMENTAL RESULTS:-

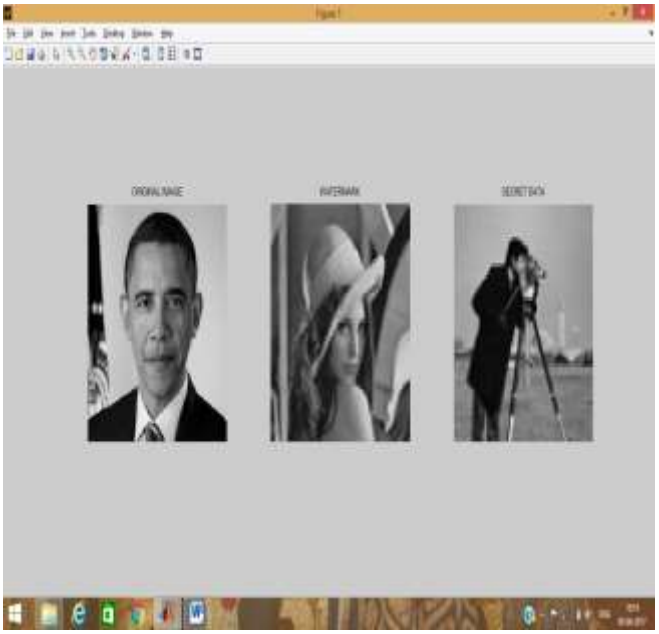


Fig 1.1- a), b), c) represent original vessel image, watermark image, secret data respectively.

DOI: 10.18535/ijsrm/v5i6.04

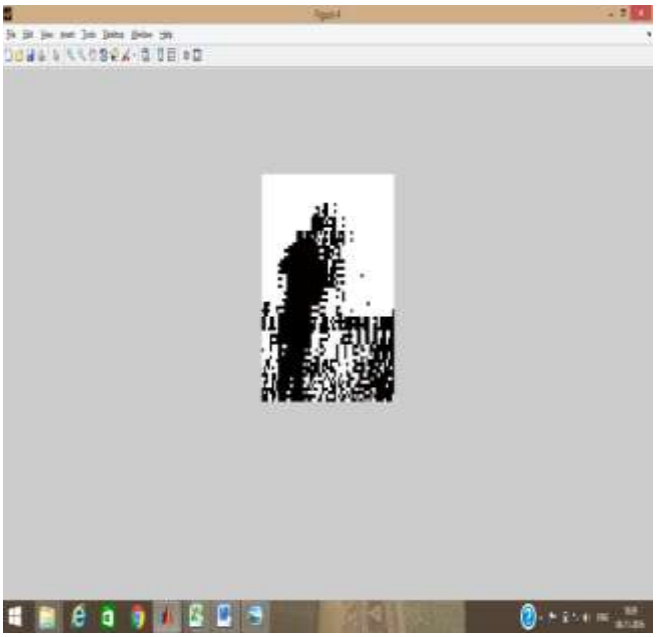


Fig 1.2 shows the compressed secret image.

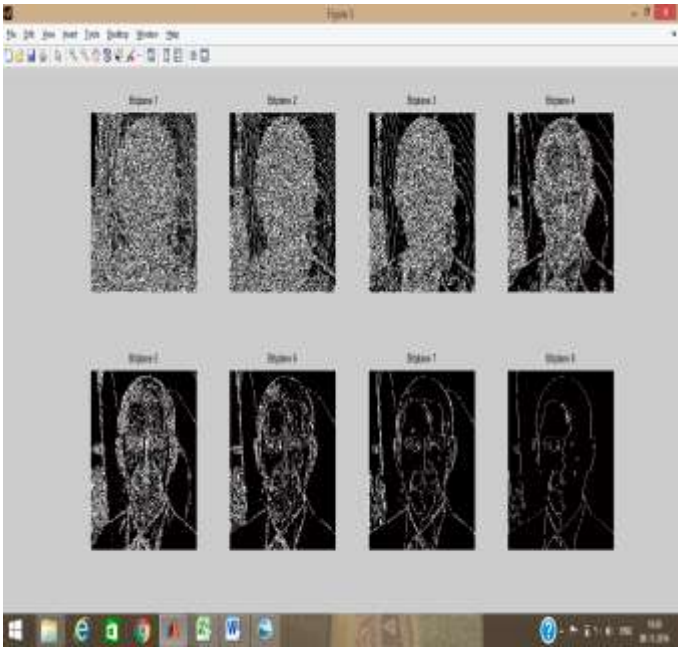


Fig 1.3 shows the bit plane slicing of the vessel image.

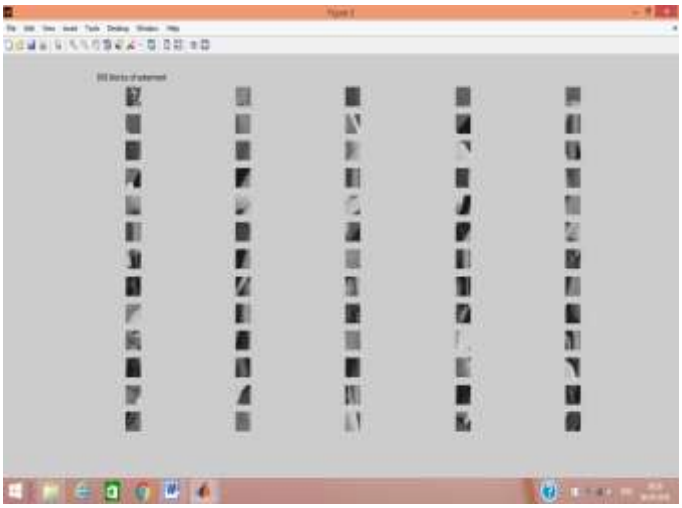


Fig 1.4 shows how a 64 x 64 watermark image is divided into 64(8 x 8) blocks.

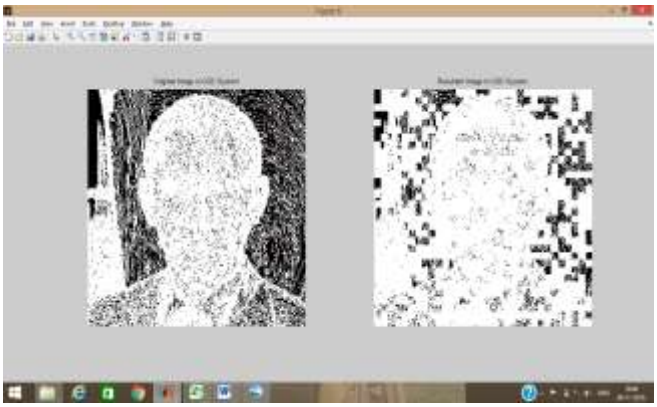


Fig 1.5 a), b) shows the original vessel image and vessel image obtained after embedding watermark and compressed secret file in CGC system.

Fig 1.6 a), b) shows the Original vessel image and vessel image which is obtained after embedding the watermark and the secret file.

DOI: 10.18535/ijsrm/v5i6.04

4. ANALYSIS

The following table shows PSNR values between original vessel images and vessel images obtained after embedding watermark and the secret file in different formats.

These PSNR values indicate that the robustness of the technique is preserved.

PSNR values between the original vessel image and stego image

Test 1.gif

Test 2.bmp

Test 3.bmp

Test 4.jpg

S. No.	Vessel image used	Watermark image used	Secret image used	PSNR Value
1	Test 1.gif	W1.jpg	Secret 1.bmp	51.28
2	Test 2.bmp	W1.jpg	Secret 1.bmp	51.30
3	Test 3.bmp	W1.jpg	Secret 1.bmp	51.19
4	Test 4.jpg	W1.jpg	Secret 1.bmp	51.23
5	Test 5.png	W1.jpg	Secret 1.bmp	51.22
6	Test 6.gif	W1.jpg	Secret 1.bmp	51.30
7	Test 7.jpg	W1.jpg	Secret 1.bmp	51.23
8	Test 8.png	W1.jpg	Secret 1.bmp	51.27
9	Test 9.gif	W1.jpg	Secret 1.bmp	51.27
10	Test 10.jpg	W1.jpg	Secret 1.bmp	51.26
11	Test 1.gif	W2.png	Secret 2.jpg	51.25
12	Test 2.bmp	W2.png	Secret 2.jpg	51.31
13	Test 3.bmp	W2.png	Secret 2.jpg	51.21
14	Test 4.jpg	W2.png	Secret 2.jpg	51.25
15	Test 5.png	W2.png	Secret 2.jpg	51.22
16	Test 6.gif	W2.png	Secret 2.jpg	51.28
17	Test 7.jpg	W2.png	Secret 2.jpg	51.27
18	Test 8.png	W2.png	Secret 2.jpg	51.28
19	Test 9.gif	W2.png	Secret 2.jpg	51.27
20	Test 10.jpg	W2.png	Secret 2.jpg	51.25
21	Test 1.gif	W3.bmp	Secret 3.png	51.29
22	Test 2.bmp	W3.bmp	Secret 3.png	51.31
23	Test 3.bmp	W3.bmp	Secret 3.png	51.18
24	Test 4.jpg	W3.bmp	Secret 3.png	51.24
25	Test 5.png	W3.bmp	Secret 3.png	51.20
26	Test 6.gif	W3.bmp	Secret 3.png	51.29
27	Test 7.jpg	W3.bmp	Secret 3.png	51.26
28	Test 8.png	W3.bmp	Secret 3.png	51.29
29	Test 9.gif	W3.bmp	Secret 3.png	51.28
30	Test 10.jpg	W3.bmp	Secret 3.png	51.26

DOI: 10.18535/ijsrm/v5i6.04

Test 5.jpg

Test 6.gif

Test 7.jpg

Test 8.jpg

Test 9.gif

Test 10.jpg

Secret 1.bmp

Secret 2.jpg

Secret 3.png

W1.jpg

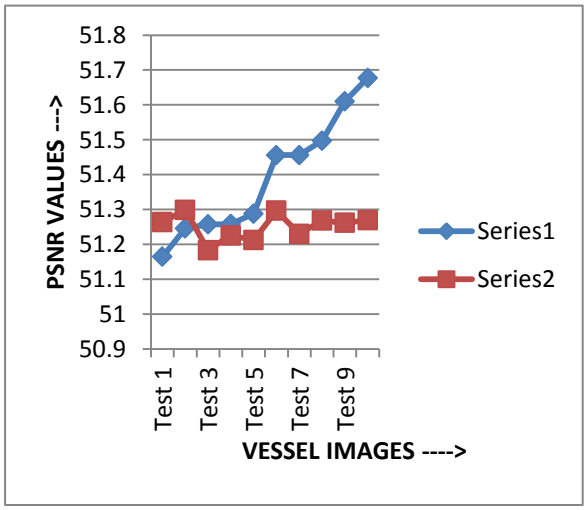
DOI: 10.18535/ijsrm/v5i6.04

W2.png

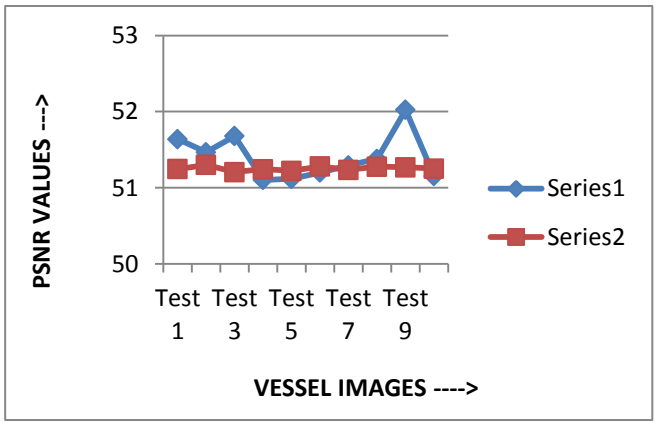
W3.bmp

5. COMPARISON WITH THE EXISTING WORK:-

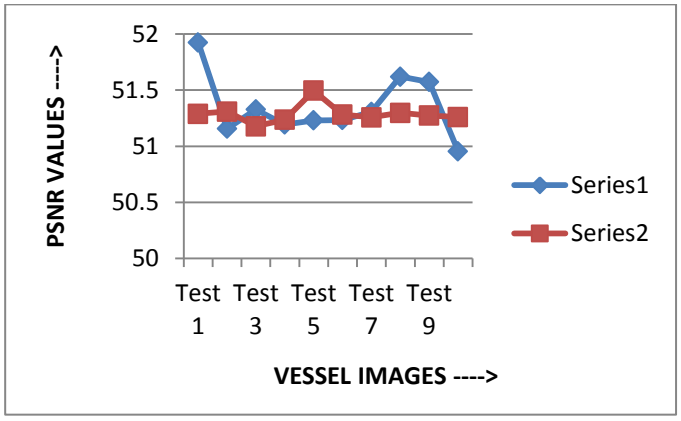
- The following graph indicates the comparison of psnr values of the ten test images (Secret1.bmp, W1.jpg used) between the original work and the proposed work.



- The following graph indicates the comparison of psnr values of the ten test images (Secret2.bmp, W2.jpg used) between the original work and the proposed work.



- The following graph indicates the comparison of psnr values of the ten test images (Secret3.bmp, W3.jpg used) between the original work and the proposed work.



6. APPLICATIONS

1. TRACKING OF TRANSACTION

   Watermarks record the recipient in each legal sale or distribution of the work. If the work is misused (leaked to the press or illegally distributed), the owner could find out about who is the traitor. Visible watermarking is often adopted in this application but invisible watermark is even better.

2. COPY CONTROL
   It combines every content recorder with a watermark detector. When a copy-prohibit watermark is detected, the recording device will refuse to copy.
3. LOCATING CONTENT ONLINE

   Notifying the owner of where their content was found, allowing them to take any actions deemed necessary. It helps companies monitor that the right content is being used on the right sites at the right time, quickly identify unauthorized usage of content to enable a range of remedies, gather useful market intelligence about what consumers are accessing and where, measure the effectiveness of

marketing programs and campaigns, ensure more effective brand management online.

7. CONCLUSION

- The most important point in this technique is that human eye cannot perceive any change in the information in the bit-planes of an image, thus protecting the copyright of image.
- By using artificial neural network for image compression, we are able to use a larger size secret image for hiding in the vessel image.

Thus combining watermarking with BPCS steganography increases the level of secret and secure communication.

8. REFERENCES

[1] https://www.researchgate.net/publication/229026489_Image_Compression_Using_Neural_Network

[2] https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf

[3] Daneshwari i. Hatti, Savitri Raju and Mahendra m. Dixit, D*esign of neural network as data flow model for image compression*, International Journal of Image Processing and Vision Sciences (IJIPVS) ISSN(Print): 2278 – 1110, Vol-1 Iss-3,4 ,2012.

[4] www.techopedia.com/definition/5967/artificial-neural-network-ann

[5] Ingemar Cox, Matthew Miller, Jeffrey Bloom and Mathew Miller, *Digital Watermarking*, Morgan Kaufmann, 2002.

[6] Eiji Kawaguchi and Richard O. Eason, *Principle and applications of BPCS-Steganography*,1999, SPIE 3528, Multimedia Systems and Applications, 464, Conference Volume 3528.

Author Profile

Ms. Rashmeet Kaur Chawla, received the B.Sc(Hons) Computer Science and M.Sc. Computer Science degrees from University of Delhi in 2014 and 2016 respectively. Her field of specialization is Information Security.

Dr. Sunil Kumar Muttoo, Professor, University of Delhi. He has a teaching experience of 36 years. He guides research students on the topics: information security and cryptography. He has many papers published in various national and international journals.