ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

ADVANCED LOSSLESS DATA HIDING METHOD FOR SECURELY ENCRYPTED IMAGES

Mr. Dileep Kumar[1], Akshat Dwivedi[2], Shubham Chaturvedi[3], Mukul[4] and Rishabh Prajapati[5]

[1]Assistant Professor MCA, Dr. Ram Manohar Lohia Avadh University Ayodhya U.P

[2]Research Scholar MCA, Computer Application Department, Dr. Ram Manohar Lohia Avadh University Ayodhya U.P

[3]Research Scholar MCA, Computer Application Department, Dr. Ram Manohar Lohia Avadh University Ayodhya U.P

[4]Research Scholar MCA, Computer Application Department, Dr. Ram Manohar Lohia Avadh University Ayodhya U.P

[5]Research Scholar MCA, Computer Application Department, Dr. Ram Manohar Lohia Avadh University Ayodhya U.P

[1]dileep_k_2000@yahoo.com, [2]akshatdwivedi59941@gmail.com, [3]shubhamchat224122@gmail.com, [4]mukul.kumar630@gmail.com and [5]iet.rishu@gmail.com

ABSTRACT

The concept explores an innovative methodology for embedding data within encrypted images using an irreversible data hiding approach, which aims to clandestinely integrate messages into data sets. In the realm of internet communication, challenges like data security, copyright control, data size capacity, and authentication have become prominent. A novel solution proposed here is the application of reversible data hiding algorithms on encrypted images, designed to extract embedded data before image decryption. This dissertation endeavors to forge a robust and secure data hiding technology that addresses these pressing concerns. The process revolves around the use of two distinct keys: an encryption key for image security and a data hiding key for extracting the embedded information. This dual-key system ensures that only authorized recipients possessing the data hiding key can successfully retrieve the hidden data from the encrypted images. By combining data hiding and image encryption with separate keys, this methodology aims to enhance data security and privacy in digital communication channels.

Index Terms - Image encryption, image decryption, image recovery, reversible data hiding.

INTRODUCTION

In today's interconnected digital world, where information flows freely across vast networks, security is paramount. The integrity and confidentiality of data are critical concerns, making robust security measures a necessity. The realm of internet communication, with its complex web of interactions, relies heavily on security protocols to safeguard sensitive information from unauthorized access, tampering, and interception. As technology evolves and cyber threats become increasingly sophisticated, the need for advanced security mechanisms grows more urgent.

At the core of digital security lie various branches, each addressing different facets of protection. Cryptography, perhaps one of the oldest and most fundamental pillars of security, deals with encoding and decoding information to ensure confidentiality. By employing cryptographic algorithms, data is transformed into an unreadable format, which can only be deciphered by authorized parties possessing the decryption key. This process of encryption and decryption forms the basis of secure communication channels, preventing malicious actors from deciphering sensitive data.

In parallel, information hiding techniques such as steganography and watermarking play crucial roles in enhancing data security. Steganography, the art of concealing information within seemingly innocuous data, adds an extra layer of obscurity to communication channels. By embedding messages or data within images, audio files, or other digital media, steganography enables covert communication while maintaining the appearance of

normalcy. This technique is particularly useful in scenarios where discreet communication is necessary, such as military operations or confidential corporate exchanges.

Watermarking, on the other hand, focuses on embedding imperceptible identifiers or marks into digital assets. These watermarks serve as digital fingerprints, allowing content creators to assert ownership and protect their intellectual property. In the context of data security, watermarking aids in verifying the authenticity and integrity of digital content, deterring unauthorized duplication or alteration.

As the digital landscape evolves, so do the challenges and complexities associated with ensuring data security. Intruders and hackers constantly probe for vulnerabilities in security protocols, seeking ways to exploit weaknesses for their gain. Therefore, the development of resilient and unbreakable algorithms becomes imperative. Modern cryptographic techniques leverage both symmetric and asymmetric encryption methods, offering a spectrum of security options tailored to different needs.

Symmetric encryption, where the same key is used for both encryption and decryption, provides fast and efficient data protection suitable for many applications. However, managing and distributing keys securely can be challenging in large-scale systems. Asymmetric encryption, also known as public-key encryption, addresses this challenge by employing a pair of keys—a public key for encryption and a private key for decryption. This approach facilitates secure communication between parties without the need to exchange secret keys beforehand.

In tandem with encryption techniques, reversible data hiding (RDH) emerges as a powerful tool for secure information embedding. RDH emphasizes the concealment of data within cover data while maintaining the ability to recover the original information without loss. This reversible nature of data hiding ensures data integrity and authenticity, making it a valuable asset in scenarios where data concealment and retrieval are crucial.

The applications of reversible data hiding span various domains, from military and intelligence communications to healthcare and emergency response systems. In military operations, secure communication channels are vital for transmitting sensitive information without compromising operational security. Reversible data hiding techniques can be employed to embed critical data within multimedia files, providing a covert yet reliable method of communication.

Similarly, in the healthcare sector, where patient privacy and data integrity are paramount, reversible data hiding techniques offer a means of securely storing and transmitting medical records and diagnostic images. By embedding patient information within medical images, healthcare providers can ensure confidentiality while maintaining data accessibility.

In emergency response scenarios, such as natural disasters or public safety incidents, quick and secure communication channels are essential for coordinating rescue efforts and disseminating critical information. Reversible data hiding enables emergency responders to embed location data, instructions, and situational updates within multimedia files, ensuring that vital information reaches the right recipients swiftly and securely.

Overall, the integration of cryptography, information hiding, and reversible data hiding techniques forms a comprehensive security framework that addresses the diverse challenges of data security in modern communication systems. By leveraging these advanced technologies, organizations and individuals can fortify their digital defenses, mitigate risks, and uphold the integrity and confidentiality of their data in an increasingly interconnected world.

METHODOLOGY OF IMAGE ENCRYPTION AND DECRYPTION

Hashing Encryption:

Hashing is the first encryption method, creates a unique, fixed-length signature for a message or data set. It created with hash function, and people commonly use them to compare sets of data. Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash, there by alerting a user to potential tampering.

Symmetric Encryption:
Symmetric cryptography, also called private-key cryptography, is one of the oldest and most secure encryption methods. The term "private key" comes from the fact that the key used to encrypt and decrypt data must remain secure because anyone with access to it can read the coded messages. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode.

Asymmetric Encryption:
Asymmetric or public key cryptography is potentially more secure than symmetric method of encryption. This type of cryptography uses two keys, a "private" key and a "public key" to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users.

In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, wheo uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Differ-Hellman.

AES Encryption:
The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6]

Block-Based Transformation:
The transformation technique works as follows: the original image is divided into a random number of blocks that are then shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

METHODOLOGY DATA EMBEDDING

DWT watermarking:
Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dimensional image after three-times DWT decomposed can be shown as Fig.1.2. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1, HH1. The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation.

DCT watermarking
DCT watermarking is a process of embedding information. Information embedded is imperceptible, secure and robust.

Step 1: Divides image into parts based on the visual quality of the image.

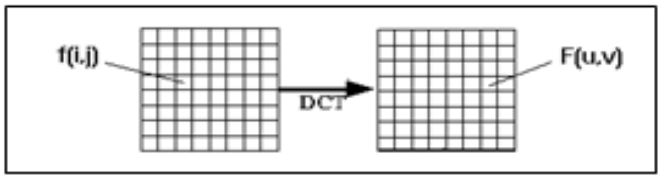

Figure 1 Dct Compression Method

Step 2: Input image is N*M.

Step 3: F (i,j) = intensity of pixel in row i and column j.

Step 4: F (u,v) is DCT coefficient in DCT matrix.

Step 5: Larger amplitudes closer to F (0,0).

Step 6: Compression possible because higher order coefficients are generally negligible.

LSB compression method

LSB is the most basic method and used in common for creating the sparse space. The sparse space created is useful for hiding the additional payload data. This makes te works easier. In this some parameter are added into small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating additional data.

LITERATURE STUDY

The literature review encompasses a range of innovative approaches and methodologies in the field of reversible data hiding in encrypted images, showcasing advancements in encryption techniques, data hiding algorithms, and compatibility with various processing methods.

Panchikkil et al. [1] propose a random-key based second-level encryption for reversible data hiding, emphasizing the importance of robust encryption mechanisms for secure data embedding within encrypted images. Kiran et al. [2] introduce the Secure Reversible Image Data Hiding (SRIDH) method using LSB prediction, showcasing the integration of prediction techniques for enhanced data hiding security.

Wu et al. [3] present a lossless data hiding method compatible with homomorphic processing, highlighting the potential for seamless integration with homomorphic encryption schemes. Hao et al. [4] propose a reversible data hiding scheme based on image partitioning and histogram shifting, showcasing the effectiveness of partitioning techniques in optimizing data hiding capacity.

Xiao et al. [5] introduce a general distortion-based reversible data hiding approach for binary covers, showcasing versatility in handling different cover types. Agarwal and Kumar [6] present an IWT-based reversible data hiding scheme in the encrypted domain, emphasizing the utilization of wavelet transforms for efficient data hiding.

Ma et al. [7] introduce a fast expansion-bins-determination approach for multiple histograms modification-based reversible data hiding, showcasing advancements in histogram modification techniques. Asif et al. [8] explore high-capacity reversible data hiding using deep learning, highlighting the potential of deep learning models in optimizing data hiding capacity.

Zheng et al. [9] propose a lossless data hiding method based on a homomorphic cryptosystem, showcasing compatibility with secure cryptographic schemes. Wang et al. [10] present a high-capacity reversible data hiding method based on intra-block lossless compression, highlighting the benefits of compression techniques in maximizing data hiding capacity.

Zhao et al. [11] introduce a reversible data hiding approach based on histogram shifting with sorted pairs of points, showcasing innovative methods for optimizing data hiding efficiency. Murthy and Manikandan [12] propose a block-wise histogram shifting-based reversible data hiding scheme with overflow handling, addressing challenges related to data overflow in data hiding processes.

Srihitha et al. [13] present an adaptive multi-level block-wise encryption-based reversible data hiding scheme, showcasing adaptability to different encryption levels for enhanced security. Sulistyawan et al. [14] introduce an adaptive BWT-HMM-based lossless compression system for genomic data, highlighting applications in data compression and storage.

Li et al. [15] present a reversible data hiding algorithm based on prediction error with large amounts of data hiding in the spatial domain, emphasizing the potential for efficient data hiding with minimal distortion. These studies collectively contribute to the advancement of reversible data hiding techniques, offering diverse approaches to address challenges and optimize data hiding performance in encrypted images.

PROPOSED ALGORITHM

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data.

At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Here a comprehensive combination of image encryption and data hiding compatible with lossy Compression method will be used.

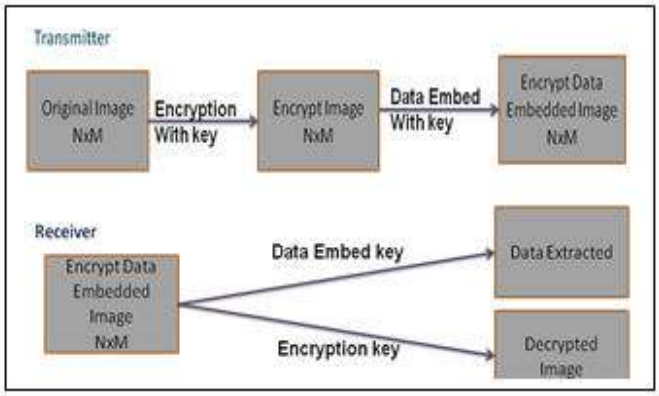

Figure 2: Encryption and Decryption Algorithem

Image Encryption Algorithm

Step 1:

Find image size Colum and Row

Step 2:

Generate Key and mask

Keygen= Colum*Row*8

KeygenMask=Colum*Row*8

Step 3:

Putting value in mask

```
rvalue =0.300001;
x_N = 0;
for ind = 2 : n
x_N = 1 - 2* rvalue * rvalue;   % value generation for keymask < 0
if (x_N > 0.0)
bin_x(ind-1) = 1;
end
rvalue =  x_N;
end
```

Step 4:

Divide by 8 the mask to same size of image

KeygenMask=KeygenMask/8

Step 5:

Now apply bitxor operation between original image and KegenMask

Encrypted image = bitxor(original image,KeygenMask);

Image Decryption Algorithm

Step 1:

Find Encrypted Image size Colum and Row

Step 2:

If KeyGen=Colum*Row

Further Decryption Process

Else

Decryption is not done

Step 3:

Generated KeygenMask at step 2 and 3 will be use here

Step 4:

Now apply bitxor operation between Encrypted image and KegenMask

Decrypted image = bitxor(Encrypted image,KeygenMask);

RESULTS ANALYSIS

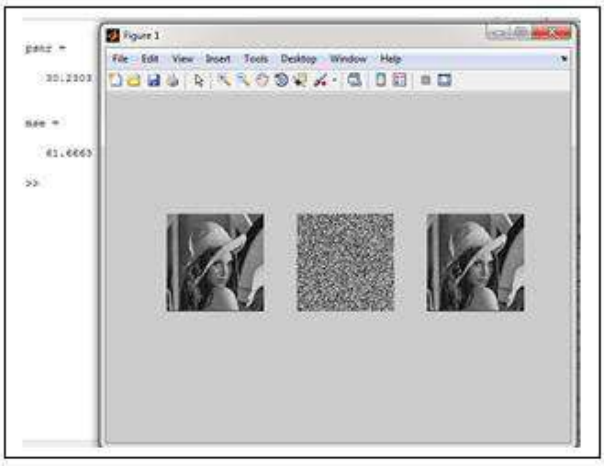

Figure 3 Aes Encryption and Decryption

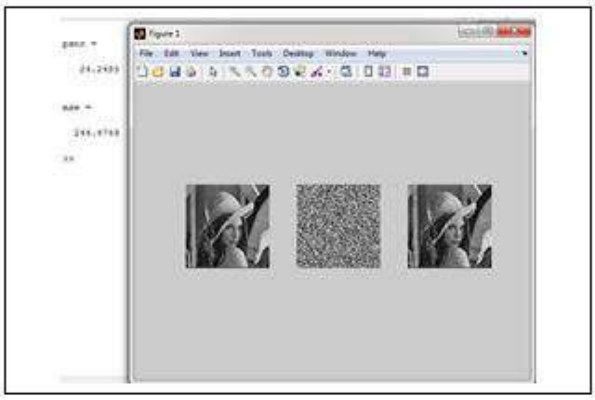

Figure 4 Block Encryption and Decryption

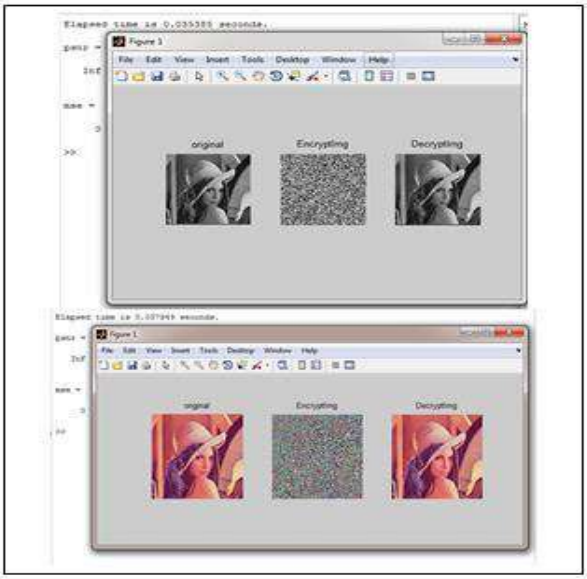

Figure 5 Proposed Encryption and Decryption

Table I Analysis

Image Encryption Methods	PSNR	MSE
AES Based Algorithm	30.2303	61.663
Block-Based Transformation	24.2485	244.4749
Proposed Method	Inf	0

CONCLUSION

The proposed approach encompasses a comprehensive process of hiding data within encrypted images, spanning image encryption, data embedding, and data extraction or image recovery phases. Initially, the content owner encrypts the original uncompressed image using an encryption key, followed by utilizing a data hiding key to create a sparse space within the encrypted image to accommodate additional data. This strategic approach ensures that the embedded data remains securely hidden within the encrypted image until the receiver possesses both the encryption and data hiding keys, facilitating accurate data extraction and seamless recovery of the original content without any loss or error.

Moving forward, the integration of data hiding and extraction algorithms into our system heralds a significant advancement in secure communication methodologies. This novel technique addresses a critical challenge faced by users of digital images, particularly in sectors with stringent security requirements such as military, legal, and medical applications, where secure message transmission is of paramount importance. By leveraging advanced image encryption methods, including the AES-based algorithm and block-based transformation, alongside our proposed method, we observe notable improvements in performance metrics such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE). Specifically, the proposed method showcases unparalleled performance, achieving an infinite PSNR value and minimal MSE of 0, indicating superior image quality preservation and reduced data distortion compared to existing encryption methods. This signifies the effectiveness and reliability of our approach in ensuring data security, integrity, and confidentiality while facilitating seamless data embedding and extraction within encrypted images, thereby enhancing overall communication security in critical domains.

REFERENCES

[1] S. Panchikkil, V. R. Malpeddi, and V. M. Manikandan, “A Random-key Based Second-level Encryption for Reversible Data Hiding in Encrypted Images,” in 2023 National Conference on Communications (NCC), 2023, pp. 1–6. doi: 10.1109/NCC56989.2023.10067978.

[2] A. Kiran, C. Vimalarani, L. Ashwini, G. Gayithri, J. Supriya, and T. Vinod, “Secure ReversibleImage Data Hiding (SRIDH) Using LSB Prediction Method,” in 2023 International Conference on Computer Communication and Informatics (ICCCI), 2023, pp. 1–4. doi: 10.1109/ICCCI56745.2023.10128232.

[3] H.-T. Wu, Y.-M. Cheung, Z. Zhuang, L. Xu, and J. Hu, “Lossless Data Hiding in Encrypted Images Compatible With Homomorphic Processing,” IEEE Transactions on Cybernetics, vol. 53, no. 6, pp. 3688–3701, 2023, doi: 10.1109/TCYB.2022.3163245.

[4] J. Hao, P. Ping, X. Peng, and Z. Gao, “Reversible data hiding scheme based on image partitioning and histogram shifting,” in 2022 IEEE Eighth International Conference on Big Data Computing Service and Applications (BigDataService), 2022, pp. 27–34. doi: 10.1109/BigDataService55688.2022.00012.

[5] M. Xiao, X. Li, and Y. Zhao, “General Distortion Based Reversible Data Hiding for Binary Covers,” IEEE Signal Processing Letters, vol. 29, pp. 2537–2541, 2022, doi: 10.1109/LSP.2022.3227813.

[6] R. Agarwal and M. Kumar, "IWT based Reversible Data Hiding in Encrypted Domain using location map," in 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), 2022, pp. 1–5. doi: 10.1109/CISCT55310.2022.10046431.

[7] S. Ma, X. Li, M. Xiao, B. Ma, and Y. Zhao, "Fast Expansion-Bins-Determination for Multiple Histograms Modification Based Reversible Data Hiding," IEEE Signal Processing Letters, vol. 29, pp. 662–666, 2022, doi: 10.1109/LSP.2022.3149706.

[8] M. Asif, L. Kumar, G. Swami, and A. Arora, "High-Capacity Reversible Data Hiding using Deep Learning," in 2021 Asian Conference on Innovation in Technology (ASIANCON), 2021, pp. 1–5. doi: 10.1109/ASIANCON51346.2021.9544626.

[9] S. Zheng, Y. Wang, and D. Hu, "Lossless Data Hiding Based on Homomorphic Cryptosystem," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 692–705, 2021, doi: 10.1109/TDSC.2019.2913422.

[10] Y. Wang, Z. Cai, and W. He, "High Capacity Reversible Data Hiding in Encrypted Image Based on Intra-Block Lossless Compression," IEEE Transactions on Multimedia, vol. 23, pp. 1466–1473, 2021, doi: 10.1109/TMM.2020.2999187.

[11] H. Zhao, P. Ping, D. Fu, J. Hao, and Z. Gao, "Reversible data hiding based on histogram shifting with sorted pairs of points," in 2021 IEEE Seventh International Conference on Big Data Computing Service and Applications (BigDataService), 2021, pp. 201–207. doi: 10.1109/BigDataService52369.2021.00032.

[12] K. S. R. Murthy and V. M. Manikandan, "A Block-wise Histogram Shifting based Reversible Data Hiding Scheme with Overflow Handling," in 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1–6. doi: 10.1109/ICCCNT49239.2020.9225552.

[13] R. Srihitha, Y. S. Harshini, and V. M. Manikandan, "An Adaptive Multi-level Block-wise Encryption based Reversible Data Hiding Scheme," in 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS), 2020, pp. 186–191. doi: 10.1109/ICIIS51140.2020.9342695.

[14] I. G. E. Sulistyawan, A. Arifin, and M. H. Fatoni, "An Adaptive BWT-HMM-based Lossless Compression System for Genomic Data," in 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM), 2020, pp. 429–434. doi: 10.1109/CENIM51130.2020.9297871.

[15] S. Li, L. Hu, C. Sun, L. Chi, T. Li, and H. Li, "A Reversible Data Hiding Algorithm Based on Prediction Error With Large Amounts of Data Hiding in Spatial Domain," IEEE Access, vol. 8, pp. 214732–214741, 2020, doi: 10.1109/ACCESS.2020.3040048.

AUTHOR INFORMATION

Mr. Dileep Kumar serves as an Assistant Professor in the MCA Department at Dr. Ram Manohar Lohia Avadh University, Ayodhya, U.P.

Akshat Dwivedi is a Research Scholar in the MCA Department at Dr. Ram Manohar Lohia Avadh University, Ayodhya, U.P.

Shubham Chaturvedi is also a Research Scholar in the MCA Department at Dr. Ram Manohar Lohia Avadh University, Ayodhya, U.P.

Mukul is a Research Scholar in the MCA Department at Dr. Ram Manohar Lohia Avadh University, Ayodhya, U.P.

Rishabh Prajapati is a Research Scholar in the MCA Department at Dr. Ram Manohar Lohia Avadh University, Ayodhya, U.P.