WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Discrete Cosine Transform Technique in Steganography

1st Humbe Rupesh, 2nd Khond Pranesh, 3rd Ukirde Rohan, 4th Prof. Dere K. D.

[1]Student Department of Computer Engineering Jaihind College of Engineering Pune, India rupeshrh.d01@gmail.com
[2]Student Department of Computer Engineering Jaihind College of Engineering Pune, India praneshk@060gmail.com
[3]Student Department of Computer Engineering Jaihind College of Engineering Pune,India rohanukirde28@gmail.com
[4]Assistant Professor Department of Computer Engineering Jaihind College of Engineering Pune, India kapilddere@gmail.com

ABSTRACT—

This research paper aims to deliver knowledge about the Steganography technique which uses ciphering through images. Encryption is the most satisfying approach for Data Protection but nowadays technology has evolved in a way that Data leakage can be Disastrous due to high-end computers having enough power to Decipher the Data that has been hidden. A huge number of messages are circulated over the internet and carry private data which requires security and protection. The Project involves the use of the Discrete Cosine Transforms (DCT) technique and Advanced Encryption Standards (AES) in Steganography which will keep attackers away from the Data. The hidden text can only be revealed or retrieved by deciphering the image. The methodology is for securing private information or confidential Data in harmless Environments under controlled situations.

Index Terms—DCT, AES, Steganography, Encryption.

INTRODUCTION

Steganography is performed to protect data from theft, which can be done in many ways. The text hidden under the images is the method we are looking to develop in an application. The project is based on Discrete Transform (DCT) technique which will be used for hiding text under the image. The Retrieval of the image needs Decoding from the platform. The project aims to secure Data or private information by En- cryption and Decryption of the image. Proper communication between platforms will help secure the Data without third- party interference which will cause damage to the data, and the information will lose its confidentiality. A large volume of data travels through the internet which interacts with platforms to communicate with one another, which requires the proper intervention of an application or a platform that will ensure the safety of the Data. Confidentiality, Integrity, and Authenticity are the three most important factors that convey that the data is safe. Cryptography ensures data protection through Encryption and Decryption in the current scenario, but the many issues are that the attackers probably now are smart enough to decipher the encrypted data to leak or tamper with it. This Project is a solution for the confidential data that is transferred for communication. Mobile devices are drastically used nowadays, Hence an Android/IOS-based application will be efficient for the current scenario of data security as well as for the future with more improvised systems and technology. The project ensures secure data transfer while communicating within various platforms such as Android/IOS.

RELATED WORK

In this paper [1] a steganography technique in JPEG images is proposed, a text steganography technique in JPEG images is presented on the bits with the least significant value. In this technique last 2 bits of DCT coefficient are used. If in case any different compression technique used then there is possibility of data loss.The results implicate that this method is able to keep more amount of secret data while the quality of the Steagno image is almost similar to the original.

In this paper [2] I learned about the various image encryption steganography. Encryption techniques used for converting input image into cipher image. Then we use image steganography for enhancing the security of system. The encryption key will be hidden into cipher image without affecting it. This will reduce the cost of key distribution and also saves time for transmission of key between sender, receiver and third party distributer.

In this paper [3] The method proposed in this study has an advantage in the aspect of imperceptibility as evidenced by the excellent value of PSNR and MSE. Where all PSNR values are more than 50dB, so does the MSE value not more than 0.3. This method is also very simple and safe because with XOR operation steganography process can be done quickly and easily. With the XOR operator, the embedded bits cannot be directly guessed. Moreover, there are three keys used, with three times the XOR operation. The use of an integrated key in the cover image also keeps the stego file the same size, and no key delivery is required to the receiver so it can speed up the messaging process as the file size is maintained. However, based on histogram analysis there is a distinct pattern difference between the cover image and stego image.

In this paper [4] an image steganography method has been presented for hiding an image into another. Using the k-LSB-based technique the proposed method start by merging the cover image and the images to be hidden. In order to detect the region that contains the hidden images, a region detection operation has been presented using the local entropy filter. Then, after extracting the hidden image, an image quality enhancement method has been applied in order to enhance the image that can bee affected during the hiding processes.from the experimental results, and using the evaluation metrics, the proposed method can hide the images and extract it with the minimum cost in term of distortion and the lose of information.

In this paper [5] LSB substitution scheme is used for embedding any secret data into gray scale images with different pixel sizes and formats. This is done in two steps:

(i) By replacing the three least significant bits of the cover image to zero's and (ii) By replacing the same LSB's by the secret data which has to be embedded. The results show that the stego image is obtained without making a perceptible distortion. Moreover, the results of the used scheme show that the used scheme provides good balance between embedding capacity and quality of the stego image. Comparison among the various images with different formats and pixel size is also done. PSNR and MSE values are also calculated. As a future work this data embedding and analysis can be done for audio or video files.

In this paper [6] Image steganography can enhance the security of the crucial data stored in smart gadgets. Jpeg steganography is a good option as jpeg images can act as innocuous cover to hide the data because of their popularity. Many algorithms have been proposed to apply jpeg steganogra- phy. This paper discussed some of the techniques suggested by the researchers. To apply jpeg steganography, three important parameters of image steganography i.e. embedding capacity, robustness and Undetectability are considered. Jsteg was the first suggested algorithm but it suffered detectability.

SYSTEM ARCHITECTURE

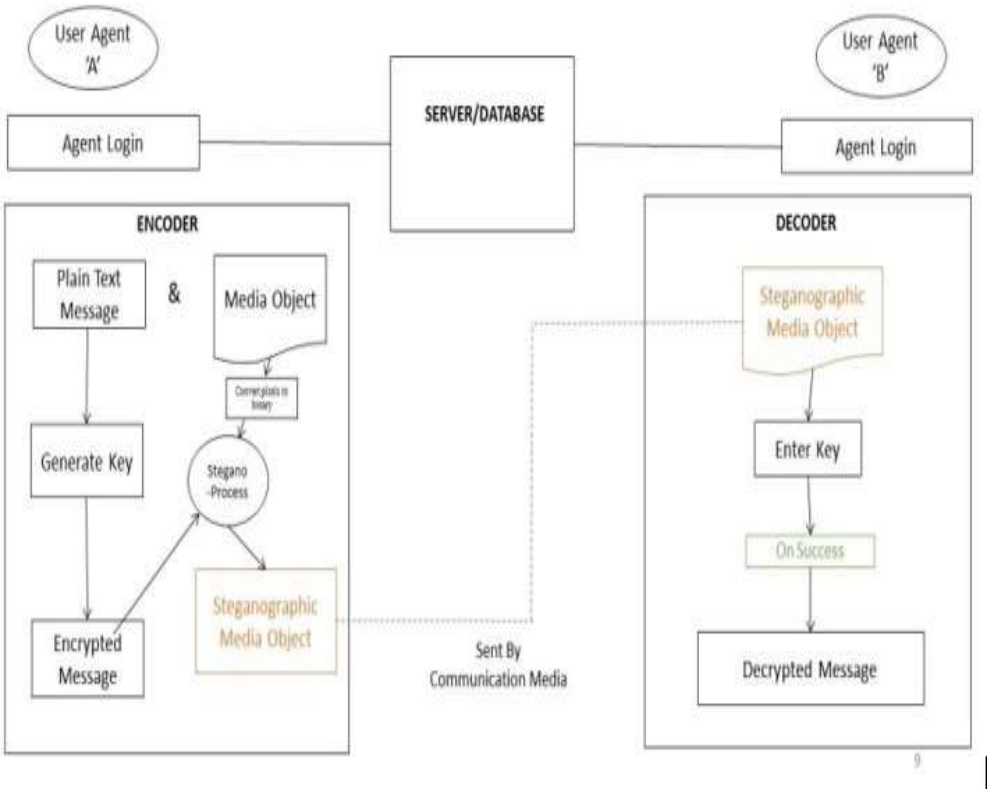

Fig. 1. System Architecture

Below figure shows the proposed system architecture where the encryption side functioning is handle by the Agent 'A' and the decryption side functioning is handle by the Agent 'B'. for both user 'A' and user 'B' side must have to go through for the login and then the agent have access to use the encryption and the decryption process. Image media object, plain text message and key is required at the encryption side then the Steganographic Media Object is given as a output by the stegano process. that steganographic media object is send to the user Agent 'B'. User Agent 'B' takes a steganographic media object (the output of encryption side) as an input. The user authentication process will takes place by entering the key which is used in the encryption side processing. After completing the successful authentication the user will be able to perform the decryption process to see the decrypted information into the plain text.

ALGORITHM

Discrete Cosine Transform (DCT):

Most commonly used transformation domain technique is DCT. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high and low frequency components. Embedding in DCT domain is simply did by altering the DCT coefficients. DCT transformation and compression using quantization and run-length coding on raw images can be used to obtain secure stego images. DCT is a lossy compression transform because its cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors in results. Variances between original data values and restored data values depend upon the method used to calculate DCT.

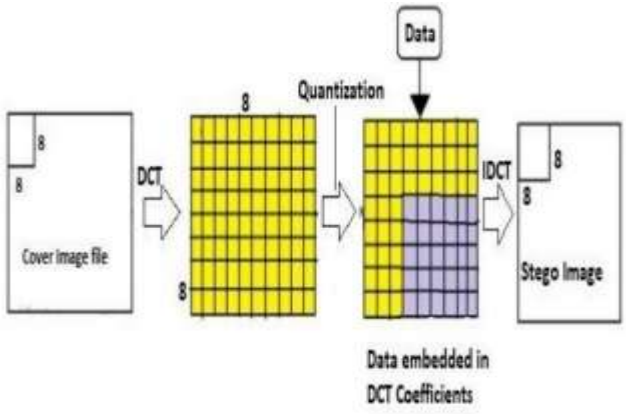

Fig. 2. Data embedding using DCT

In JPEG compression, image is divided into 8 × 8 blocks, and then the two-dimensional Discrete Cosine Transform (DCT) is applied to each of these 8 × 8 blocks. Then in LSB of each DCT coefficient the Secret image is hidden. In JPEG decompression, the Inverse Discrete Cosine Transform (IDCT) is applied to the 8 × 8 DCT coefficient blocks. For Trans4: Android/iOS Based Secure Data Transfer Application Using DCT Technique of Steganography Sinhgad College Of Engineering, Pune - Information Technology 2021-22 28 most images, much of the signal energy lies at low frequencies appear in the upper left corner ofthe DCT. Since the lower right values represent higher frequencies, and are small values, enough to be neglected with little visible distortion compres- sion can be achieved.

Advanced Encryption Standard (AES):

The Advanced Encryption Standard (AES) is a fast and secure form of encryption that keeps eyes of attacker away from our data. The earliest types of encryptions were simple, using techniques like changing each letter in a sentence to the one that comes after it in the alphabet. As people got better at cracking codes, the encryption had to become more sophisticated so that the messages could be kept secret. The rise of electronic communication and the increasing use of internet becomes the need for encryption. In the 1970s, the US National Bureau of Standards (NBS) began searching for a standard encryption technique that could be used to encrypt sensitive government information. A result of their search was to adopt a symmetric key algorithm developed at International Business Machines (IBM), which was called as Data Encryption Standard (DES)

The first thing that happens is that your plaintext (which is the information that you want to be encrypted) is separated into blocks. The block size of AES is 128-bits, so it separates the data into a four-by-four column of sixteen bytes (there are eight bits in a byte and 16 x 8 = 128). The different transformations operate on the intermediate results, called state. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4. (In the Rijndael version with variable block size, the row size is fixed to four and the number of columns varies. The number of columns is the block size divided by 32 and denoted Nb). It is important to know that the cipher input bytes are mapped onto the state bytes in the order (a0,0, a1,0, a2,0, a3,0, a0,1, a1,1, a2,1, a3,1 ...)

A State:

a0,0	a0,1	a0,2	a0,3
a1,0	a1,1	a1,2	a1,3
a2,0	a2,1	a2,2	a2,3
a3,0	a3,1	a3,2	a3,3

The cipher key is similarly pictured as a rectangular array with four rows. The number of columns of the cipher key, denoted Nk, is equal to the key length divided by 32, and the bytes of the cipher key are mapped onto the array in the order (k0,0, k1,0, k2,0, k3,0, k0,1, k1,1, k2,1, ...)

A Key:

k0,0	k0,1	k0,2	k0,3
k1,0	k1,1	k1,2	k1,3
k2,0	k2,1	k2,2	k2,3
k3,0	k3,1	k3,2	k3,3

At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds.

RESULTS

Fig. 3. Splash Screen Page

Fig. 4. Intro Slider Page

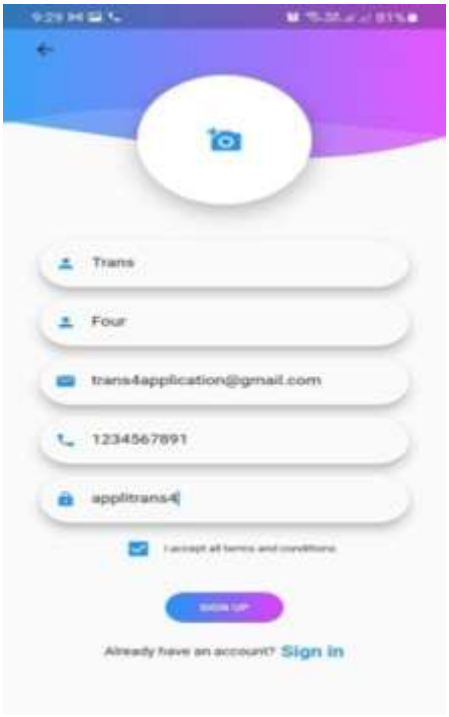

Fig. 5. Sign-Up Screen

Fig. 6. Sign-In Screen

Fig. 7. Encryption Screen

Fig. 9. Password Reset Screen

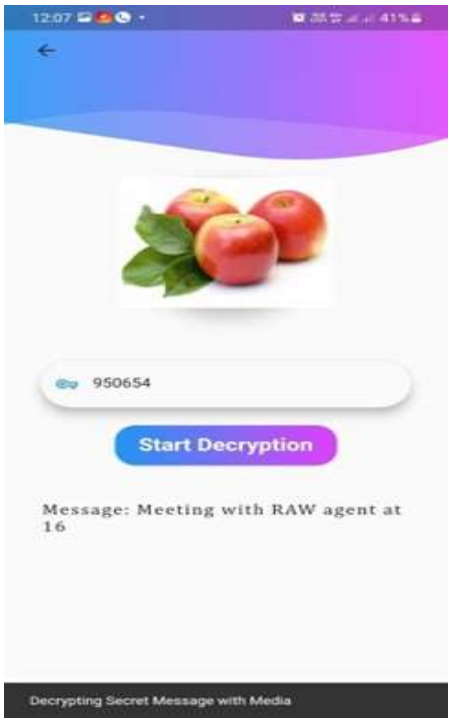

Fig. 8. Decryption Screen

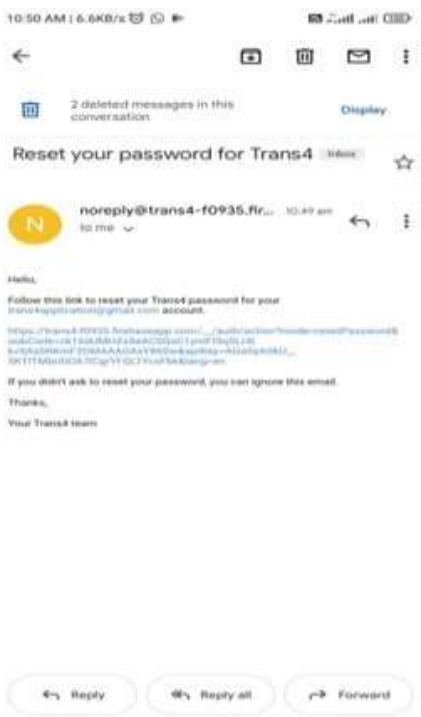

Fig. 10. Password Reset Gmail Screen

CONCLUSION

Steganography is a technique of writing secret message, such a way that no one can doubt for the existence of the message apart from the sender and considered recipient. It is possible by using only steganography technique the external entity can detect presence of text message in the image file and then might be successful in extraction of secret information from the encrypted image . However, if we use both steganog- raphy and AES methods, this

will lead to ‘security in depth’. We have proposed our project plan to build our system to hide the secret data into the cover image using steganography and AES methods that are combined together to achieve much stronger encryption routines.

FUTURE SCOPE

The work presented in this thesis is, hopefully, compre- hended within the defined scope, but research never ends, therefore, future research is expected to explore horizons be- yond the scope of this thesis. The effectiveness and efficiency of the proposed system can be improved and enhanced in the way of capacity, Security and robustness. Strict algorithm can be performed either privately, or in a public way of embedding the secret message and made them secure and robust. A more concrete model is expected by analyzing the probability that the hidden message can be robust at a certain data hiding rate. Several algorithms in the area of image steganography have been successfully developed. Therefore, the proposed algorithms are only focused on the combing text and image. The extension of currently proposed methods to the other multimedia such as video, Audio and other type of image steganography is also interesting research topic.

ACKNOWLEDGMENT

I would like to take this opportunity to thank my guide Prof. K. D. Dere. and Project co-ordinator Dr. S. D. Gunjal for giving me all the help and guidance we needed. we really grateful to them for their kind support. Their valuable suggestions were very helpful. We also grateful to Dr. A. A. Khatri, Head of Computer Engineering Department. Jaihind college of Engineering,Kuran for his indispensable support, suggestions. We also want to express our gratitude to Dr. D.

J. Garkal, the principal of Jaihind College of Engineering in Kuran, for his invaluable advice and support. We also thank All Staff Members, at Jaihind College of Engineering. Kuran, for their invaluable assistance and advice.

REFERENCES

Darbani, A., AlyanNezhadi, M. M., Forghani, M. (2019, February). A new steganography method for embedding message in JPEG images. In 2019 5th conference on knowledge-based engineering and innovation (KBEI) (pp. 617-621). IEEE.

Dahiya, M., Kumar, R. (2018, December). A Literature Survey on various Image Encryption Steganography Techniques. In 2018 First International Conference on Secure Cyber Computing and Communica- tion (ICSCCC) (pp. 310-314). IEEE.

Astuti, Y. P., Rachmawanto, E. H., Sari, C. A. (2018, March). Simple and secure image steganography using LSB and triple XOR operation on MSB. In 2018 International Conference on Information and Com- munications Technology (ICOIACT) (pp. 191-195). IEEE.Elharrouss, O., Almaadeed, N., Al-Maadeed, S. (2020, February). An image steganography approach based on k-least significant bits (k- LSB). In 2020 IEEE. International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 131-135). IEEE

Kaur, H., Kakkar, A. (2017, September). Comparison of different image formats using LSB Steganography. In 2017 4th International Conference on Signal Processing. Computing and Control (ISPCC) (pp. 97-101). IEEE.

Watni, D., Chawla, S. (2019, October). A comparative evaluation of jpeg steganography. In 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 36-40). IEEE.

Bandekar, P. P., Suguna, G. C. (2018, October). LSB Based Text and Image Steganography Using AES Algorithm. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 782-788). IEEE.

Zhang, Q., Ding, Q. (2015, September). Digital image encryption based on advanced encryption standard (aes). In 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Commu- nication and Control (IMCCC) (pp. 1218-1221). IEEE.