IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006079 |

Hiding Data in the Images Using Steganography Techniques

Aeman A. Patel, Dr. Rachana. Y Patil

PG Student, Dept. of C.S., Pimpri Chinchwad College of Engineering, Pune, India

Assistant Professor, Dept. of C.S., Pimpri Chinchwad College of Engineering, Pune, India

ABSTRACT: Steganography key goals are undetectability, resilience (i.e. resistance to various image processing methods), compression, and capacity of the concealed data. Steganography is distinguished from comparable techniques such as watermarking and cryptography based on these features. This work proposes a novel Steganographic method for conveying pictures based on the discrete Curvelet transform.

.

KEYWORDS: Steganography, LSB, DCT, DWT, Curvelet Transform

I. INTRODUCTION

Steganography is a Greek term that means "enclosed or secret writing." Data concealment should be utilised in the form of covert transmissions, closed captioning, indexing, or watermarking. In contrast to cryptography, where the message's survivability is not veiled, but the content is hidden, Steganography is used in a variety of domains, including military and industrial uses. The technique stretches back to ancient times, when messengers hid tattooed messages on their scalps, which were exposed by shaving. Computer advancements have made steganography simpler since the 1980s. Everything from speech over IP to digital file systems may now be used to conceal more information in increasingly sophisticated ways.

Messages in digital files may be read and encoded by hundreds of computer applications. Plainly visible encrypted messages, no matter how impenetrable, will draw suspicion and may be damning in nations where encryption is prohibited. The frequency domain approach is the topic of this study. The curvelet transform has gotten a lot of interest in a variety of signal processing applications, including picture watermarking. The core notion of curvelet transform is derived from multi-resolution analysis. This entails dividing a picture into frequency channels with constant bandwidth on a logarithmic scale. With a wide range of applications in signal processing and statistics. With general, in steganography, the real information is not kept in its original format and is instead translated into a similar multimedia item, such as a picture, video, or audio, which is then buried within another object. This apparent message (known as cover text in common parlance) is forwarded across the network to the receiver, where it is separated from the true communication. Steganography is a method of achieving data privacy over secrecy.

Information security has become an important factor in the modernization of communications. That's why data can be encrypted and transmitted. Data is usually exchanged over the Internet. Every day some kind of data can be seen on the Internet such as pictures, videos, audio, text etc. Other data can be encrypted through the image if wanted. For hackers, huge amounts of information are being lost during transmission. So in the field of information and communication, security measures are taken like cryptography and Steganography. Steganography can hide data via audio, video, text, images. In this paper the method have been presented in which used two important algorithms have been used, one is Advanced Encryption Standard (AES) and the other is RC5. As known, AES can create a 128-bit cipher text and in our method, the 128 bit of block size is used in the RC5 algorithm. Watermark will also be created on each image so that the pictures are transmitted through confidential security. LSB, DCT, DWT are among the few ways a cover image can be composed.

II. RELATED WORK

It created steganographic strategies for spaces utilizing XOR administrators. Message input is finished with the initial two XOR capacities set at one and eighth pieces and the second at 2, seventh piece. The exhibition result is then analyzed and utilized as a message input message. The cover picture is a 512 * 512 dark picture with three message sizes, 1024 pieces, 2048 pieces, and 4096 pieces. The measure of PSNR got is roughly 69 dB with a message length of 4096 pieces. [1]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006079 |

It proposed steganographic systems and LSBs incorporated with XOR administrators. The message is stuck to three more modest pieces. There before the encryption of mystery, messages made XOR work. With the dim cover's picture size, 256 * 256 pixels can be inserted with a sizeable 196608-piece message. Simultaneously, the measure of PSNR found in high implanting is more than 37 dB. [2]

It proposing Steganography in photography utilizing a fracture cycle in pieces 5 and 6. In the event that there is a distinction in pieces 5 and 6 which is equivalent to the bits of secret data, at that point no change is conceivable. Meanwhile, if there is a distinction in worth, the worth changes to fifth piece with the goal that the estimation of the distinction relates to the base an incentive in the classified data. The cover picture utilized is a dark picture and shading picture with size 512 * 512. Along these lines, PSNR 51.17977 dB in Lena's grayscale picture and PSNR 52.3438 in Lena's shading picture, with a stacked heap of 262144 pieces. [3]

It proposed arrangement in which they consolidate three calculations: RSA, Vigenere Cipher and Message Digest 5 (MD 5). The mix of TheMD5 and Vigenere improves result than simply hash work. The mix of this capacity is done in the picture and the picture document name: vigenere and RSA and coded. The closeness of MD5, Vigenere and RSA is a cryptographic calculation, so the calculation has been effectively coordinated. This calculation can shield you from picture control or different picture changes. [4]

Despite the fact that the pixels have changed marginally, as proven by the PSNR estimation of up to 86.7532 dB, the calculation effectively distinguishes pixel picture advances and document name changes to the computerized signature picture. Along these lines, if the cycle of picture move happens a twisting that is harming the picture, this calculation can make security more secure.

This paper proposes the utilization of Discrete Cosine Transform (DCT) in light of 8x8 squares to change the first picture from an area over to a typical space. The impact of the DCT change will deliver A.C. what's more, D.C. coefficients Next, DC coefficients are gathered in the framework to be changed over through DWT. The DWT change impact produces four sub bands.

The L.L. sub band is then chosen to embed copyright as a double picture with a specific measure of watermark power. The last advance in changing over DWT-DCT transformation is to create a picture with a watermark. In view of the after effects of this examination, elevated levels of obscurity were affirmed by PSNR and MSE. [5]

Social organizations, for example, the Internet are advancing, quicker, and less expensive, to utilize data trade. This can build the odds of secret data being taken and misused by unapproved people. This investigation proposed a blend of two Steganography areas combined with Cryptography which expected to make private data safer and difficult to reach to unapproved people. Messages are scrambled utilizing the 3-DES strategy. [6]

In this investigation, the StegoCrypt cycle is proposed utilizing a blend of Discrete Wavelet Transform (DWT) and One-Time Pad (OTP). The cover picture in size 512 * 512 is changed over by Wavelet transformation of four levels. In the first to third level, subband L.L. is chosen to procure LL3 subband. In the fourth stage, LL3 is then changed over to HH4 subband with the assistance of wave transformation. [7]

In this paper it additionally proposes message inserting in the region at the edge of the picture. In his exploration he joined steganography methods utilizing LSB procedures and cryptographic strategies utilizing DES. Before the image message is entered, the message is encoded utilizing the DES technique.

The cover picture utilized is a shading picture with a size of 1024 * 1024, and this message is additionally a shading picture with a size of 64 * 64. As per the consequences of this investigation, the normal estimation of PSNR 72.21584 dB, found in five sorts of pictures. [8]

III. PROPOSED ALGORITHM

A. *Curvelet Transform:*

The Curvelet transform is a higher dimensional generalization of the Wavelet transform designed to represent images at different scales and different angles. Curvelet enjoy two unique mathematical properties, namely: Curved singularities can be well approximated with very few coefficients and in a non-adaptive manner - hence the name "Curvelet." Curvelet remain coherent waveforms under the action of the wave equation in a smooth medium.

Actually the ridge let transform is the core spirit of the Curvelet transform. In 1999, an anisotropic geometric wavelet transform, named ridge let transform, was proposed by Candies and Donoho. The ridge let transform is optimal at representing straight-line singularities.

Unfortunately, global straight-line singularities are rarely observed in ral applications. To analyse local line or curve singularities, a natural idea is to consider a partition of the image, and then to apply the ridge let transform to the obtained sub-images. This block ridge let-based transform, which is named Curvelet transform, was first proposed by Candes and Donoho in 2000.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006079 |

Apart from the blocking effect, however, the application of this so-called first generation Curvelet transform is limited because the geometry of ridge lets is itself unclear, as they are not true ridge functions in digital images. Later, a considerably simpler second-generation Curvelet transform based on frequency partition technique was proposed. The second-generation Curvelet transform has been shown to be a very efficient tool for many different applications in image processing. The overview of the Curvelet transform is shown below for four STEPS:

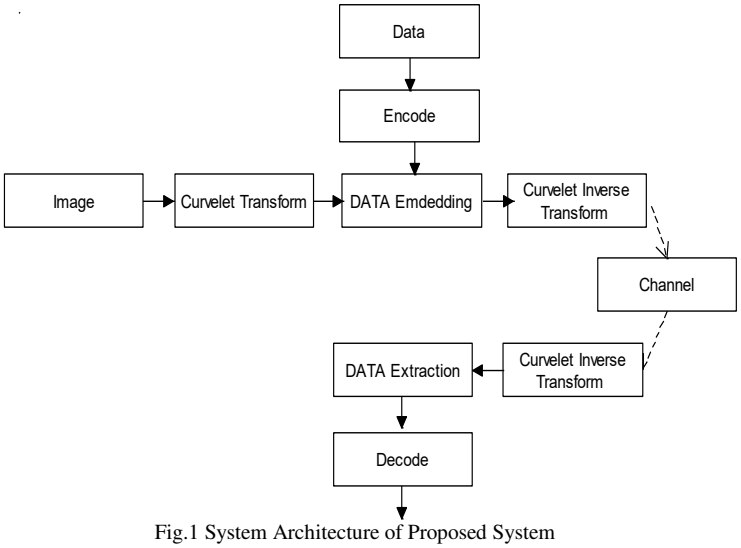

Fig.1 System Architecture of Proposed System

B. *Description of the Proposed Algorithm:*

Input: A cover-image of size w × w and secret-image of size h × h.

Output: A stego-image of size w × w.

1) Select a cover-image of size w × w and secret-image for hiding of size h × h.

2) Radon Transform for secret-image is used to increase security of embedded image.

a) The Radon Transform will randomly permute the data so that nobody can read the secret image without taking the inverse Radon Transform.

b) Also nobody can guess the generated Radon sequence without knowing the secret key. This ensures that only recipients who know the corresponding secret key will be able to extract the message from the stego image.

3) Decompose the cover-image by using the Curvelet transform.

4) Convert the secret-image into a 1D bit stream.

5) The data sequence should be inserted into the least significant bit (LSB) of the Curvelet sub bands according to data length, since the receiver must know the data length in order to extract the data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006079 |

IV. CONCLUSION AND FUTURE WORK

In this study, we broaden our field of study by encrypting picture data and employing images in the embedding process. In this research, we introduced a combined steganography technique based on the discrete curvelet transform (dct), which provides picture security as well as the authenticity of the image creator in an online setting. The suggested solution for picture transmission security would be extremely useful in the internet, where a significant number of users share photographs via email and social networking sites. It is critical in both defence and civil uses. This might also be useful in space technology, as satellites relay photographs of planets, keeping them from falling into the hands of the wrong people. As a result, the nation's overall security would benefit.

REFERENCES

1. K. Joshi, P. Dhankhar and R. Yadav, "A New Image Steganography Method in Spatial Domain Using XOR," in Annual IEEE India Conference (INDICON), New Delhi, 2015.
2. K. Joshi and R. Yadav, "New Approach Toward Data Hiding using XOR for Image Steganography," in International Conference on Contemporary Computing (IC3), Noida, 2016
3. A. U. Islam, F. Khalid, M. Shah, Z. Khan, T. Mahmood, A. Khan, U. Ali and M. Naeem, "An Improved Image Steganography Technique based on MSB using Bit Differencing," in International Conference on Innovative Computing Technology (INTECH), Dublin, 2016.
4. R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICONSONICS), Yogyakarta, 2017.
5. A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, 2017.
6. G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi and E. H. Rachmawanto, "Hybrid Method using 3-DES, DWT and LSB for Secure Image Steganography Algorithm," in International Conference on Information Technology, Information System, and Electrical Engineering (ICITISEE), Yogyakarta, 2017.
7. A. Setyono, D. R. I. M. Setiadi and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2017.
8. E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto and D. R. I. M. Setiadi, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in International Conference on Innovative and Creative (ICITech), Salatiga, 2017.
9. C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in International Conference on Informatics and Computational Sciences (ICICoS), Semarang, 2017.
10. Y. P. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, 2018, pp. 191-195, doi: 10.1109/ICOIACT.2018.8350661.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details