International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

AN INNOVATIVE HASHKEY CRYPTOGRAPHY-BASED METHOD FOR WATERMARKING 3D OBJECTS

[1]K .Bhargavi, [2]Dr.Ch.Venugopal Reddy,[3]M.Sreeja ,[4]N.Vijayalakshmi, [5]D.Sai Sowmya

[2] Asst.prof,ECE Dept, RISE Krishna Sai Prakasam Group of Institutions,Ongole-523001,AP
[1,3,4&5]IV-B.Tech(ECE) RISE Krishna Sai Prakasam Group of Institutions,Ongole-523001,AP
(1karyambhargavi@gmail.com;2phdvenu@gmail.com;3sreejaravindhar@gmail.com;4nvlnagireddy@gmail.com; 5saisowmyadasari@gmail.com)

ABSTRACT

For a number of uses, a watermark embeds copyright and caption information into the data (image, video, and audio) by adding an invisible signal. Before describing the basic 3D watermarking standards, the proposed research project explains how 3D watermarking would be employed in this work. After that, fundamental attacks on 3D geometry watermarking are discussed, along with solutions. The previous study concentrated on hiding the data without altering the data or signal distortion in order to eliminate a watermark. Nonetheless, watermarks are frequently used to control copyright, forbid alteration, and permit the manipulation of signals. This research presents a novel hash key cryptography method for image watermarking.The watermark item is encrypted and decrypted using a hash key. It is improving the security of the watermarking approach

Keywords:
Cryptography,Watermarking,Encryption,Decryption,Image compression,Data hiding, Attacks secret image,Frames,Wavelet transforms,Visible and invisible technologies

INTRODUCTION

Since digital technology is a rapidly developing and expanding field, the inability to tolerate copying of digital content has led to the need for content ownership, or copyright protection. One way to address this issue is through watermarking [1], where a hidden, indiscernible text is imprinted in the original material so that the content quality remains appropriate. The owner of the original work can demonstrate originality by extracting the watermark from the data. Figure 1 shows the watermarking techniques that are very commonly used in the digital marketing process.As the embedder inserts the genuine message into the actual image at the embedder site, the data is transmitted via a medium channel. This data or image may degrade, convert, or undergo other signal processing during transmission via a media. The detector aims to eliminate the embedded picture from the final image after striking the target. Depending on the application's architecture, the presence of original data is frequently required during the detection process. When it comes to telecommunication,3D digital data has been widely employed in hardware design, multimedia, motion, etc. These 3D data are typically characterized by polygonal meshes, which cause deformation when watermarking, compression, and filtering are applied. Securing the transmission between the transmitter and the receiver is the aim of a revolutionary 3D objective watermarking approach that uses hash key cryptography. defending against third parties and hacking.

LITERATURE SURVEY

This paper discusses techniques for embedding data into three-dimensional polygonal models of geometry.The techniques presented here generate polygonal models with data contained in either their vertex coordinates, their vertex topology (connectivity), or both, given objects that are points, lines, (connected) polygons, or curved surfaces. Examples of applications for such data embedding include theft prevention, copyright protection, copyright notice, and inventory management for 3-D polygonal models. Following an explanation of the background and prerequisites, the topic of where and how data can be included into 3-D polygonal models is covered. A number of data embedding algorithms based on these basic techniques are then presented in the paper along with examples. We demonstrate the feasibility of embedding data into 3-D polygonal models using these approaches and examples.

In the all-optical domain, we suggest an optical image concealment technique based on compressive sensing (CS) and dual-channel simultaneous phase shifting interferometry (DCSPSI). The DCSPSI design first embeds a hidden image in the host image without damaging the original host's form. Then, two CCDs concurrently collect two interferograms with $\pi/2$ phase shifts that are caused by the polarization components. After that, CS further compresses the holograms to sample the less data. The suggested approach will significantly lower the interferogram data volume and offer a practical solution for the transmission of optical images securely in real time. The experimental outcome shows that the suggested approach is both viable and valid. It used simultaneous phase shifting interferometry to boost the data capacity.It decreased the amount of data stored and was especially helpful for applications with constrained bandwidth.Because phase shifting and other precision equipment are required, the system costs a lot of money. Interferometry Sensitive environmental factors include temperature fluctuations and vibrations.

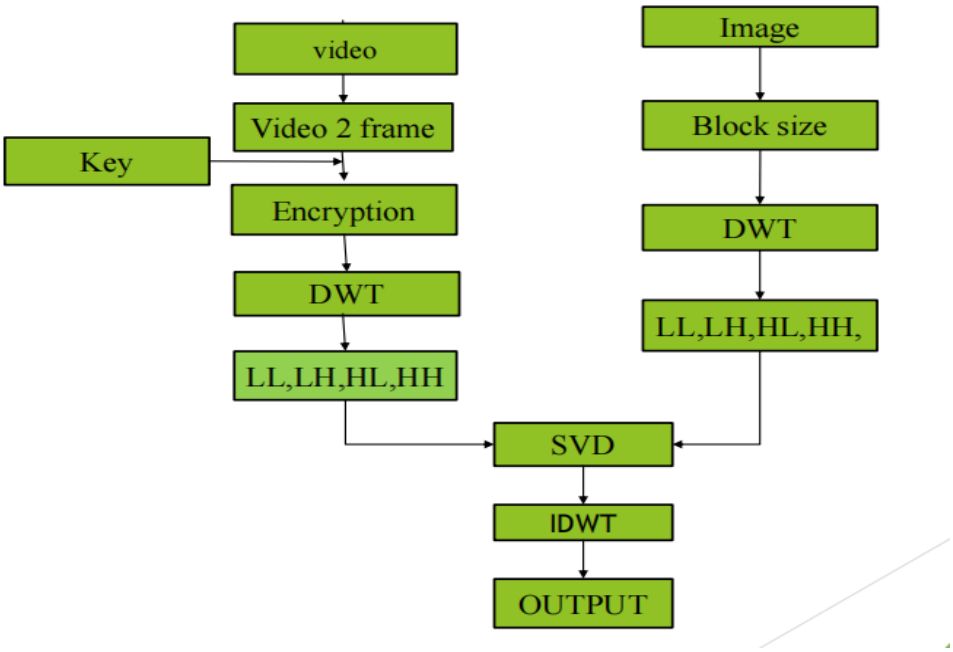
This study introduces a new geometry-based watermarking method for 3D models that guarantees blind detection and robustness. Our approach embeds a watermark by taking advantage of intrinsic geometric features, which makes it resistant to several types of attacks. Accurately evaluating 3D meshes' visual quality has grown more crucial as a result of their extensive availability and use in a variety of applications. Despite the importance of this task, there aren't many No-Reference (NR) methods available in the literature for assessing 3Dmeshes' visual quality. This research fills this gap by putting out a novel NR method designed especially for 3D mesh quality scoring. A pre-trained convolutional neural network automatically extracts deep features from a 3D mesh after it has been rendered into 2D views and patches. The quality score of the produced images is then predicted using these attributes in a Multi-Layer Perceptron regressor.

After combining the acquired scores with the matching BRISQUE scores, the final score is predicted using a second MLP regressor. We provide experimental findings that show our method's efficacy and resilience on a variety of challenging 3D mesh datasets. The suggested approach's improved performance and adaptability are highlighted by comparisons with current NR approaches. All things considered, this work advances NR methods for evaluating 3D mesh quality and provides a useful resource for scholars, professionals, and developers working with 3D models in a variety of fields.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

EXISTING SYSTEM

The current methods for watermarking 3D objects frequently entail inserting watermarks into either:1.Spatial domain: Modifying the 3D object's vertices, edges, or surfaces directly is known as the "spatial domain."2. Transform Domain: including the watermark into the 3D object's frequency or wavelet coefficients. To protect the watermark, these strategies are coupled with conventional cryptographic procedures. Unauthorized access is avoided by using the cryptographic key to embed and extract the watermark.Input: Cryptographic key, watermark information, and the original 3D object. Embedding Techniques:1.Geometry-BasedEmbedding: Changing the mesh's topology or vertex coordinates. 2. Transform-Based Embedding: incorporating data into representations that have been altered (e.g., Discrete Wavelet Transform, Discrete Fourier Transform)



Existing system

DATA ENCRYPTING IN A BINARY IMAGE BASE ON MODIFIED

1.DATA HIDING METHOD :

This encryption method replaces a mystery bit with a modified piece location to control sub-partitioned squares. At least three pixels from the host paired image are present in the sub-separated square. Each square choose to conceal a mystery. The visual nature of the obvious parallel picture can be enhanced by determining the pixel position to incorporate a surprise bit for every square.

2. ENCRYPTING METHODS

Let C be the mXn-bit mystery information and let H be the host double picture of MXN pixels. Another pixel value is denoted as h'(i,j) for pixel esteem h(i,j) of H. An information bit is shrouded using the accompanying processes. For a specific H. To hide a mystery information

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

bit, pick a sub-partitioned square Buv of size pXq. Summing all pixels of Buv.If S(Buv) is equivalent to 0 or pXq, isn't utilized to store a mystery information bit in the square.If mod(S(Buv),2) is equivalent to the C(z), at that point don't roll out an improvement and spare the information bit in this square. If the C(z) is not equal to mod(S(Buv),2)Allow H* to be a simple double image that has been altered from H, and give H the opportunity to be a host twofold picture. Encoded codes are present in the clear picture H*'s constituent parts, and they are grouped into five groups. The underlying location is determined by using the identifiable proof codes to determine whether or not the codes jumbled in H* employ the encoding approach suggested in this research.The underlying position of the upper left of the sub-separated square is distributed using codes.

PROPOSED SYSTEM

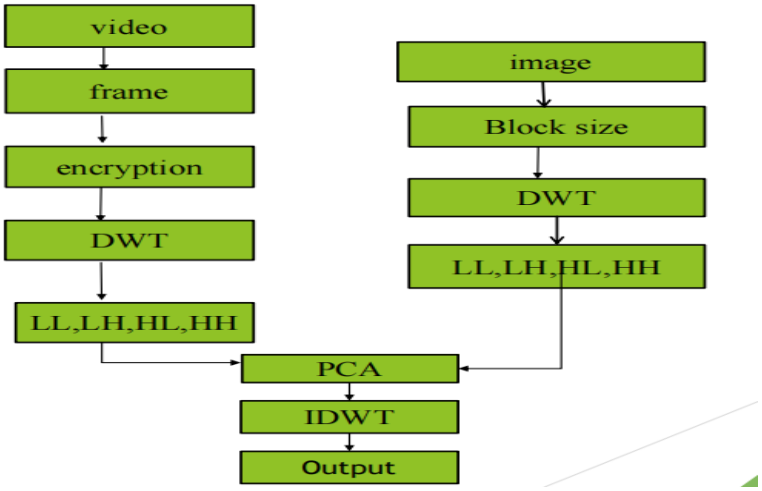
Proposed techniques for The simulation results show that when noise disturbing attacks the encrypted image or shear transformation attacks the encrypted image.The information in the matching decrypted image is destroyed when an image or shear transformation attack is made on the encrypted image. This indicates that the permutation transform mentioned above is not resistant to shear transformation and noise disturbance attacks. We will provide a novel approach to address this issue and improve the security of the aforementioned picture encryption algorithm. The basic concept is to store each pixel of the image in multiple locations. Here is a description of the improved algorithm. This is how the rest of the paper will be structured. We will begin by giving a quick overview of the integer wavelet transform. Second, we'll go over the suggested encryption scheme. After discussing the data obtained, we will wrap up the paper and make recommendations for future system enhancements

Image Encryption: Assume the original image with a size of N1XN2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as bi,j,0,bi,j,1,…,bi,j,7 where 1<=i<=N1 and1<=j<=N2, the gray value as, and the number of pixels as N(N=N1XN2).That implies In encryption phase, the exclusive-or results of the original bits and pseudo- random bits are calculated. When stream cipher is employed, the encrypted image is generated by

$$[[f]]=Enc(f,K)=f+k$$

Where f and [[f]] denote the original and the encrypted images, respectively. Here, K denotes the key stream generated using the secret encryption key K . In this paper, without loss of

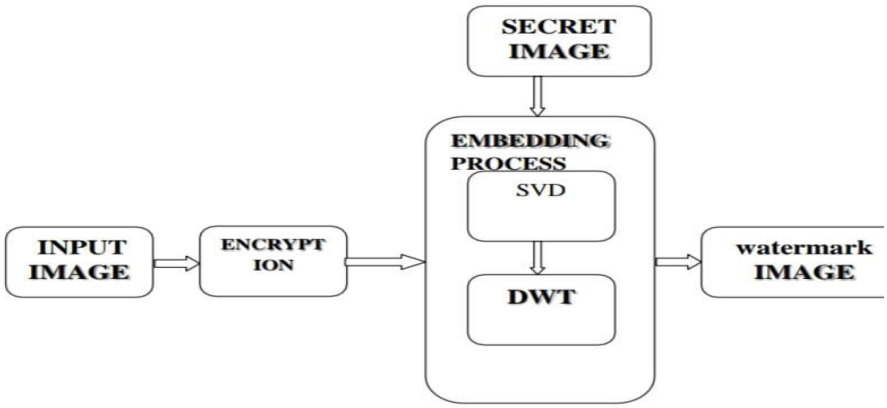
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



Proposed system

DISCRETE WAVELET TRANSFORM

By hiding data in areas that the human visual system (HVS) is less sensitive to, including the high resolution detail bands (HL, LH, and HH), we can improve robustness without sacrificing visual quality. This is made possible by the wavelet domain. An integer data set can be mapped into another integer data set using the integer wavelet transform. Any truncations of the floating point values of the pixels that should be integers may result in the loss of the hidden information and the failure of the data hiding system because the wavelet filters used in the discrete wavelet transform have floating point coefficients.



LL Sub band distorted image

By hiding data in areas that the human visual system (HVS) is less sensitive to, including the high resolution detail bands (HL, LH, and HH), we can improve robustness without sacrificing visual quality. This is made possible by the wavelet domain. An integer data set can be mapped into another integer data set using the integer wavelet transform. Any truncations of the floating point values of the pixels that should be integers may result in the loss of the hidden information and the failure of the data hiding system because the wavelet filters used in the discrete wavelet

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

transform have floating point coefficients.resulting LL sub-band is distorted as shown in above figure.

Image of DWT

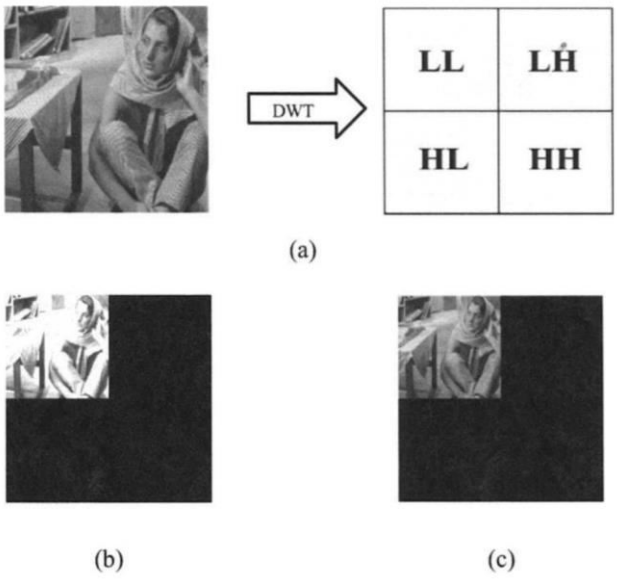


Fig 4.2 Images of DWT

Essential Attacks And Their Solutions In 3d Geometry Watermarking:

Translation attack:Placing an object so that its mass center matches the original coordinate system is known as a translation attack . Invariant metrics are formerly employed for translation in embedding (e.g. A mesh triangle composed of comparable angle set). Rotation attack:Theelement's z-axis coordinates are turned so that they align with the main component . Invariant metrics were previously utilized for rotation in embedding (e.g. A mesh triangle composed of similar angle sets).Additive Noise attack:Following frequency-based modification, a watermark is applied to the mesh model and encoded into each resolution's coefficients. Methods for Transforming Domains.Compression attack: Watermarks are applied to the coefficients of each resolution after frequency-based modification across the mesh model. (Transform Domain Techniques) The suggested approach provides an example of how to use a cryptographic hash key for watermarking. The process is made more secure by the algorithm's introduction of security measures.

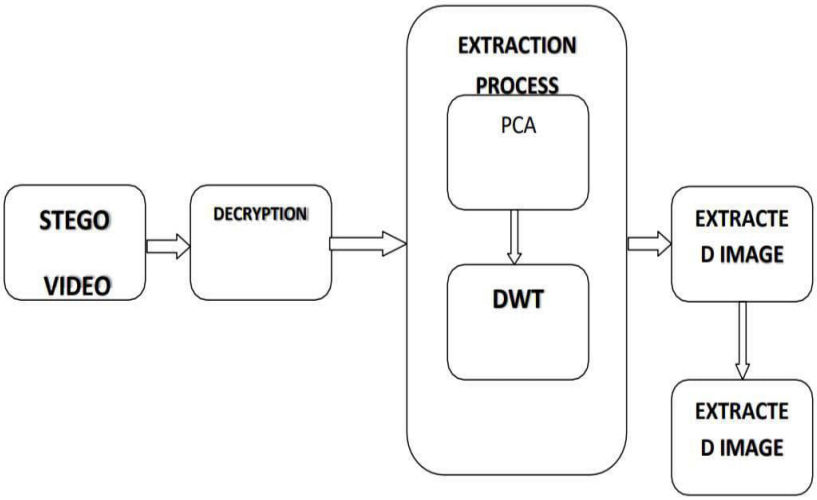
The strategy employed in this paper is one of several methods for performing integer wavelet transforms, including lifting schemes. The example below demonstrates how lifting strategies can be used to generate integer wavelet transforms without sacrificing invertibility by simple truncation. Simple pairwise averages and differences can be used to express the Haar wavelet transform

IMAGE DECRYPTION AND DATA EXTRACTIONANDCONTENT RECOVERY

Subsequent to getting an encoded picture containing extra information, the collector right off the bat performs unscrambling utilizing his private key. We mean the unscrambled pixels as m'(i, j). Due to the homomorphic property, the decoded pixel esteems in Set A meet

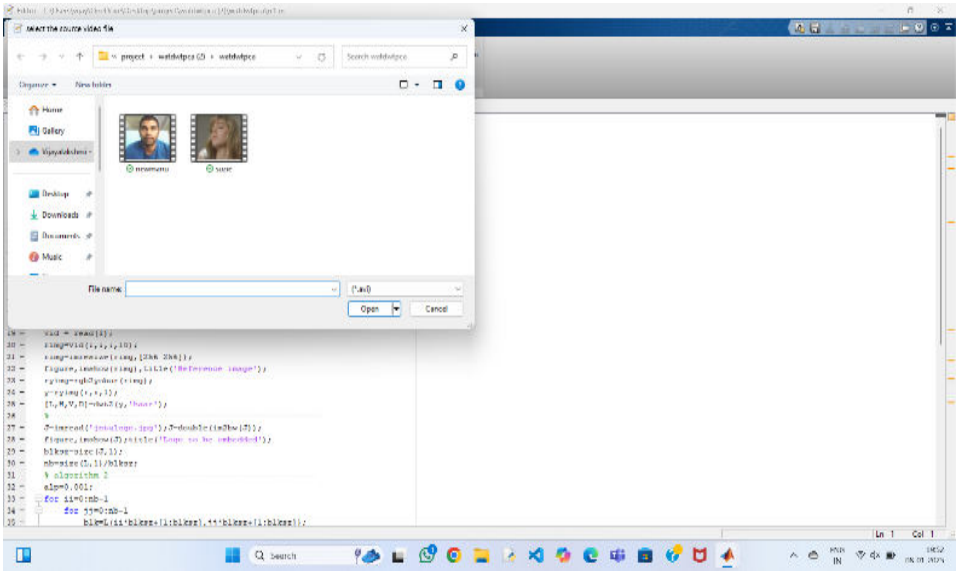
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Then again, the unscrambled pixel esteems in Set B are simply mT(i, j) since their ciphertext qualities are unaltered in information inserting stage. At the point when δ is little, the unscrambled picture is perceptually like the first plaintext picture. At that point, the beneficiary with the information concealing key can separate the installed information from the straightforwardly unscrambled picture.



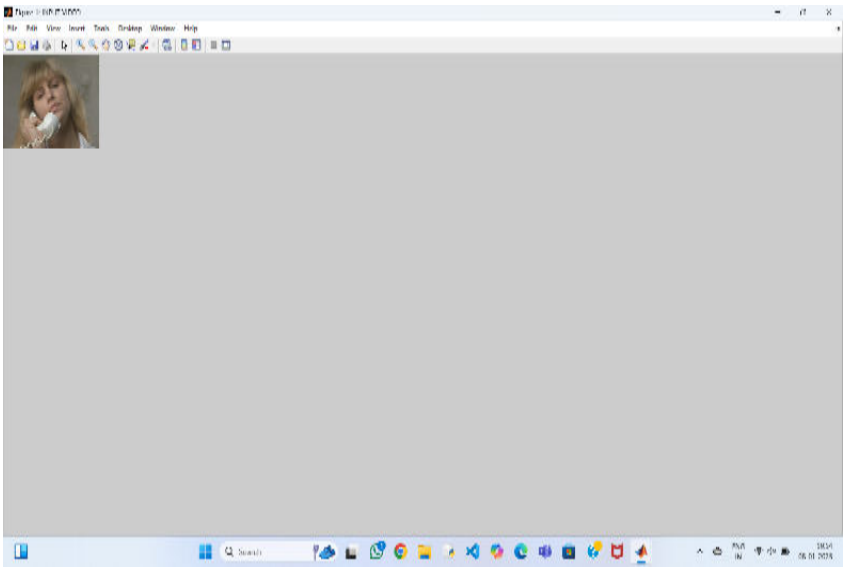
Unscrambled picture

OUTPUTS

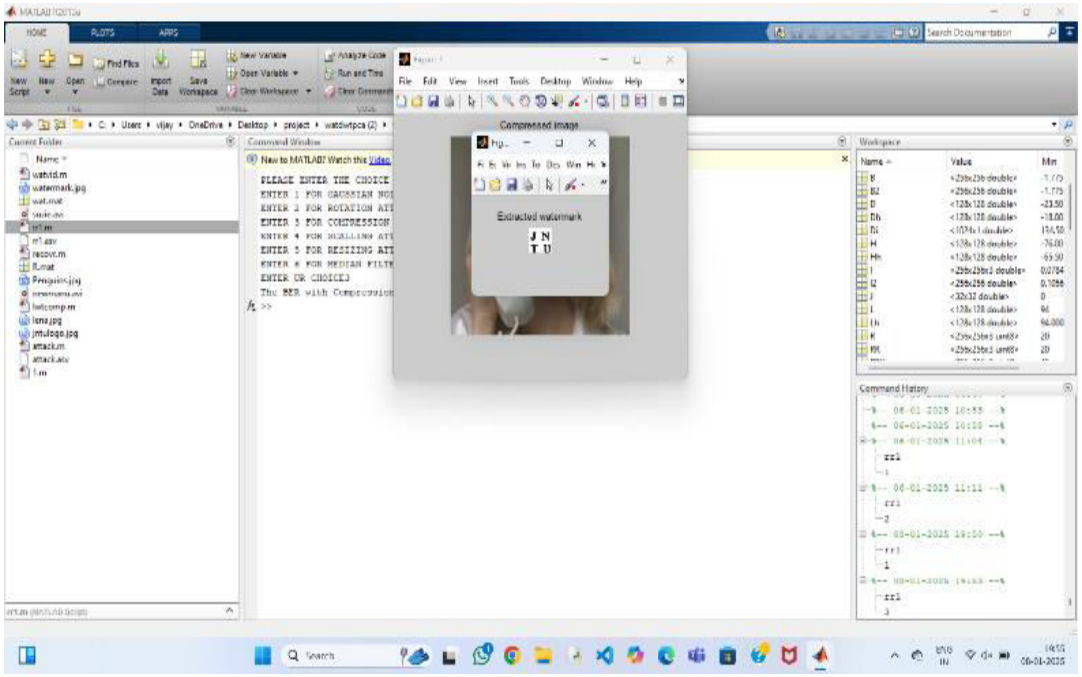


Selecting input video

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362



The selected video after attacks



The final output message

CONCLUSION

For figure content images encoded using open key cryptography, this work suggests a lossless, reversible, and consolidated information hiding scheme with probabilistic and homomorphic features. In the lossless plan, new attributes are used to implant the additional information into the LSB-planes of the cipher text pixels, replacing the figure content pixel esteems. Therefore,

the information insertion task has no effect on the unscrambling of the unique plaintext picture, and the implanted information can be legally extracted from the scrambled area. In the reversible plan, half of the cipher text pixel values are changed for information installation, and a preprocessing of the histogram therapist is done before to encryption.Even though the unscrambled picture shows a minor distortion, the first plaintext picture can be recovered without any errors if the collector removes the excess information from the plaintext area. The information implanting operations of the reversible and lossless plans can be carried out simultaneously in an encoded image due to the two plans' similarities. In this manner, the collector can recover the first plaintext image in the plaintext area, concentrate another piece of implanted information, and remove a piece of installed information from the scrambled space.

REFERENCES

[1] A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.
[2] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits
and Systems for Video Technology, 13(8), pp. 890−896, 2003.
[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.
[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing,
[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.
[6] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia,
15(2), 316−325, 2013.
[7] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding
for General Distortion Metrics and Its Applications," IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.
[8] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video
Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778,
2007.
[9] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.
[10] X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013
[11] X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters,

18(4), pp. 255−258, 2011.
[12] W. Hong, T.-S.Chen, and H.-Y. Wu, “An Improved Reversible Data Hiding in Encrypted Images Using Side Match,” IEEE Signal Processing Letters, 19(4), pp. 199−202, 2012.
[13] J. Yu, G. Zhu, X. Li, and J. Yang, “An Improved Algorithm for Reversible Data Hiding in Encrypted Image,” Proceeding of the 11th International Workshop on Digital-Forensics Watermark (IWDW 2012), Shanghai, China, Oct. 31-Nov. 02, 2012, Lecture Notes in Computer Science, 7809, pp. 358-367, 2013.
[14] W. Puech, M. Chaumont, and O. Strauss, “A Reversible Data Hiding Method for Encrypted
Images,” Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, Proc. SPIE, 6819, 2008.