DATA HIDING IN ENCRYPTED IMAGE AND CRYPTOGRAPHY

SURYA V[1], KAVYA MONISHA K[2], AISHWARYA D[3]

[1]Assistant professor, Dept. of Computer Science Engineering, SRMIST college, Tamil Nadu, India
[2]Student, Dept. of Computer Science Engineering, SRMIST college, Tamil Nadu, India
[3]Student, Dept. of Computer Science Engineering, SRMIST college, Tamil Nadu, India

---***---

Abstract - Data hiding is a technique used in hiding the data in cover media. Protection of data is very much necessary nowadays which is used for private transmission, video reconnaissance, and military and clinical field applications. Data can be hidden with compression and encryption. Data hiding is the process in which additional message has been covered with a way so unique spread substance can be reestablished impeccably and can be separated from the picture. In this paper we propose a process called Cryptography in which Homomorphic encryption algorithm and Cipher text policy attribute based encryption algorithm have been used. Encryption is the process through which data is encoded so that it is inaccessible to unauthorized users. It is the process of making plain data like a message and hiding the original data. Homomorphic algorithm helps in the Conversion of data into cipher text. It also allows the complex mathematical operations to be performed on encrypted data. Cipher text policy attribute based encryption algorithm ensures that if some attribute is revoked, then the cipher text like this attribute will be updated in order that only the individuals whose attributes meet the access control policy. By this data will be revoked and will be ready to perform the key updating and decrypt the cipher text successfully. Both the client and the recipient share a solitary key. The client utilizes this key to scramble plain content and send the encoded content to the collector. On the opposite side the collector applies a similar key to unscramble the information. It ensures the data privacy and higher standards of data security.

***Key Words*: Cryptography, Data privacy, Data hiding, Encryption, Decryption, Cipher text.**

1.INTRODUCTION

Data hiding is a process for hiding information or messages from unauthorized or unauthenticated users to access, view, modify, or delete the particular information. Data Hiding in Encrypted Image and Cryptography (DHEIC) is a system used for hiding data, especially data in the form of text which is shared in an outsourced environment. The data which is shared in an outsourced environment or cloud environment from a sender to a targeted receiver is first encoded into an image and then the data is sent to the targeted receiver in the form of encoded image. The receiver decodes the encoded image to view the data. The DHEIC (Data Hiding in Encrypted image and Cryptography) system mainly uses two encryption algorithms to encode and decode the data. The two main algorithms are Homomorphic encryption algorithm and Ciphertext-policy Attribute-based encryption algorithm.

2. EXISTING SYSTEM

Reversible information stowing away in scrambled pictures utilizes multi-mystery sharing as the fundamental encryption, which brings an explode issue of the key size. It has been presented for information installing and for saving picture security. Picture supplier, information hider and beneficiary are the three gatherings which are included by RDHEI. Offer free mystery key (SIK), Share no mystery key (SNK) and shared one key (SOK) are the three classes which are included on the security with key setting. No mystery key is partaken in SNK, while in SIK, the picture supplier and information hider is separately offering the mystery keys to the beneficiary. RDHEI address shared one key (SOK) setting, where the picture supplier imparts the mystery key to the beneficiary and information hider implants a mystery message with no information on the key.

SOK helps in indicating adequacy, proficiency, and security by testing and examining it. Mystery sharing fills in as the crude contribution security, different mystery jelly size unpredictability and inalienably added substance homomorphism understands the information inserting. The technique gives formal portrayal and present an unmistakable idea which is called as expansion homomorphism in multi mystery sharing.The calculation utilized in this framework is lightweight cryptography calculation. Lightweight cryptography is a class of cryptography that gives security answers for asset compelled gadgets. RDHEI utilizes two strategies from lightweight cryptographic calculation.

Moreover, this system has the following drawbacks

- It has complicated algebra structures.

- Large embedding distortions.
- Recover the cover image only for small data.
- May result in incorrect extraction, when block size is small.
- High computational cost.

3. PROPOSED SYSTEM

The Data Hiding in Encrypted Image and Cryptography is initiated for protecting data against the access of unauthorized users and to protect the data confidentially. The main functionality of the Data Hiding in Encrypted Image and Cryptography is to secure the data transmitted by the sender confidentially to the targeted receiver by encrypting and decrypting the data. The DHEIC system uses the stenography to encrypt the data. The DHEIC system implies two main algorithms The Homomorphic Encryption algorithm and The Ciphertext-policy Attribute-based encryption algorithm. The Data Hiding in Encrypted Image and Cryptography system is built using Python. The embeds the data that has to be encrypted into an image .This process is done by first converting the text data into string. The strings are then concatenated. The keywords are selected from the concatenated string. An Image is selected and uploaded to embed the data for encryption. The messages are converted to bits. The image is also converted to bits. Then the system checks if the message can be embedded into the image by checking the size of the image. The size of the image is checked by using this formula.

Image_max_size = H*W*C*2.

H= Img.shape[0].

W= Img.shape[1].

C= Img.shape[2].

If the message can fits into the image. The data is embedded into the image by using the Homomorphic Encryption algorithm and the Ciphertext-policy Attribute-based encryption algorithm.

The Homomorphic encryption algorithm is used to compute specific type of computations on cipher texts. This algorithm obtains an encoded result. Applying a common encryption method leads to deadlock. If the data is stored unencrypted, the data can expose delicate information to the storage service provider. On the other side if the data is encrypted,it is impossible for the provider to work on it. Homomorphic encryption is also an enticing feature in contemprory communication system structure. The Homomorphic encryption allows binding different services together without revealing the data to each of those services.

The encrypted data is stored in a server. Therefore if the data stored in a server is compromised. The confidentiallity of the data is also compromised. To solve this we use Ciphertext-policy attribute-based Encryption. Ciphertext-policy Attribute- based Encryption is a technique used to keep the encrypted data confidentially even if the data stored sever is untrusted. This method is also secure against collusion attack. The party encryption determines who should decrypt the data.

Fig 1. Rebel alliance

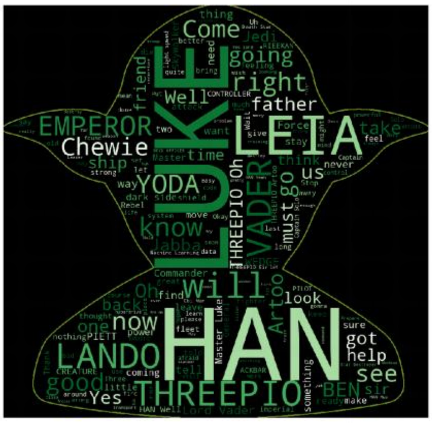


Fig 2. Wordcloud

4. MODULES

The Data Hiding In Encrypted Image and Cryptography comprises of three main modules.

i. Preprocessing.

ii. Feature selection.

iii. Data Encoding and Decoding.

i) PREPROCESSING:

Fourier transform is a keen tool for image processing. The Fourier transformer tool is utilized to dissolve the image into its cosine and sine components. The product of this fourier conversion shows the image in the frequency domain where the input image is spatial domain equivalent. Throughout this process of image acquisition or during transmission noises are produced. Therefore noise removal is done in this process. Noises in the image can be classified as impulse noise, Gaussian noise, and speckle noise.

ii) FEATURE SELECTION:

Feature selection is the process of selecting the best feature among all the features that are used to segregate classes. FSA model is computational algorithm.

iii) DATA ENCODING AND DECODING:

The data hiding process is used for embedding the information into the cover media for the intent of privacy. Cover image is one of the best media to fount information. This produce huge scope for covering private data that emerge into Stego-Image subtle to human view, unique stenographic access depending on information hiding approach such as pixel- value discriminating. This process implements both huge embedding scope and phenomenal subtle for the stego-image.

5. ARCHITECTURAL DESIGN OF DATA HIDING IN ENCRYPTED IMAGE AND CRYPTOGRAPHY

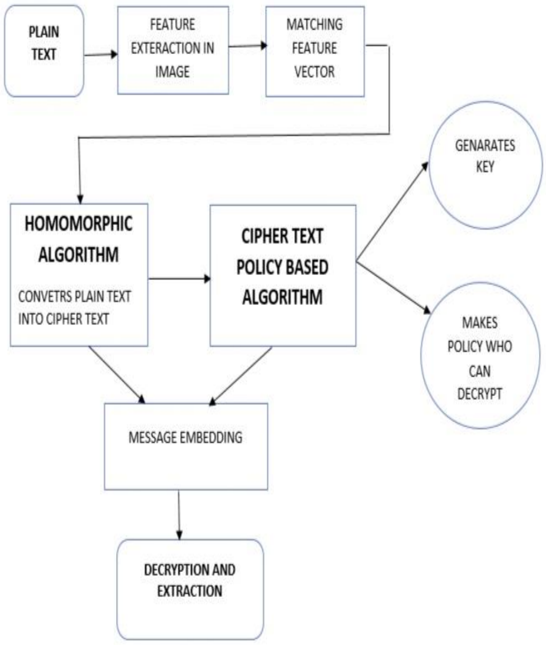

PLAIN TEXT
FEATURE EXTERACTION IN IMAGE
MATCHING FEATURE VECTOR
GENARATES KEY
HOMOMORPHIC ALGORITHM
CONVETRS PLAIN TEXT INTO CIPHER TEXT
CIPHER TEXT POLICY BASED ALGORITHM
MAKES POLICY WHO CAN DECRYPT
MESSAGE EMBEDDING
DECRYPTION AND EXTRACTION

Fig 3.System Architecture

6. SOFTWARE DESCRIPTION

Python:

Python is a mediator, object-arranged, significant level programming language with dynamic semantics. Its raised level inborn data structures, got together with unique creating and dynamic authority, make it amazingly charming for RAD(Rapid Application Development), similarly concerning use as a paste or scripting language to relate existing parts together. Python's clear, easy to learn accentuation underscores clarity and thusly decreases the cost of program upkeep. Python reinforces groups and modules, which supports code reuse and program estimated quality. The Python interpreter and the wide standard library are available in source and twofold structure without charge for each and every noteworthy stage, & can be energetically appropriated.

NumPy:

In the world of python we have so many module, one such module is Numpy. It is a module which is alternate for mat lab. It is mainly used for two important use case with respect to python. Numpy is used to create multi-dimensional array. Also used for perform all the mathematical functions. Basically, numpy has so many predefined mathematical functions which can be reused.

Eclipse:

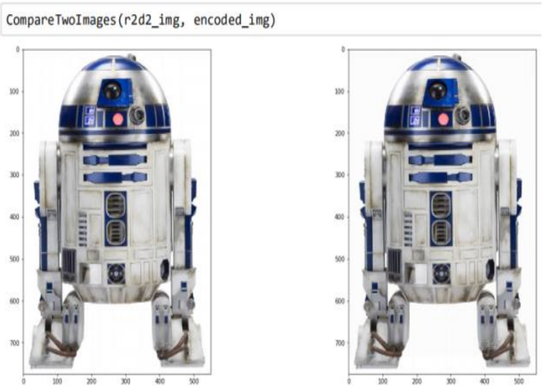
Eclipse is a joined improvement condition used in PC programming. It contains an extensible module system for changing the earth and a base workspace . Eclipse gives an average (UI) model for working with contraptions. It is planned to run on various working structures while giving solid coordination each shrouded OS.

Anaconda:

Anaconda is unbound and open-source.It has over than 1.5k Python packages Anaconda facilitate package deployment and management. Anaconda has mechanism to effortlessly gather information from origin using AI. It develops an environment that is effortlessly manageable for fixing any project. Anaconda is that the industry standard for creating, training and testing on a machine. It has best community support.

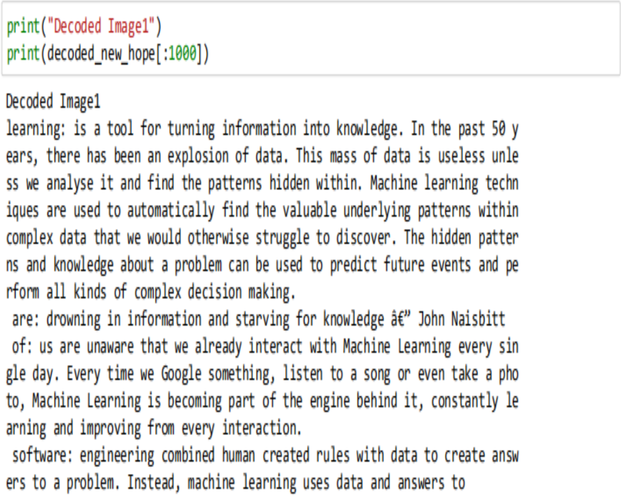
7. EXPERIMENTAL RESULT ANALYSIS

In this study, algorithm of homomorphic encryption and Ciphertext-policy Attribute based encryption algorithm has been used to encrypt the data that has to be transmitted from the sender to the targeted receiver. The result of the system ensures that the data is secure without the access of unauthorized users. The proposed model ensures the message embedded and hidden into the cover content is recovered without any data loss. The hidden message is decrypted without losing the quality of the content. The framework additionally intends to accomplish adaptable administrations more than a large number of scrambled pictures, we plan a safe and productive list structure, which empowers down to earth and exact social disclosure from the cloud, without uncovering any picture profile or picture content. The system also scrambles the cover image used for embedding data. Thus the system checks that both the cover content and the data embedded is regenerated perfectly. Our examination shows the security of the structure, and the execution shows a little stockpiling overhead and correspondence overhead for both portable customers and cloud servers.The decoded cover content is compared for completeness.The compared decoded image and the decoded content is attached below as screenshot.



```
CompareTwoImages(r2d2_img, encoded_img)
```

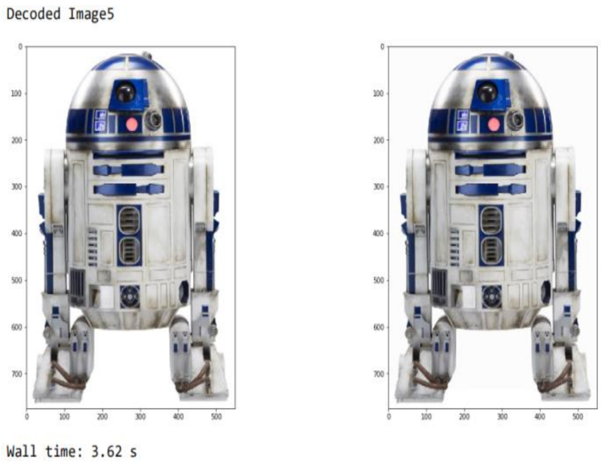
Fig 4. Encoded image



```
print("Decoded Image1")
print(decoded_new_hope[:1000])
```

```
Decoded Image1
learning: is a tool for turning information into knowledge. In the past 50 y
ears, there has been an explosion of data. This mass of data is useless unle
ss we analyse it and find the patterns hidden within. Machine learning techn
iques are used to automatically find the valuable underlying patterns within
complex data that we would otherwise struggle to discover. The hidden patter
ns and knowledge about a problem can be used to predict future events and pe
rform all kinds of complex decision making.
 are: drowning in information and starving for knowledge â€” John Naisbitt
 of: us are unaware that we already interact with Machine Learning every sin
gle day. Every time we Google something, listen to a song or even take a pho
to, Machine Learning is becoming part of the engine behind it, constantly le
arning and improving from every interaction.
 software: engineering combined human created rules with data to create answ
ers to a problem. Instead, machine learning uses data and answers to
```

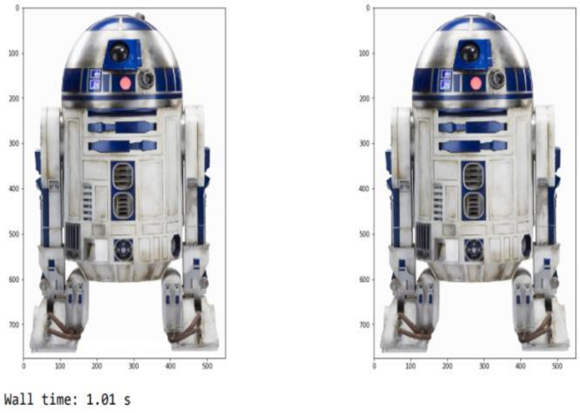
Fig 5. Decrypted message



```
Decoded Image5
```

```
Wall time: 3.62 s
```

Fig 6. Decoded Image



```
Wall time: 1.01 s
```

Fig 7. Scrambled image

8. CONCLUSION

The proposed security scheme for Data Hiding in Encrypted Image and Cryptography provides confidentiallity against unauthorized users and malware. In this paper, we present a new class of data hiding in encrypted image and cryptography using Homomorphic Encryption and Ciphertext-Policy Attribute-based encryption. The systems achieves in embedding data into digital images using stenography.The embedded data is computized in its encrypted form without decrypting the data into plain text. The data confidentiallity is achieved in this system using ciphertext-Policy Attribute-Based Encryption. By ensuring that the user holding the given set of attribute can access or decrypt the data.

REFERENCES

1. J. Bernarding, A. Thiel, and A. Grzesik, "A JAVA-based DICOM server with integration of clinical findings and

DICOM-conform data encrytion," International Journal of Medical Informatics 64, pp. 429–438, 2001.

2. R. Norcen, M. Podesser, A. Pommer, H. Schmidt, and A. Uhl, "Confidential Storage and Transmission of Medical Image Data," Computers in Biology and Medicine 33, pp. 277–292, 2003.

3. A. Uhl and A. Pommer, Image and Video Encryption: From Digital Rights Management to Secured Personal Communication, Springer, 2005.

4. K. Chung and L. Chang, "Large encrypting binary images with higher security," Pattern Recognition Let-ters 19, pp. 461–468, 1998.

5. C. Chang, M. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," The Journal of Systems and Software 58, pp. 83–91, 2001.

6. A. Sinha and K. Singh, "A technique for image encryption using digital signature," Optics Communica-tions 218, pp. 229–234, 2003.

7.A.Eskicioglu and E.Delp, "An Overview of Multimedia Content Protection in Consumer Electronics devices," Signal Processing: Image Communication 16(7), pp. 681–699, 2001.

8.F.Y. Shih and S. Y. Wu, "Combinational image watermarking in the spatial and frequency domains,"Pattern Recognition 36, pp. 969–975, 2003.