IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 4, April 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

Secret Sharing Based Reversible Data Hiding Using AES128-Bit Key Algorithm

F. Mary Harin Fernandez[1], Fathima shifana N[2], Pavithra J[3], Sivashree S[4]

Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai, TamilNadu, India[1]

Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai, TamilNadu, India[2]

Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai, TamilNadu, India[3]

Student, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Chennai, TamilNadu, India[4]

ABSTRACT: In the existing system a reversible data hiding method is used in encrypting the images with single data hider for sharing secret data. If the data hider gets damaged the original image cannot be reconstructed or recovered. To overcome this issue, a novel model is proposed. The proposed system is based on secret sharing of data with multiple data hiders for RDH-EI using SOK. It stores the text information in the watermarked image and sends to the data embedder for data hiding. To get the corresponding marked encrypted image each data hider embed data into the encrypted image independently. Here we address shared one key (SOK), where the sender only can share a secret key with the receiver at the time of registration. The data (secret message) is embedded and hidden by the data hider without the knowledge of secret key. Here we use AES 128-bit key algorithm, so that the data hider can embed and hide large amount of text inside the watermarked image. A light-weight encryption technique is used to reduce the key size issues. To preserve the key size efficiency a light-weight cryptographic algorithm is used. By experiments and analysis, the proposed technique shows the effectiveness, efficiency and security with the support of SOK scheme.

KEYWORDS: Secret sharing, Watermarking, Shared one key, Data Embedding, Image encryption, Reversible data hiding.

I. INTRODUCTION

Reversible data hiding(RDH) permits the extra data to be embedded and converts secret message into cover media like confidential military and medical images. RDH performs a reversible procedure that extracts the secret message that was hidden in the image encryption process and reconstructs the first cover content perfectly. Numerous reversible data hiding methods are introduced before 20 years. Difference expansion and histogram shifting are the two seminal ideas of RDH. In difference expansion method to release a replacement LSB(Least Significant Bit) plane, the difference between the two adjacent pixels are doubled for the key message to be carried.The zero and peak points want to embed the key message by modifying the pixel values slightly by using histogram shifting method. For the enhancement of two concepts, payload and image quality has been elaborated by many RDH studies. Recently RDH-EI (RDH over an encrypted image)has been introduced as a replacement of RDH. And regarding owner privacy the subsequent real-life scenario is captured, that is referred as image privacy.

Within the middle of workflow there is an inferior assistant or a channel administrator who is permitted to insert some additional data like authentication data, image notations or origin information within the encrypted image, where the present party doesn't know the first image content. For preserving the patient'sprivacy, the medical images are encrypted and a couple of data is embedded into the corresponding encrypted images only by the database administrator. It must guarantee that the content is often reconstructed perfectly after decryption and extraction of the key message by the receiver to ensure the consistency of medical image.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

Image processing method can extract some useful information or an enhanced image by performing or processing some operations on the image. It is a kind of signal processing in which the input is a image and the output is also an image or features related to that image. Image processing is one of the rapidly growing technologies in the current days. Within engineering and also in computing disciplines it forms a core research area.

Image processing has three subsequent steps:

- Image acquisition tools are used to import the image.
- The image is analyzed and manipulated
- Result are often altered image or report that supports image analysis during output.
- Analogue and digital image processing are the two sorts of method used for the image processing. For the hard copies like images and printouts, Analogue image processing is used often. The various fundamentals of interpretation are used by the image analysts while using visual techniques.

While using computers for the manipulation of digital images, the digital image processing technique is used. There are three general phases in which each one sorts the data. While using the digital technique the data needs to undergo pre-processing, image enhancement, display and the information extraction is done.

Encryption of image are often defined in such how that it's the method of encoding secret image with theassistance of some encryption algorithm in such how that unauthorized users can't access it. An image is often encrypted in the same way the software encrypted the text. AES128-bit key algorithm is a sequence of mathematical operations is used on the binary data which comprises a picture and during a predictable way, values of the numbers are changed by the encryption software.

In digital image watermarking, a multimedia product is used to embed the watermarked data and later the data is extracted from the watermarked product. Verification of the content, authentication, tamper-resistance and image integration is ensured by these methods. Invisible modification of the smallest amount significant bits within the file are often the opposite way of digital watermarking. Least significant bits are modified during a unique pattern and it's not visible. Layering visible symbol on the highest of the image may be a method for digital watermarking. Watermarking is that the process of superimposing a logo or piece of text atop a document or image file, and it's a crucial process when it involves both the copyright protection and marketing of digital works.

Image that has to be recovered perfectly after the marked image exactly extracted the embedded message, it is permitted by the technique of reversible data hiding. Over the last 20 years, the popularity has been gained by the RDH techniques. In Reversible data hiding the first message is often restored from the image where the data is embedded. The histogram modification of image that embed the data by using height point within the image that is supported by earlier works in RDH.

II. LITERATURE REVIEW

The proposal of [9] introduces a technique to minimize additive distortion in steganography using non-binary embedding process. The total distortion is set to sum of per-element distortions. The sender with payload-limited and the sender with distortion-limited are involved. Decomposition of non-binary case takes place and individual bits are replaced in the cover elements. The Viterbi algorithm (to equip dual convolution codes) based syndrome coding scheme is used for binary case. The system is used to achieve state-of-the-art result and are reported for more relative set of payloads and for different profiles which is distorted. [4] proposes steganography while minimizing function which is distorted. It is defined in a complex model space sufficiently. For simple attacks the immunity is not automatically guaranteed even in high-dimensional cover model. Even a cover model which is incomplete can be compromised with security if the distortion is optimized in it. [3] proposes the hiding of occurrences of communication as the main part of steganography.

In today's world invisible methods are used and the statistical irregularities are revealed during mathematical analysis. These variances show that the hidden communication is taking place.[6]proposes distortion which is universal and estimate the cost of modifying an image element from residuals (directional) acquired by using Daubechies wavelet filter bank. The perception is to restrict the changes during embedding process only to those parts that are difficult to model in various directions while evading smooth and clean edges. The demonstration of utility is constructed by using spatial scheme and compare the security.[8] purposes machine learning tool-based ensemble classifier which scales

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

much more complementary. The lower training complexity come up with the probability to work with models and train the sets. The ensemble classification is illustrated and the power of suggested framework is exemplified based on the method that lock-up the message in the image.

RELATED WORK

The existing system of reversible data hiding works on two different models: traditional model and secret sharing model. Both models have a data owner, a single data hider and receiver to perform the encryption of image, data hiding process, extraction of data and recovery of image respectively. The system uses an encryption key and a hiding key which is stored in a database or a key management system. The capacity to embed for this type is restricted and the distortion on watermarked image is intense.

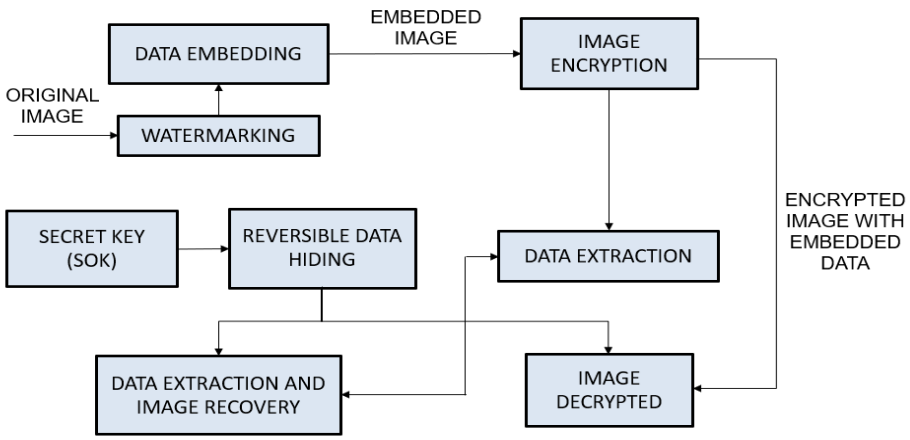
The limitations of existing system are:

- The existing model using reversible data hiding with encrypted image involves a single data hider. So, if a data hider gets damaged, the original image cannot be recovered.
- Since the encrypted image size is large when generated, expansion of data may occur at the data hider end.
- The storage of keys used for encryption and data hiding may be hacked and used by any external unauthorized person.

III. PROPOSED METHODOLOGY

The proposed model with data hiders for reversible data hiding supported secret sharing method using shared one key store the exact text information to the pictures and sends to data hider for data embedding and hiding. Here multiple data hiders can independently embed data in the watermarked image. The marked encrypted image is then decrypted when receiver uses shared one key obtained at the time of registration. To protect the key size efficiency, a light weight cryptographic method for compression is applied.

The system architecture diagram for the proposed system is shown in the below figure 1; It has 5 phases namely, digital watermarking, data embedding, image encryption, reversible data hiding and extraction of data and image. The original image used for data embedding and hiding is referred as a cover image. The shared one key is used at the time of decryption at the receiver end. If the key is wrong the image decryption is not possible.



PROCEDURE OF PROPOSED SYSTEM

Step 1: Initially the sender and the receiver are registered at the time of registration and each of them login into the system when both the users want to share the secret data.
Step 2: Then the sender chooses an image through which the secret data has to be shared with the receiver. The original image is watermarked with another image using digital watermarking technique and the watermarked image is sent for embedding the data in it.
Step 3: Now the embedded image is sent for image encryption process where we use AES128-bit key algorithm. After encrypting the image, it will create shares based on number of data hiders present.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

Step 4: At the receiver end, a shared one key (SOK) is used to extract the data and to recover the image after decryption.
Step 5: Finally, the image is recovered and the data is extracted with the help of reversible data hiding (RDH)using shared one key concept.

DIGITAL WATERMARKING

This module briefly describes about the watermarking process of the Original image. First the sender and the receiver must register themselves to share and receive data. Then, it takes the original image in which data has to be embedded and the image with which the original image has to be watermarked. These two images undergo digital watermarking which is visible. The Digital watermarking is done so that the authority of the digital media is intact and prevents copying of the data. The figure 2 shows the procedure of digital watermarking process.

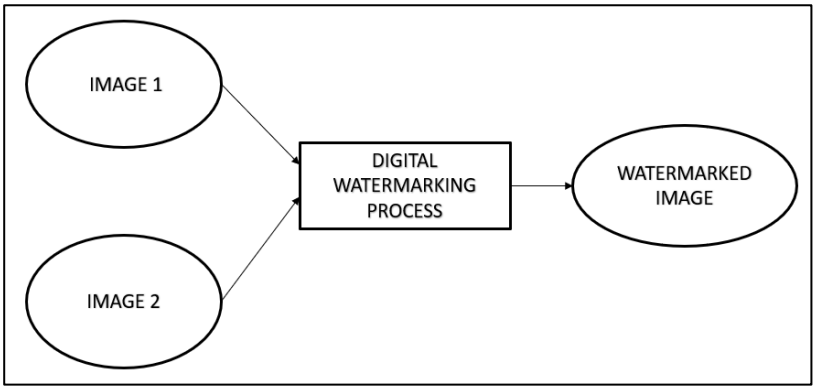


Figure 2: Digital watermarking

DATA EMBEDDING

The process of embedding data in the image for sharing secret data is called as data embedding. This technique uses even-odd embedding method. The sender embeds the piece of data to be shared with the receiver without involving any hiding keys. The watermarked image and the secret data are given as input for data embedding and a marked image with data hidden is gained as output. The process involved in data embedding is shown in the below figure 3.

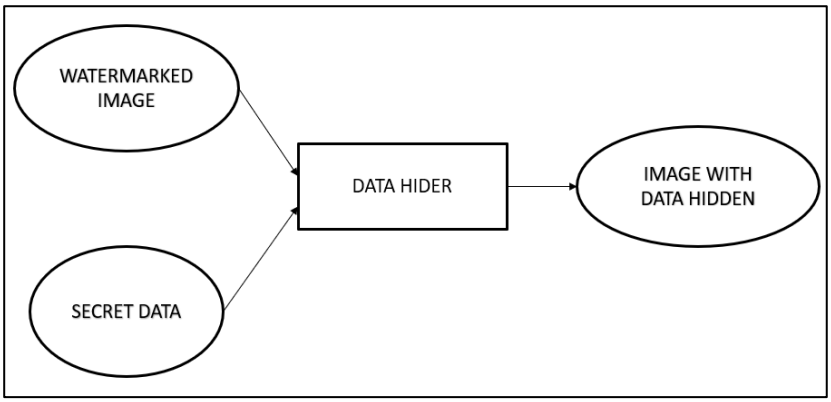


Figure 3: Data Embedding

Here the Even-Odd embedding technique is used which involves two phases. In phase 1, the secret data is embedded in the pixels of odd values and in phase 2, the secret data is embedded in the pixels of even values.

IMAGE ENCRYPTION

The encryption of image is done by using a visual cryptographic algorithm where the image is coverted into streams of data array and then encrypted. There is no encryption key used or stored anywhere ad thus eliminates the key storage

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

and unauthorized access of intruders. The marked image with data hidden is given as input. Then AES 128-bit key algorithm is applied to increase the embedding capacity of large amount of data in the image. Finally, a marked encrypted image with embedded data is gained as output. The process involved in image encryption is shown in the below figure 4. encrypt the image. So first the image is converting into streams of data array.

ALGORITHM

Here we use a symmetric block cipher which is Advanced Encryption Standard (AES) Algorithm. The image of block size 128 bits is processed using three different cipher key size of lengths 128, 192 or 256 bits. The number of execution round is based on the key size length (10, 12 or 14 respectively). The system uses block size of 128 bits and key size of 128 bits. Since the key size is of 128 bits it will take 10 rounds of execution.

STEP 1: To encrypt the image with data an 8-byte initialization vector is created.

byte[] iv = new byte[] with values below

{ 0x00, 0x01, 0x02, 0x03, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };

STEP 2: Two instances of cipher namely, ecipher and dcipher for encryption purpose is created. Here AES/CBC/PKCS5 Padding is currently used for encrypting image with 128-bit key size.

ecipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

dcipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

STEP 3: Cipher Block Chaining (CBC) requires an initialization vector which acts as a mode of operation for block cipher. A buffer is used to transport the bytes from one stream to another.

byte[] buf = new byte[1024]

STEP 4: The image to be encrypted is selected and then converted to bytes. The bytes to out will be encrypted and is named as Encrypted.png.

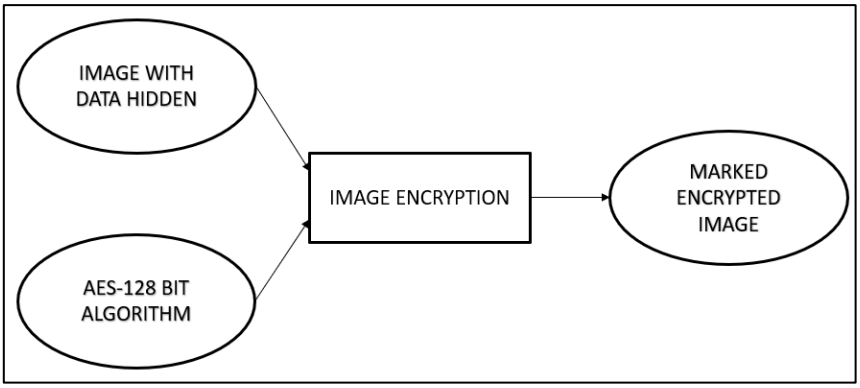


Figure 4: Image Encryption

REVERSIBLE DATA HIDING

The process in which the stego image can be regained or reversed to the original image is known as reversible data hiding. The marked encrypted image is sent as an input for reversible data hiding process. The processing takes place to remove the water marking. Finally, the image with the data hidden is obtained as an output. The figure 5 shows the procedure involved in reversible data hiding.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

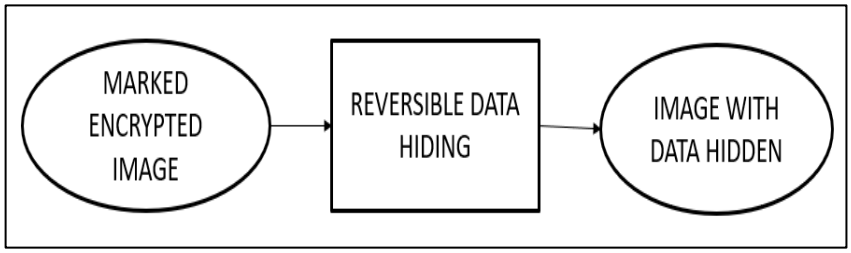


Figure 5: Reversible Data Hiding at receiver end

EXTRACTING DATA FROM ENCRYPTED IMAGE

To obtain the final result a secret key called as shared one key(SOK) is used. It is a 16-bit personal key for every authorized user with which the data is extracted from the previous output gained. The receiver can extract the data without key is not possible and is not a public key. This key is received by the receiver at the time of registration. It extracts the secret data sent by the sender and thus the image is recovered. The figure 6 shows the procedure involved in image decryption and data extraction.

ALGORITHM

The reverse process of encryption is AES decryption process. The process takes the encrypted image as the input and the decryption is done with the help of shared one key (SOK). The encrypted image is in unreadable format. After the application of AES decryption algorithm, the original image is recovered.

STEP 1: The image to be decrypted is selected and fed to the decrypter class and after decryption the image is stored in Decrypted.png.

STEP 2: For time being a secret key is assumed and used.

```
String key Value="TheBestSecretKey";
Key key = new SecretKeySpec(keyValue.getBytes(), "AES");
```

STEP 3: The key is converted to bytes and the AES decryption process takes place by sending to the method for which the instance is created.

```
c = Cipher.getInstance(ALGO);
c.init(Cipher.DECRYPT_MODE, key);
```

STEP 4: The image after decryption is gained and then with the help of secret key the extraction of information is done.

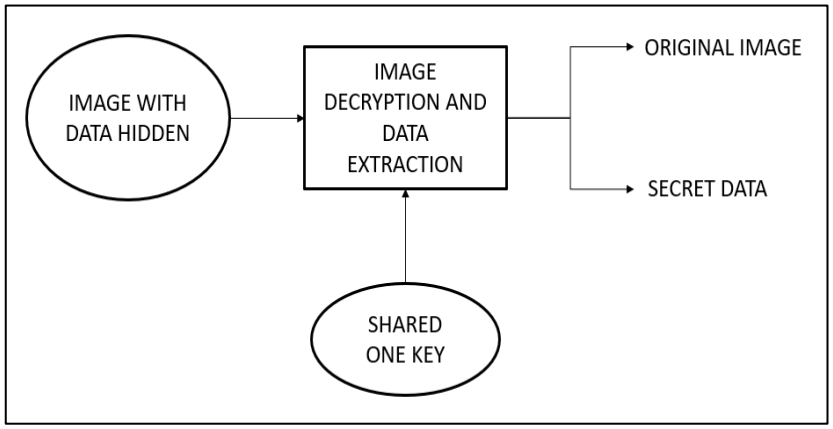


Figure 6: Extraction of data from encrypted image

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

IV. EXPERIMENTAL RESULTS

Initially, the user registration is done for secret sharing. It is required to login as a confidential person. A light-weight cryptographic method is used for embedding large amount of data in the image. The secret key used for image decryption is not stored anywhere. Instead, the encrypted image is alone stored in the database. This concept has resulted in elimination of key and hiding of large amount of data. The figures 7, 8 and 9 shows the processing of input and how the output is obtained at the receiver end after decryption.

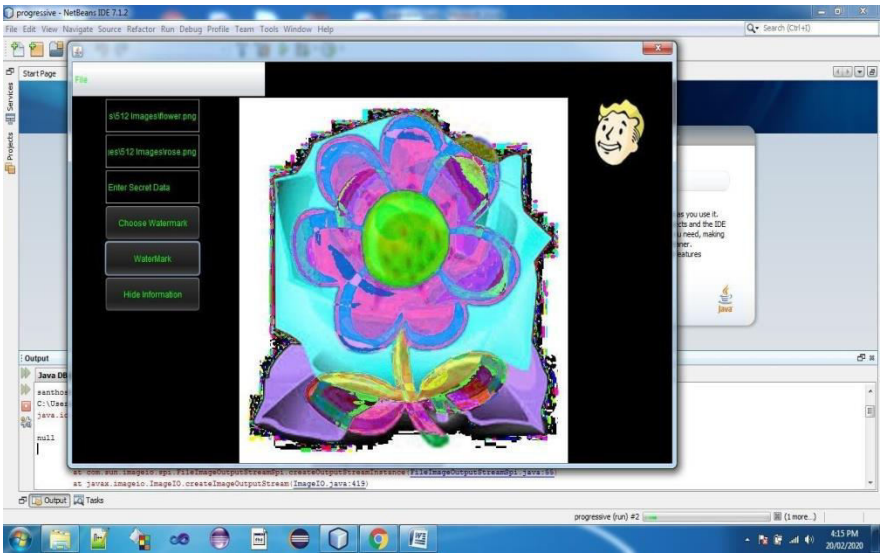


Figure 7: Watermarked image

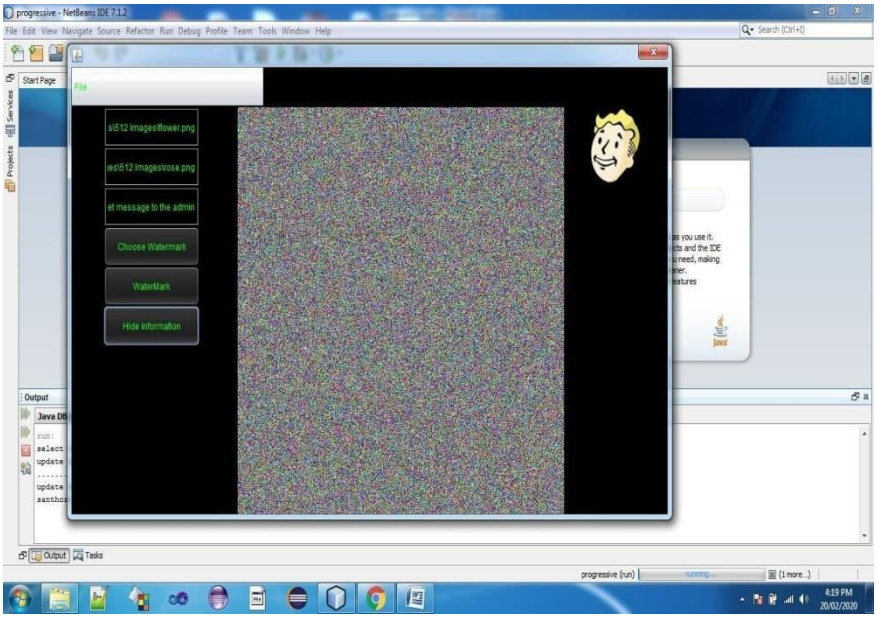


Figure 8: Image Encryption

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004156

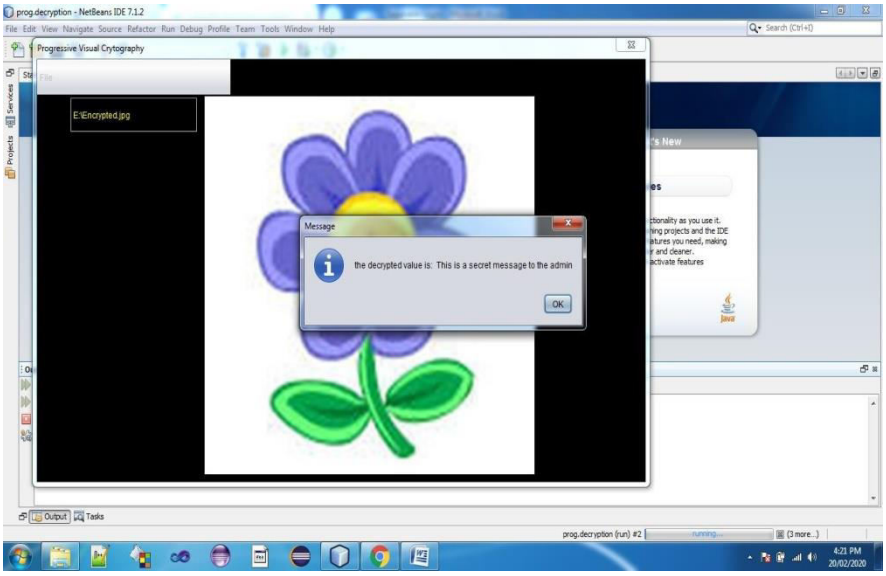


Figure 9: Output after data extraction

V. CONCLUSION

The novel concept of RDH-EI using shared one key is presented. The AES 128-bit key algorithm is used to increase the embedding capacity of data in the image, whether a word or paragraph or pages. The secret key (SOK) is used to extract the data and recover the image from the receiver side which eliminates key storage. This system is extremely useful for few applications like military and medical field which needs secure way to share information.

REFERENCES

[1] BingChen,WeiLu,JiwuHuang,JianWeng,Yicong Zhou, "Secretsharing based reversible data hiding in encrypted images with multiple data hiders", IEEE Transaction on Dependable and Secure computing, DOI 10.1109/TDSC.2020.3011923, Aug2020.

[2] Khan, A. Siddiqa, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," Inf.Sci.,vol.279,pp.251–272,Sep. 2014.

[3] Diljith M. Thodi, Jeffrey J. Rodriguez, " Expansion embedding techniques for reversible watermarking ", IEEE Transactions on Image Processing, Volume: 16, Issue: 3, March2007.

[4] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.16, no. 3, pp. 354–362, Mar. 2006.

[5] X. Li, B. Li, B. Yang, and T. Zeng, "General framework to histogram shifting-based reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 6, pp. 2181–2191, Jun.2013.

[6] Dinu Coltuc, Jean-Marc Chassery, "Very fast watermarking by reversible contrast mapping", IEEE Signal Processing Letters, Volume: 14, Issue: 4, April2007.

[7] J. Lee, Y. Chiou, and J. Guo, "Reversible data hiding based on histogram modification ofSMVQindices," IEEETrans.Inf.ForensicsSecur.,vol.5, no. 4, pp. 638–648, Apr.2010.

[8] Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam, Sundaram Suresh,Yun Qing Shi, "Reversible watermarking algorithm using sorting and prediction", IEEE Transactions on Circuits and System for Video Technology, Volume: 19, Issue: 7, July2009.

[9] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[10] S. Weng, Y. Zhao, J.-S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixelpairs,"IEEE Signal Process.Lett., vol. 15, pp. 721–724,2008.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details