Indian J.Sci.Res. 17(2): 625-628, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

CONCEALING MESSAGE IN IMAGE AND ENCRYPTING USING AES

[1]P. PreethiMadhav, [2]Chandrashekhar Reddy,[3]K. Vidya
[1]Department of Computer Sceince and Engineering, Aurora's Engineering College, Bhongir, Hyderabad, India.

***Abstract*-**Steganography is a process of hiding data that means some sort of information in the form of images like pictures which tends to secure the secret information from hack of the data. It uses the distortion techniques, such as primary distortion method for a given message that is hidden with UED rule, which, does not make us to modify randomly, it embed the information uniformly to separate all potential magnitudes. In this process, it gives us less hacking ability that reduces the changes of the computations for separate transformations. Here the image obtains effectiveness and stego analyzers allow us to make any modifications to the image. In this method, it uses Advanced Encryption Standard (AES) algorithm to encrypt the data that is being projected to the user and it maintains the secrecy of the information that is hidden in an image using distortion mechanisms.

***Keywords*:**Steganography, UED rule, AES algorithm.

I. Introduction

Steganography is a process of hiding message into an image file or video file with some part of secret key for the duration of this assignment, a brand new distortion perform is given to at ease JPEG Steganography.[1-2]

It incorporates the distortion technique, the marginal distortion for a given message is embedding with a distortion algorithmic rule that spreads the information uniformly, which, rather than creating random modification, it spreads the embedding information uniformly to amount separate ripple remodel coefficients of all potential magnitudes. During this approach, less applied mathematics notice ability is achieved, that owes to the reduction of the changes of the statistics for DWT coefficients are completed [3].

II. System Model

A. Existing System:

Inside the existing system additional attention is paid to reversible statistics pastime (RDH) in encrypted photographs, because it continues the fantastic assets that the primary cover can be lossless.All earlier strategies engraft information by removing the area from the encrypted pictures, which can cause some errors on the image.In previous technique before encoding the area is empty from the image, then the receiver cannot get the image.[4-5]

B. Proposed System:

The method we implemented, in proposed system is as follows.

- During this method, we tend to apply RDH method on simple photos to cover the image and it achieves high-quality overall performance even as no longer lack of the secrecy.
- This method can do actual changeableness, separate facts extraction and greatly development on the usual of marked decrypted pix.
- We can come thru actual changeableness, that is, facts extraction and image restoration area unit free of any error.

a)Analysis

We have analyzed our model by Windows 7 and JDK 1.7. The following points will describe the designed complete module:

b)Reversible data hiding:

Reversible information concealing extra ordinarily | is incredibly helpful for a few extremely image such like medical pictures and military pictures. Within the reversible information concealing schemes, some schemes area unit sensible performance at concealing capability however have a foul stego image quality, some schemes location unit sensible stego photograph first-class but have a espresso concealing functionality. it is tough to are looking for out the balance among the concealing functionality and stego picture best. for the duration of this paper, a completely unique reversible statistics concealing subject is projected. The projected theme uses a replacement embedding technique that is named Even-Odd embedding technique, to stay the stego image quality in an appropriate level.

- **Image Encryption:**

Here we have a tendency to use visual cryptography rule for cipher the image. Thus initial the image is changing into streams {of information-ofknowledge|--of information} array and every data are going to be encrypted.

[1]Corresponding Author

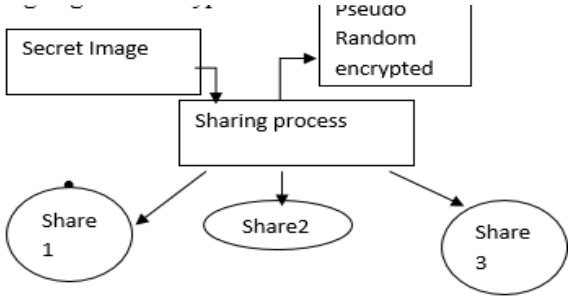

Fig.1: Image encryption

- **Data Embedding:**

This module describes concerning the embedding the info for secret sharing. It takes one random encrypted image. Watermark affords the identity of the supplier. Here we have a propensity to use LSB rule for records embedding. Earlier than facts concealing we have a tendency to initial cipher the information victimization mystery key.

The embedding technique of watermark is given as follows

a) Count on that the scale of the host image is 512×512. Host image is split into tiny M×M blocks Z, block Z is split into tiny M ×M blocks Y. If M=8 is employed, the dimensions of block Y is 8×8.

b) Variety of pairs of coefficients (A,B) in block Y area unit chosen as A = a1, . . . , an, B = b1. . . bn

c) For embedding, 2 constant values (ai, bi) area unit changed by add parameter that could be a parameter for watermark strength. i=1,…, n.

- **Data Protection:**

Image retrieval is computationally intensive and may get pleasure from offloading to save lots of energy. we have a tendency to contemplate 2 retrieval algorithms: Image request and Dennis Gabor filtering, and 2 protection schemes: Steganography and homomorphy coding. Steganography uses a canopy image to disguise the key image so it's tough to observe. a straightforward and usually used image Steganography technique is concealing pictures by substitution bits from the duvet image with bits from the key image. coding transforms plain information to form them illegible. Steganography is completely different from encryption: the previous hides the existence of information. In distinction, coding makes the info mindless while not the key. ImgSeek is performed on Steganography information as supported the linear property of feature extraction. homomorphy coding is employed in Dennis Gabor retrieval, as a result of Dennis Gabor filtering largely performs additions and multiplications on encrypted information.

- **Extracting Data from Encrypted Images:**

To manage and update personal info of pictures that area unit encrypted for shielding clients' privacy, Associate in nursing inferior info manager might solely get admission to the datainformationthe records concealing key and want to control information in encrypted domain. The order of facts extraction earlier than photo cryptography guarantees the feasibleness of our upload this case. Once the factstheinformationrecordsbase supervisor gets the data concealing key, he will rewrite the LSB-planes of and extract the more statistics by using immediately reading the decrypted model. as soon as asking for exchange data of encrypted snap shots, the data manager, then, updates info thru LSB alternative and encrypts updated information consistent with the info concealing key everywhere another time. Because the whole method is totally operated on encrypted area, it avoids the leak of unique content material.

- **Extracting statistics from Decrypted pix:**

In Case, every embedding and extraction of the information vicinity unit manipulated in encrypted area. On the opposite hand, there's a special state of affairs that the user needs to rewrite the image initial and extracts the info from the decrypted image once it's required. the subsequent example is Associate in Nursing application for such state of affairs. Cloud server and time stamps, to manage the encrypted pictures. Note that the cloud server has no right to try to any permanent harm to the photographs. Currently a licensed user, Bob United Nations agency has been shared the coding key and also the information concealing key, downloaded and decrypted the photographs. Bob hoped to induce marked decrypted pictures, i.e., decrypted pictures still together with the notation, which may be accustomed trace the supply and history of the info. The order of image cryptography before/without information extraction is absolutely appropriate for this case.

- **Reversible Data Hiding:**

Reversible knowledge concealment pictures could be a technique, by that the first cowl are often lossless recovered when the embedded message is extracted.

Images secret writing is a good and in style suggests that because it converts the first and significant content to incomprehensible one. Though few RDH techniques in encrypted pictures are revealed however, there are some promising applications if RDH are often applied to encrypted pictures. Obviously, the cloud service supplier has no right to introduce permanent distortion throughout knowledge coloring into encrypted knowledge. Thus, a reversible knowledge coloring technique supported encrypted knowledge is most popular. Suppose a medical image information is keep in a very knowledge center, associated a server within the knowledge center will implant notations into an encrypted On the opposite hand,

a doctor, having the science key, will rewrite and restore the image in a very reversible manner for the aim of additional diagnosis.

- **Image Encryption:**

With a stream cipher, the secret writing version of is well obtained. Maybe, a grey worth starting from zero to 255 are often delineated by eight bits, , specified The encrypted bits are often calculated through exclusive- or operation wherever is generated via a customary stream cipher determined by the secret writing key. Finally, we have a tendency to implant ten bits info into LSBs of 1st ten pixels in encrypted version of to inform knowledge hider range|theamount|the quantity} of rows and therefore the number of bit-planes he will implant info into. Note that when image secret writing, the information hider or a 3rd party cannot access the content of original image while not the secret writing key, so privacy of the content owner being protected.

- **Data hiding in Image:**

Since has been rearranged to the highest of , it's easy for {the data|theinfo|the info} hider to browse ten bits information in LSBs of 1st ten encrypted pixels. The market bit-planes with further data. Finally, the information hider sets a label following to illustrate the tip position of embedding method and additional encrypts in keeping with the information concealment key to formulate marked encrypted image denoted by. Anyone United Nations agency doesn't possess {the knowledge|theinfo|the information. Figure 2 describes the architecture of the designed module.

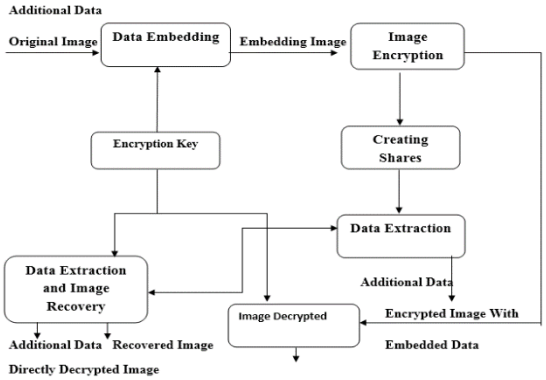

Fig.2: Proposed Architecture For Extracting Data And Image

III. RESULT AND IMPLEMENTATION

The projected work provides information integrity mistreatment hash rule MD5. Wehave a tendency to produce message digest that's sent on encrypted information. This digest is hidden in image. At receiver aspect, receiver initial get information from image, decode it and so realize message digest mistreatment same rule and match with original message digest.

A.PROPOSED ALGORITHM

The projected image cryptography formula has 2 major steps. Firstly, realize the place wherever the message is to be embedded and Second, the embedding formula.

Step 1:

1. Divide the quilt image into blocks.
2. Now median is found for every block.
3. Calculate the root value for the above value.

S=fix (sqrt(M))

4. Calculate the distinction worth for every 2 consecutive pixels Pi and Pi+1.

Di=Pi-Pi+1

5. If Di&grt; =S then insert the message in Pi.

(Go to step 2)

Step 2: Embedding algorithmic program

1. Split every constituent Pi into 2 equal elements.
2. Create the smallest amount important four bits of the constituent to zeros.
3. Split the Message into 2 equal elements.
4. Make the first 4 bits to zero.
5. Nowbitxor is made on the above two results.

V.Conclusion

A remarkable circumstance for distinct reversible mastery movement in encoded picture is arranged, that incorporates photograph cryptography, learning installing and measurements extraction/picture-reclamation stages. Inside the underlying angle, the substance material proprietor scrambles the underlying uncompressed picture exploitation A cryptography key. in spite of the fact that a data hider does never again comprehend the underlying substance material, he will pack the littlest sum basic bits of the scrambled photo the utilization of an understanding-concealing key to make a conveyed region to house the more noteworthy measurements. With A scrambled picture containing moreover aptitude, the beneficiary may perhaps remove the more noteworthy know-how exploitation absolutely the insights concealing key, or assemble a photograph simply like the underlying one exploitation completely the cryptography key. Once the beneficiary has each of the keys, he will remove the similarlygreater data and recuperate the underlying substance with none missteps with the asset of misusing the spatial connection

in normal picture if the wide assortment of extra know-how isn't overlarge.If the lossless pressure procedure is utilized for the encoded picture containing implanted comprehension, the more noteworthy ability will be all things considered separated moreover the first substance could be furthermore recouped since the lossless pressure would not revision the substance of the scrambled photograph containing installed know-how. Be that as it may, the loss of pressure strategy similarly invested with scrambled pictures produced through detail change isn't appropriate ideal here on the grounds that the cryptography is performed by methods for bit-XOR operation. Inside the future, a thorough blend of photo cryptography and aptitude side interest very much coordinated with loss of pressure merits additional examination.

Acknowledgment

The author wishes to thanks to the Principal and Head (R&D cell) of Aurora's Engineering College Bhongir to support us to do the same.

References

[1] T. Kalker and F.M.Willems, "Capacity bounds and code constructionsfor reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing(DSP2002)*, 2002, pp. 71–76.

[2] W. Zhang, B. Chen, and N. Yu, "Improving various reversible datahiding schemes via optimal codes for binary covers," *IEEE Trans.Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

[3] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEETrans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques forreversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3,pp. 721–730, Mar. 2007.

[5] K. Hwang and D. Li, "Trusted cloud computing with secure resourcesand data coloring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22,Sep./Oct. 2010.