International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Effective Data Hiding Mechanism Based on Encrypted Image in a Discrete Wavelet Zone of a Carrier Image

[1] Prof. Aniket K. Shahade [2] Miss. Priyanka V. Deshmukh [3] Prof. V. S. Mahalle
[1] Department of Information Technology [2][3] Department of Computer Science and Engineering
[1][2][3] Shri Sant Gajanan Maharaj College Of Engineering, Shegaon, Maharashtra, India
[1] aniket.shahade11@gmail.com [2] priyanka8deshmukh@gmail.com [3] vsmahalle@gmail.com

***Abstract*— Now a day's to keep up secrecy and confidentiality of an information could be a vivacious field with 2 totally different approaches being followed, the primary being encrypting the pictures through cryptography algorithms victimization keys, the opposite approach involves concealing knowledge victimization data concealing algorithmic program to keep up the pictures secrecy.**

A content owner use cryptography key to perform the cryptography of original pictures, and employing a information hiding key a data hider will plant further data into the encrypted image although he doesn't recognize the first content, because the encrypted image contains some further information, with the assistance of cryptography key a receiver 1st decipher it then extract the embedded information and recover the first image in line with the data-hiding key.

***Keywords*— Cowl image, Knowledge concealing, Knowledge extraction, Image secret writing, Image decoding, Knowledge recovery, DWT.**

I. INTRODUCTION

Cryptography may be a technique for securing the key data that we tend to transferring from one purpose to a different. In cryptography sender encrypts the message exploitation the key and so sends it to the receiver. When receiving from the sender the receiver decrypts the message to urge the key information. The most focus of cryptography is on keeping the content of the message secret wherever as knowledge activity concentrates on keeping the existence of the message secret [1]. For secured communication the opposite technique is knowledge activity. Knowledge activity involves activity data therefore it seems that no data is hidden in the slightest degree. If associate someone views the article that is hidden inside he or she's going to don't have any concept that there's any hidden information, in order that it's terribly troublesome for person conceive to decipher the data

[2]. Knowledge activity is image has several applications, particularly in today's fashionable, hi-tech world. Privacy and secrecy may be a concern for many individuals on the web. Hidden image permits for 2 parties to speak in secret and covertly.

The strength of information activity gets amplified if it combines with the cryptography. In knowledge activity, the terminologies used are cover-image, hidden image, secret message, and secret key and embedding algorithmic program. Cover-image is that the carrier of the message likes audio file, video or image. Cover-image carrying the embedded secret knowledge is that the hidden image. Secret message is that the data that's to be hidden during a cowl image. The key secret is a costumed plants the message reckoning on the activity algorithmic program [2]. The embedding algorithmic program is that the manner, that is employed to plant the key data within the cover image.

The securities of the transformation of hidden knowledge are often obtained by 2 ways: Cryptography and Knowledge activity. Mixes of the 2 technique are often accustomed increase the information security. Cryptography may be a technique during which the message is modified in such the way in order that no knowledge are often disclosed if it's received by associate wrong doer. Whereas in knowledge activity, the key message is embedded into a picture usually known as cowl image, and so sent to the receiver who extracts the key message from the quilt message. Once the key message is

embedded into cowl image then it is known as a hidden image [6]. The visibility of this image shouldn't be distinguishable from the quilt image, in order that for wrongdoer it nearly becomes not possible to find any embedded message.

Here we have a tendency to work the info concealment technique that is reversible in nature. Therefore it's termed as Reversible information hiding technique. In severable reversible information hiding technique first of all a content owner encrypts the first uncompressed image then an information hider compress the image to create house to accommodate some further information. Reversible information concealment could be a technique to engraft further message into some distortion-unacceptable cowl media, such as military or medical pictures, with a reversible manner in order that the original cowl content is utterly renovated once extraction of the hidden message. As a good and common means for privacy protection, cryptography contains encryption and decryption. It converts the standard signal into incomprehensible information, in order that the final signal processing generally takes place before cryptography or once decryption.

II. LITERATURE REVIEW

Fridrich et al. (2001) [3], planned the reversible knowledge embedding technique for the authentication purpose that the embedding capability of this technique is low. Zhang empty out house for knowledge embedding within the plan of press encrypted pictures, to filter out the info extraction from image cryptography [4], [5]. An encrypted binary image may be compressed with a lossless manner by finding the syndromes of low-density parity-check codes, a lossless compression technique for encrypted grey image victimization progressive decomposition and rate compatible pierced turbo codes is developed in [4]. W. Liu, W. Zeng, the loss compression technique given in [5]. An encrypted grey image may be expeditiously compressed by discarding the overly rough and fine data of coefficients generated from orthogonal remodel. A receiver might reconstruct the principal content of original image by retrieving the values of coefficients, once we get the compressed knowledge. The computation of remodel within the encrypted domain has additionally been studied X. Zhang [8]. W. Liu, W. Zeng planned, once we transmit the encrypted secret knowledge, a channel supplier with none data of the cryptanalytic key might tend to compress the encrypted knowledge attributable to the restricted channel resource, a lossless compression technique for encrypted grey image victimization progressive decompose and rate compatible turbo codes is developed in [5].

The method in [6] compressed the encrypted LSBs to vacate space for added knowledge by finding syndromes of a parity-check matrix, and therefore the data that is employed at the receiver facet is that the special correlation of decrypted pictures. A completely unique technique for RDH in encrypted pictures, that we tend to don't "vacate space when encryption" as drained [7], however "reserve space before encryption". In ways of [6]–[7], the encrypted 8-bit gray-scale pictures are generated by encrypting each bit-planes with a stream cipher.

III. ANALYSIS OF PROBLEM

Now a day, a brand new challenge consists to insert knowledge in encrypted pictures, because the entropy of encrypted image is largest, the embedding step like noise isn't potential by victimization common place knowledge concealing algorithms. New plan is to use reversible knowledge concealing algorithms on encrypted pictures by desire to get rid of the embedded knowledge before the image cryptography. There is each other downside if either concealing key or cryptography key's leaked then welcome person will extract or rewrite the image through data concealing key or rewrite the image through cryptography key.

Another downside found is that, the key use for encrypting the image and knowledge concealing is same. That the user who is aware of the key use for cryptography will access the embedded knowledge and original knowledge. We are able to retrieve the first image from encrypted image when extraction or removing the info hidden within the image. The content owner and knowledge hider share constant cryptography key for cryptography of image and knowledge concealing. Up to this, there is no provision of selecting the key and additional encoded code time consumption. There is various knowledge concealing programs on the market. A number are glorious in each respect sadly, several of them lack usable interfaces, or contain several bugs, or inconvenience of a program for alternative operative systems.

IV. PRAPOSED WORK

Data concealing provides straight forward approach of implementing the strategies. The most purpose behind this is often to supply a economical technique for concealing the info from hackers and sent to the destination firmly. This technique is principally involved with the formula making certain the secure knowledge transfer between the supply and destination. For that we tend to initial used cryptography and so knowledge concealing and vice-versa.

In knowledge concealing we'll use cowl image for security purpose. The medium during which info is to be hidden is termed as cowl image. The key use for encrypting the image and knowledge concealing is same. To resolve that drawback we'll use one secret key for encrypting the image and another secret key for knowledge concealing. A content owner encrypts the first image victimization cryptography key and employing a knowledge-hiding key a data-hider will plant further data into the encrypted image. With an encrypted image containing further knowledge, receiver might initial decode it in keeping with the cryptography key, and so recover the first image in keeping with the knowledge hiding key by extracting the embedded data. Thus, if the each keys area unit completely different then there are a unit sample securities in knowledge transmission.

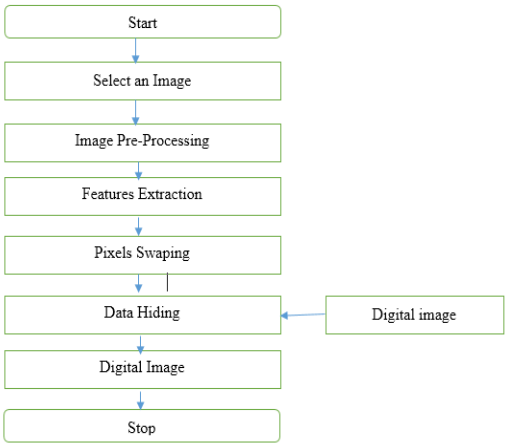

Fig.1. Proposed Data Embedding Flowchart

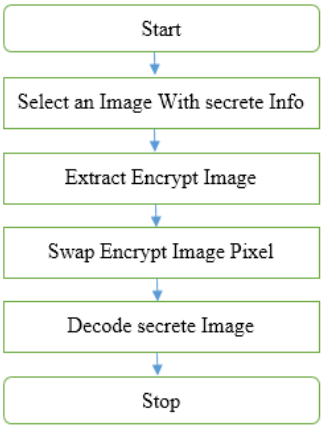

Fig.2. Proposed Data Extraction Flowchart

V. THE PROPOSED ALGORITHMS

A. Feature Extraction Process :

This section 1st describes the feature extraction module that extracts feature pictures from the natural shares. The module which is that the core module of the feature extraction method is applicable to written and digital pictures at the same time. Then, the image preparation and also the pixel-swapping modules are introduced for process written pictures. Assume that the scale of the natural shares and also the secret image area unit w nine h pixels which every natural share is split into variety of b nine, b picture element blocks before feature extraction starts. We tend to outline the notations as follows :

1. b represents the block size.
2. n denotes natural shares.
3. x, y denotes coordinates of pixels in the natural shares and secret image x1.w, y1.h
4. x1,y1 represents coordinates of left top pixel in each block.
5. Φ denotes the value of color code like R,G,B.
6. Pixel value $H_{x,y}$ is the sum of RGB color value of pixel x,y.

B. The Image Preparation and Pixel Swapping Processes :

The image preparation and pixel swapping processes are used for preprocessing written pictures and for post processing the feature matrices that are extracted from the written pictures. The written pictures were handpicked for sharing secret pictures, but the contents of the written pictures should be non heritable by computational devices so be reworked into digital data. The advised flow of the image preparation method is shown in Fig. 3. Within the initiative, the contents of the written pictures are often non heritable by well-liked electronic devices. To scale back the distinction in the content of the non heritable pictures between the encoding and cryptography processes, the kind of the acquisition devices and the parameter settings (e.g. resolution, image size) of the devices ought to be constant or similar in each processes. The next step is to crop the additional pictures. Finally, the photographs are resize in order that they have constant dimensions because the natural shares. An example of the image preparation method is illustrated in Fig. 4.

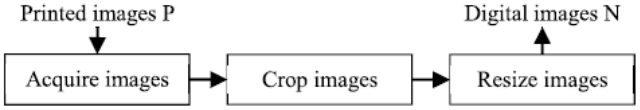

Fig. 3. Flow of the image preparation process

Fig. 4. Example of image preparation method : (a) A hand printed image (b)The resultant picture

C. Encryption/Decryption Algorithms:

The planned theme will code a true color secret image by n-1 innocuous natural shares and one noise like share. For one image, we tend to denote a trifle with an equivalent weighted price within the same color as a trifle plane, then a real color secret image has twenty four bit planes. Thus, the feature pictures and therefore the noise-like share are also extended to twenty four bit planes. Every plane bit of a feature image consists of a binary feature matrix that corresponds to an equivalent bit plane because the secret image. Before cryptography of every bit plane of the key image, the planned algorithmic program initial extracts n-1 feature matrices from n-1 natural shares. Then the bit-plane of the key image like noise share and n-1 feature matrices execute the XOR operation to get the bit plane of the share image. Therefore, to cipher a true color secret image, the cryptography procedure should be performed iteratively on the twenty four bit-planes.

VI. CONCLUSION

Here during this paper, I have planned an honest technique of information concealing in an exceedingly separate ripple zone of carrier image. It contains most utilization of information and conjointly pictures in an exceedingly single carrier image. At the time of decipherment if any of images is corrupted then we will rewrite alternative pictures in same carrier image. It contains maximum utilization of channels and because of this we can hide maximum data at a time.

VII. RESULT

A. Input Printed Image

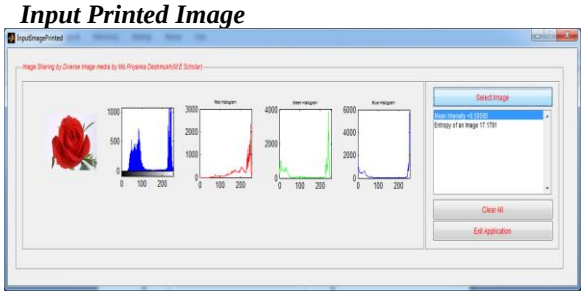

Fig.5. Input Printed Image

B. Input Digital Image

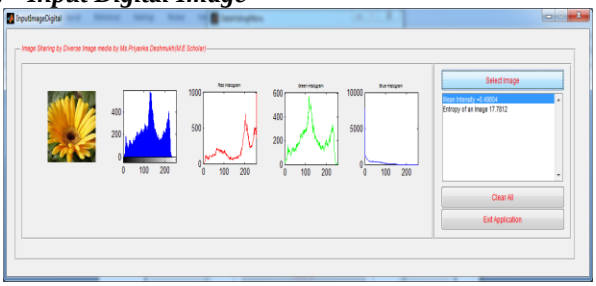

Fig.6. Input Digital Image

After performing all operations on printed image, the resultant extracted original image is:

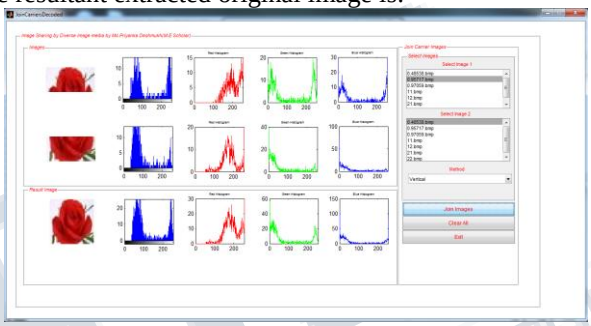

Fig.7. Extracted Original Printed Image

C. Comparison between original Printed image and extracted printed image with respect to Entropy:

Sr. No.	Printed Image	Entropy of Printed Image	Entropy of Recovered Printed Image
1.	Red.jpg	17.1791	17.486
2.	Girl.jpg	17.5022	17.7035
3.	Rose.jpg	17.9348	17.885
4.	Violet.jpg	17.3617	17.1862

Table.1. Comparison with respect to Entropy

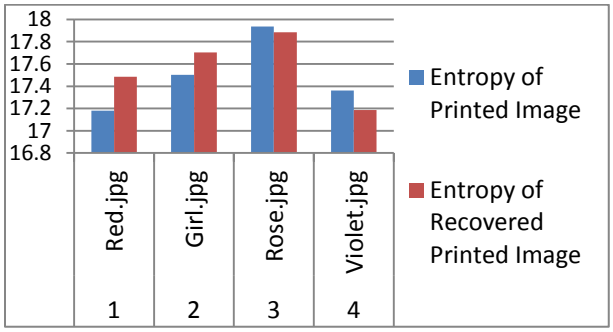

Fig.8. Entropy Graph

REFERENCES

[1] Lini Abraham, Neenu Daniel ," Secure Image Encryption Algorithms: A Review", International Journal of Scientific & Technology Research volume 2, issue 4, April 2013, PP-186 189.

[2] Mohanraj Arumugam and Rabindra Kumar Singh,"Data Hiding and Extraction Using a Novel Reversible Method for Encrypted Image" IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013, PP-1-5.

[3] Kim, H.J., Sachnev, V., Shi, Y.Q., Nam, J., Choo, H.G. 2008. A novel difference expansion transform for reversible data embedding. IEEE Transaction Information Forensics and Security 3 (3), 456–465.

[4] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. SignalProcess.*, vol. 52, no. 10, pp. 2992–3006,Oct. 2004.

[5]W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[6] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[7] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[8] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,pp. 53–58, Feb. 2011.

[9] W. Puech" Image Encryption and Compression for Medical Image Security" PROCEEDING OF IEEE Image Processing Theory, Tools & Applications.

[10] W. Puech, M. Chaumont and O. Strauss "A Reversible Data Hiding Method for Encrypted Images" Author manuscript, published in "IS&T/SPIE Electronic Imaging 2008 - Security, Forensics, Steganography, and Watermarking of Multimedia Contents, San Jose, CA : United States".