IMPLANTING HIGH CAPACITY OF DATA INTO IMAGES USING MASKED LITHOGRAPHY

K. Kamalakannan

Assistant Professor, PG & Research Department of Computer Science, Sun Arts and Science College, Rajapalayam, Tiruvannamalai, Tamilnadu

Abstract:

A new way of technique called embedding high volume of information into images through watermarking by bicolor image into a color image. At this point, a written sign image is encrypted into a color image through this, the sign can be secured in two ways. The first one is starting point to the encoded image, which is depend upon the size of the image and secondly the starting point of the bicolor image will be encoded in the colored image that will be stored in the four byte blocks in the encoded format and these things is done by public key.

The main aim is to encode the bicolor image data's and it is decoded by a private key and then we have to extricate the encoded bicolor image data's from the colored image and this technique needed mastery of the normal colored images for the healing of the written sign image at the receiver point of view. This algorithm reconstructs the original image. Even though the proposed system is embedded in a bicolor written sign image of 80*60 pixels size in the color image of 513*513 pixels. This algorithm furnishes highest degree of strength.

Key Words: Encryption, Image Processing, Watermarking & Lithographic Algorithm.

1. Introduction:

Hiding the data, I may be defined as the process in which a messages signals or by an image is invisible immerse into a host or by getting a composite signals. And the common structure of data hiding is shown in the figure 1.

Our contemplation is to embed information into an image format and this will sustain strike on the untrusted networks. This remarkable issue is to embedding the bytes without generating the visual mortification into a host images. All this process entail in embedding the data by this way it will adjust with the confined feature of an image and next stage we moving on to composite digital image embedding method. This method is proposed to hide an image onto another image; this way provides the best quality of the already recovered image which develops appreciably. To best of our grasp, this one is the first digital embedding method for hiding the data. The proposed method can be applied for a protecting the ownership and authentication of any digitals media. This technique works for a specific purpose to focus on protection and its authenticated of a signature and the design for this method is based on the large scale inquisitive as well as the modeling for the hiding the data process. This embedding rates the report to provide the remarkable meaning for improving the state of art.

2. Literature Survey:

This previous paper is about as the digital age is destroyed and the security's and the protecting the information about the multimedia and to prevent the multiple techniques. We must secure the data's by beating the new schemes for that we have to concentrate in particular techniques.

The process which is embedding the data is called as lithography and this can be visible to the users or not visible to them. In this paper they said that the new techniques that is used to predict the function to create a new lithographic image which

International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

can be much capable and confirmable and fixed to the existed by the protected and detected technique.

And they introduced the new thing to embedding the data's into a binary image and these images will be scanned perfectly and the hand written sign also included over here shambling is applied to the image before they embed and to equalize. The separated the uneven images by part by part's by this the hidden data's can be removed without using the original part of the images and this can be correctly separated by the very high quality of the images by printing it and this can done by with the help of registering the watermarks into it.

The author A. Bartolini and K. Barni were discussed about the issues that how to authenticates the several images. After that they motivated for the watermarking arrangements. And this kind of things must satisfy for certain application. This algorithm is used to visualize the data.

In the year of 2011 Mr. F. Masry's proposed the kind of lithographic algorithm which is designed for the chart image. This algorithm is deals about how to portion the images into similar regions and that will add a several lithographic signals in an image. This part will be resolved using a detector .the synchronized errors can be detected by cropping the images.

In the year 2010, Rehab's and Kidman have dentally explained the procedure that how the edges of a particular images can be detected by using the filters and the second thing is to check the lbs is used in the each and every pixels of an images. The third level deals with connecting the approach with the ASCII coding. This process is used to hide the specific information. This method will embedded by these three methods using digital images.

Yusumk Lim and Deved Dagun Freng in 2011 developed the web application that contains two parts. First one is watermarking system and another one is authenticating the system. In the case of water marking, it will be installed in the system as sever application, that can be accessed by any server and they can produce the own image. This kind distribution can be used in any kind of a networking such as FTP, HTTP. Once the images are distributed to the external users, any client can authenticate the image and verifying it.

Hiding the data in form of paired wised computation is the proposed method can reach the more advantage of reversible and dropping which hides the data can be hosted into an image. And it will not be reduced the optical quality of recovered old images. These works will be done after recovering the hidden data's. All over hiding the data will be obtained randomly.

The hidden data may be recovered faithfully under charge, which compresses the little amount of a specific images and resizing it. The authors found the three things in it 1) limiting the recognize curve when user hides the large amount of data. 2) By using the local standard it will be considered whether to hide the data that causes asynchronous of encoding and decoding. These issues can be resolved muscular and this method is easily implemented which can be correcting the codes that will be durable will overcome with different works. 3) For simpler quantization will be done for hiding the data and the information will be theoretic with the help of some guidelines it will guided. This model provides the scalar quantized technique. And this hiding scheme will combine the many methods in the basis of RSA algorithm and embedding the unseen message.

Debarnath and Chowdhri have been proposed hiding the data with respect to size of an image it should be doubled compare to original image and then the original

value will be updated. This algorithm, an overview of watermarking images into original handwritten image and that original image will be converted into a decided one. The watermarked images will be converted according to the user need and from the original image the data's will be taken. This is new technique for hiding the data.

3. Existing System:

Hiding the data method, where the size of image importer image will be doubled in the source image. It is needed then some extra bytes will be added into image for required size. To do this, the header value must be updated instantly through new value.

In the previous work, I am dealing with the watermarking of a digital image. In this, data can be marked through a host image and this image can be either visible or invisible to the user. This system is sustainable to assaults of altering that image by this data's will be removed if the invader known by the algorithm.

And this system has some drawbacks over it in the digital water marking where the data can be water marked into cloud image this will be either visible or invisible. Thus the system exposed to attacks as altering the image has visible.

3.1 Proposed System:

This embedding high volume of information into images without affecting the key is challenging one. The main problem to hide an image by the signature and it will embedded by another image into it. To get the original image by this experiment the quality of the image will be improved and it will decode at last. The data will be hided through hybrid method through algorithm.
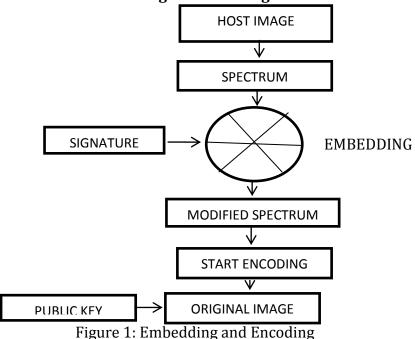
3.2 Advantage of Proposed System:

The advantages of the proposed system are the double folded security of the signature at the source of the embedding is done the starting point will be encrypted using the key method. At the final stage the starting point of the image will be decoded by the encrypted key and it will extract the image using the algorithm.

3.3 Encoding the Image:

The original image is been encoded in the starting point of the image and that image is hidden by the signature by the host image. The dct gets the starting point of an image and inverse it to get the original image with the default pixel value.

3.3.1 Insertion Process of Embedding and Encoding:

Figure 1: Embedding and Encoding

International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

3.3.2 The Discrete Co-Sine Transforms:

The discrete co-sine transform divide the image into many parts according to the importance. And it is similar to discrete Fourier transform and it transform the signals or an image into an three dimensional area.
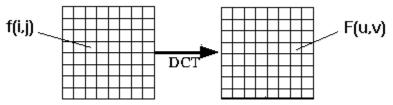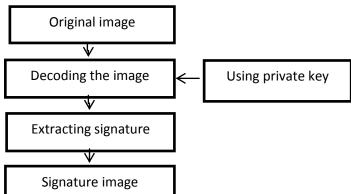

Figure 2: Tranformation

3.3.3 Key Generating Algorithm:

1. First generate the two random prime, that is p and q, it should be equal size and its product is N=pq of a certain bit length
2. Calculate N=pq and pi= (p-1) (q-1)
3. Choose any of the integer number suppose e, 1<e<phi, and gcd should be 1
4. And calculate the secrete exponent that is d that should be less than phi and mod is 1 Ed=1
5. The public key should be (n, e) and the private key is (n, d) now the values are d, p, q, phi keep it has secret value.

4. Decoding the Image:

The decoding is done by extracting the image using signature by an algorithm. And this mainly used for extracting the signature which is handwritten. The signature will be recovered from an original image without any visual filth that image will achieved with the original quality of an image.
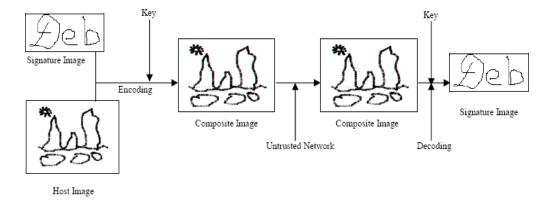

Figure 4: Tested Image

5. Conclusion:

This paper a new method is proposed that is invisible lithography. The image will be extracted and output will be shown in perfect quality and the work of the research is hiding the data which is the new technique.

6. References:

1. Hybrid Digital Embedding Using Invisible Watermarking- IEEE 2008.
2. N.F.Johnson and Sushil Jajodia,"Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol.31, No.2, pp.26-34, feb.1998.
3. D. Kundur and D. Hatzinakos, "Towards a Telltale Watermarking Technique for Tamper Proofing", Proc. ICIP, Chicago, Illinois, Oct 4–7, 1998, vol 2.
4. R. B. Wolfgang and E. J. Delp, "A Watermark for Digital Images", Proc. IEEE Int. Conf. on Image Processing, vol. 3, pp. 219–222, 1996.
5. www.digitalwatermarking.com
6. www.stegnography.com
7. Nedeljko Cvejic and Tapio Seppiinen, "Channel Capacity of High Bit Rate Audio Data Hiding Algorithms in Diverse Transform Domains - 2011
8. Chang-Lung Tsai, Kuo-Chin Fan, Char-Dir Chung and Thoma Chiang Chuang, "Reversible and lossless data hiding with application in digital library", ICME '04. 2004
9. Upamanyu Madhow, B. S. Manjunath and Shivkumar Chandrasekaran, "Robust Image Adaptive Data Hiding Using Erasure and Error Correction", December 2010
10. Wen Chung Kuo, Chin Chih Lin and Jiin Chiou Cheng, "Design a Data Hiding Scheme using RSA
11. Ammar, A. S. S. El-Kabbany M. I. Youssef and A. Emam, "A Novel Data Hiding Using Residue Number System
12. Yongjian Hu and Byeungwoo Jeon, "Reversible Visible Watermarking and Lossless Recovery of Original Images", November, 2009.
13. Debnath Bhattacharyya, Deepsikha Choudhury and Samir Kumar Bandyopadhyay, "Bi-Color Nonlinear Data Embedding and Extraction of Handwritten Signature", IEEE Electro Information Technology Conference, EIT-2007, May 17-20, 2007
14. Debnath Bhattacharyya, Shanta Phani, Poulami Das and Samir Kumar Bandyopadhyay, "Information Hiding Using Enzyme Substrate Watermarking Technique",
15. Debnath Bhattacharyya, Poulami Das and Samir Kumar Bandyopadhyay, "Handwritten Signature Extraction from Watermarked Images using Genetic Crossover".