Literature Survey-Digital Watermarking on Camera Captured Color Images

Ms. Ankita P. Deshmukh, Prof. Dr. S.R.Suralkar
Department of Electronics and Telecommunication
Shram Sadhna Bombay Trust College Of Engineering and Technology ,Jalgaon , India

Abstract: **Digital watermarking provides secured communication. Due to vast expansion of Internet, digital data such as audio, images and videos has been used on a large scale for communication. To protect these digital media it is essential to use digital watermarking for authentication, copyrights and security purposes. This paper gives the detail of digital watermarking concept and the main contribution in the field of steganography. In image Steganography, communication in a coded or secret way is achieved to embed a message into cover image (the original image where the message is embedded) and generate a stenographic-image (image consisting of the embedded message). In this paper analysis has been done on different stenographic.**

Index Terms: **Digital watermarking, stenography, Fragile watermarking, hash function.**

I. INTRODUCTION

A digital watermarking is a bit pattern ,inserted into a digital image files that identifies the file's copyright information (author, rights, etc). Digital Watermarking is done by embedding information in digital data, such that it cannot be detected without special software without the confirmation that the embedded data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/remove it. Digital watermarking has been used to authenticate images and overcome the problems related with the copyright protection. There are two types of watermarking systems; robust and fragile. Robust watermarks are are used to keep in check the illegal copying and is made for the copyright protection. The fragile watermarks is used to detect every possible tampering in the watermarking of the digital media. The main purpose of watermarking is to hide a message in some image, to get new data image. Digital watermarking concentrates mainly on the protection of rights and the authentication of digital media. Similar to stenographic methods, digital watermarking methods hide information in digital media. Steganography is the art of communication such that the presence of a message is not detected. The main purpose of steganography is to hide message in some image, to get new data image in such a way that an unauthorized user cannot detect the presence of message in new data image

II. OBJECTIVES

The main objective of this concept used in the paper is to allow user for a secured communication using digital multi media. It allows user to hide a secret massage which is retrieve by the user at the receiver end. A Fragile watermarking technique is used which helps in detection of tempering. Fragile watermarking is very sensitive to tempering which does not allow the access of secret message even if the image is been slightly tempered. Hash function is used to check if the original file and the received file is identical or different.

III. LITERATURE SURVEY

In [3] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a stego-key. This private stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for color image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

Yang *et al.*, in [4] proposed an adaptive LSB substitution based data hiding method for image. To achieve better visual quality of stego-image it takes care of noise sensitive area for embedding. Proposed method differentiates and takes advantage of normal texture and edges area for embedding. This method analyzes the edges, brightness and texture masking of the cover image to calculate the number of k-bit LSB for secret data embedding. The value of k is high at non-sensitive image region and over sensitive image area k value remain small to balance overall visual quality of image. The LSB's (k) for embedding is computed by the high-order bits of the image. It also utilizes the pixel adjustment method for better stego-image visual quality through LSB substitution method. The overall result shows a good high hidden capacity, but dataset for experimental results are limited; there is not a single image which has many edges with noise region like 'Baboon.tif'.

In [5] anthers have proposed LSB based image hiding method. Common pattern bits (stego-key) are used to hide data. The LSB's of the pixel are modified depending on the (stego-key) pattern bits and the secret message bits. Pattern bits are combination of MxN size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to achieve

security of hidden message in stego-image using a common pattern key. This proposed method has low hidden capacity because single secret bit requires a block of (MxN) pixels.

In [6] author proposed a Pixel value difference (PVD) and simple least significant bits scheme are used to achieve adaptive least significant bits data embedding. In pixel value differencing (PVD) where the size of the hidden data bits can be estimated by difference between the two consecutive pixels in cover image using simple relationship between two pixels. PVD method generally provides a good imperceptibility by calculating the difference of two consecutive pixels which determine the depth of the embedded bits. Proposed method hides large and adaptive k-LSB substitution at edge area of image and PVD for smooth region of image. So in this way the technique provide both larger capacity and high visual quality according to experimental results. This method is complex due to adaptive k generation for substitution of LSB.

In [7] authors proposed a method of Multi-Pixel Differencing (MPD) which used more than two pixel to estimate smoothness of each pixel for data embedding and it calculate sum of difference value of four pixels block. For small difference value it uses the LSB otherwise for high difference value it uses MPD method for data embedding. Strength is its simplicity of algorithm but experimental dataset is too limited.

In [8] author proposed another pixel value differencing method, it used the three pixels for data embedding near the target pixel. It uses simple k-bit LSB method for secret data embedding where number of k-bit is estimated by near three pixels with high difference value. To retain better visual quality and high capacity it simply uses optimal pixel adjustment method on target pixels. Advantage of method is histogram of stego-image and cover-image is almost same, but dataset for experiments are too small.

In [9] authors have introduced a high capacity of hidden data utilizing the LSB and hybrid edge detection scheme. For edge computation two types of canny and fuzzy edges detection method applied and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding. The proposed scheme is tested on limited images dataset. This method is not tested on extensive edges based image like 'Baboob.tif'.

Madhu *et al.*, in [10] proposed an image steganography method, based on LSB substitution and selection of random pixel of required image area. This method is target to improve the security where password is added by LSB of pixels. It generates the random numbers and selects the region of interest where secret message has to be hidden. The strength of method is its security of hidden message in stego-image, but has not considers any type of perceptual transparency.

In [11] proposed an image stenographic method of mapping pixels to alphabetic letters. It maps the 32 letters (26 for English alphabetic and other for special characters) with the pixel values. Five (5) bits are required to represent these 32 letters and authors have generated a table where 4 cases design to represent these 32 letters. According to that table, each letter can be represented in all 4 cases. It utilizes the image 7 MSB (Most Significant Bits) (27 = 128) bits for mapping. Proposed method maps each 4-case from the 7 MSB's of pixel to one of the 32-cases in that table. These 4-cases increase the probability of matching. This algorithm keeps the matching pattern of cover-image which is then used for extracting data from the stego-image. Proposed method does not required any edge or smoothness computations but secret data should be in the form of text or letter for embedding.

In [12], authors have introduced a data hiding technique where it finds out the dark area of the image to hide the data using LSB. It converts it to binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find dark region its connectivity and has not tested on high texture type of image. Its hiding capacity totally depends on texture of image.

Babita *et al.*, in [13] uses 4 LSB of each RGB channel to embed data bits, apply median filtering to enhance the quality of the stego image and then encode the difference of cover and stego image as key data. In decoding phase the stego-image is added with key data to extract the hidden data. It increases the complexity to applying filtering and also has to manage stego-key. Proposed scheme has high secret data hiding capacity.

In [14] author have proposed a pixel indicator technique with variable bits; it chooses one channel among red, green and blue channels and embeds data into variable LSB of chosen channel. Intensity of the pixel decides the variable bits to embed into cover image. The channel selection criteria are sequential and the capacity depends on the cover image channel bits. Proposed method has almost same histogram of cover and stego-image.

Hamid *et al.*, in [15] have proposed a texture based image steganography. The texture analysis technique divides the texture areas into two groups, simple texture area and complex texture area. Simple texture is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method. On the other hand over complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both (2 to 4 LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g PSNR etc.

IV. CONCEPT

Fig.1 shows a simple concept of embedding a message into image using steganography. Firstly the image which is be embedded with the secret message, say the original image in convert into bit stream. Then the message which is to be encoded is converted into a bit stream. This message bit streams is then embedded in the original image to form a data image say the steganography image. This is identical to the original image. The difference in the original image and the stego-image can not be detected with the necked eyes. The detection of the message is the vice-versa process.

Now for the authentication , fragile watermarking is used. Fragile watermarking is destroyed when tempered. Considering this property , fragile watermarking can detect a slight tempering in the original image. This shows that some kind of hacking is tried on the image. And if the image is hacked the secret message cannot be displayed .

Hashing algorithm is used to execute this concept. Hash function is applied on the block of image say the original image and if there is even a small change in the image the hash function will be changed.

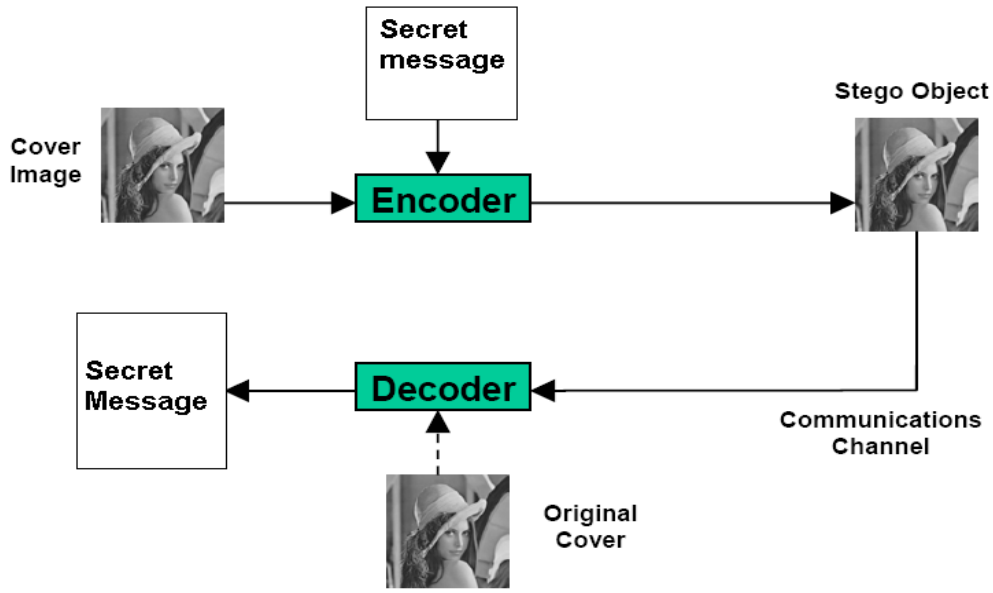

Figure 1: General block diagram of message encoding and decoding

V. CONCLUSION

This paper gives an overview of different stenographic technique which have been proposed in the literature during last few years. We have analyzed the application of fragile watermarking, showing the effective detection of tempering, which helps in the authentication of the image from threats due to unauthorized user.

VI. REFERENCES

[1] Taha. Jassim and Raed Abd-Alhameed, Hussain Al-Ahmad," New Robust and Fragile Watermarking Scheme for Color Images Captured by Mobile Phone Cameras",2013 UKSim 15th International Conference on Computer Modelling and Simulation.

[2] Mehdi Hussain and Mureed Hussain," A Survey of Image Steganography Techniques"

[3] International Journal of Advanced Science and Technology Vol. 54, May, 2013

[4] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, **(2010)** March 1.

[5] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, **(2009)**, pp. 509-516.

[6] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, **(2009)**.

[7] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[8] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[9] H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on **(2009)** May.

[10] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, **(2010)** April 4.

[11] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, **(2010)**.

[12] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol. 5, no. 1, **(2009)**, pp. 33-38.

[13] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, **(2007)**.

[14] B. Ahuja, M. Kaur and M. Rachna, "High Capacity Filter Based Steganography", International Journal of Recent Trends in Engineering, vol. 1, no. 1, **(2009)** May.

[15] M. Tanvir Parvez and A. Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference, **(2008)**, pp. 1322-1327.

[16] M. Hamid and M. L. M. Kiah, "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, **(2009)**.