ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 3, March 2018

A Literature Review on the Framework of Camouflage of RIT with RDH Methods for Plain Text Images towards Better Outsourcing

[1] S.Tamilselvi, [2] R.Sasikala,

[1] M.Phil Scholar, Sankara College of Science and Commerce, Coimbatore. [2]Assistant Professor, Sankara College of Science and Commerce, Coimbatore

Abstract: **- Nowadays there is the very big problem of data hacking into the networking era. There is the number of techniques available to overcome this problem. So, Data hiding is a technique for embedding information into covers such as image, audio, and video files, which can be used for media notation, copyright protection, integrity authentication, covert communication, etc., In this thesis, various existing Data Hiding techniques are studied and reviewed. In this thesis mainly focus on embedding data and restore data with better quality. This thesis discusses Reversible Data Hiding techniques based on Reversible image transformation to embed data and then extract data. The proposed techniques are applied and compared to find which methods are suitable for hiding data into the camouflage image and then losslessly restore the information.**

Keywords**: Reversible Data Hiding, Reversible Image Transformation, Embedding.**

I. INTRODUCTION

In every field they needs some data transfer but very fast and secretly. The requirement of information is highly secure for every field. Nowadays image transmission is a regular process and must find an better way to transmit over the systems. To reduce the communication or transfer time must do the data compression process. To provide security for the multimedia data or image by the Encryption or Data hiding processes. The steps of data compression, encryption and data hiding is very difficult to do in a single step. We have two set of technologies for those purpose. Every encryption processes has some methods for Binary and Grey-level images. The next step of data hiding is secretly embedding data into a image.The secret key used for encryption of compressed image and the data hiding is same. So, the user who knows the secret key used for encryption can access the data embedded and the original data. The original image can be retrieved from the encrypted image after extracting or removing the data hidden in the image. The content owner and the data hider share the same encryption key for the encryption of the image and data hiding. If someone has the data hiding key but not the encryption key he cannot extract any information from the encrypted image containing additional data. Encryption provides security to confidential data. The major two areas stegenography and cryptography provides secure data transmission over internet. Stegenography provides much more security than the security provided by cryptography alone. Cryptography can protect the data during transmission but when it is decrypted, there is no more protection left.

The technique Reversible Data Hiding is established based on the steganography & security. That is the data is embedded in an encrypted image. In the very first step, the image is encrypted using any encryption algorithm. Then the data to be secured is embedded in the encrypted image. With an encrypted image with additional data, if the receiver has the data-hiding key, then he can extract the additional data even though he does not know the image content. If the receiver has the encryption key, then he can decrypt the received data to recover an image similar to the original image, but no able to extract the additional data. If the receiver has both the keys, then he can extract the additional data and also he can recover the original content which is errorless. The data hiding techniques can be done in a lossless or reversible manner. The terms lossless and reversible can be distinguished in different manner. We can say that a data hiding method is lossless if the display of cover image containing embedded data is same as that of original cover even though the cover data have been modified for data embedding.

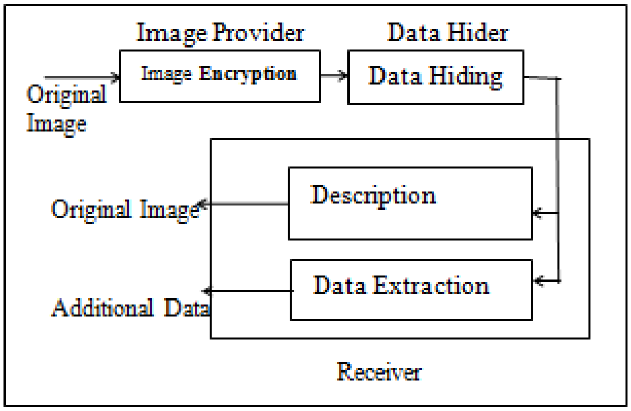

Fig.1 Sketch of lossless data hiding scheme

On the other hand, we can say that a data hiding method is reversible if the original image content can be perfectly recovered from the image version containing embedded data even though a slight distortion has been introduced in data embedding procedure

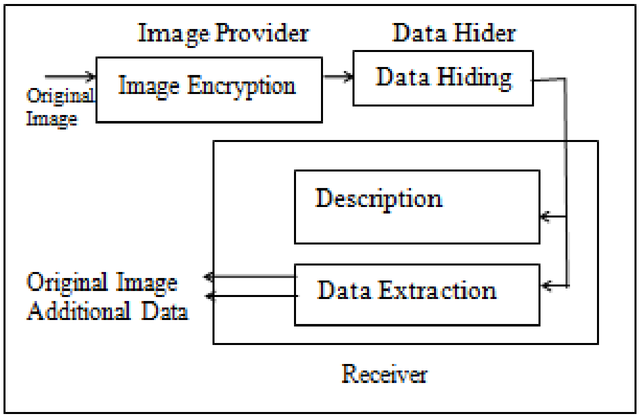

Fig.2 Sketch of reversible data hiding scheme

Both these lossless and reversible data hiding schemes can be combined together to get a more secure and error free data hiding technique .The data embedding process can be done in encrypted domain in both schemes. But the data extraction processes in two schemes are different. Hence by combining these two schemes we can embed two parts of data into a single image. That means the additional data for various purposes may be embedded into an encrypted image, and a part of the additional data can be extracted before decryption and another part can be extracted after decryption.

II. LITERATURE SURVEY

The task of watermarking and extraction has attracted much attention both from security applications designers and from computer vision scientists. It gives a literature survey on state of the art watermarking algorithms. The following research papers focus on variety of issues.

This paper aims to enhance scheme of reversible data hiding (RDH) in encrypted images using Slepian-Wolf source encoding[1] which was inspired by DSC. After the original image is encrypted by the content owner using a stream cipher, the data-hider compresses a series of selected bits taken from the encrypted image to make spare room to accommodate for the secret data. With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. If the receiver has both the embedding and encryption keys, receiver can extract the secret data and perfectly recover the original image. The proposed method achieves a high embedding payload and good image reconstruction quality and avoids the operations of room-reserving by the sender. This research paper enhance invisible image watermarking algorithm based on Singular Value Decomposition (SVD)[2] to prevent the copy or hostilely modification of the products. An effective watermarking algorithm should have certain characteristics such as robustness, security, invisibility, adequate capacity of information etc. In spatial domain watermarks, the pixel value of the image is modified such as LSB while in transform domain the image is first translated using DCT or DWT and then watermark is embedded in any of these transforms. Singular Value Transform (SVD) is an effective numerical analysis tool used for matrices and is used in image processing.

Digital Watermarking technique is becoming more important in the developing society of Internet. It is being used as a key solution to make the data transferring secure from illegal and unauthorized access. In this paper, the two main domains of watermarking have been discussed viz. Spatial (pixel) and Transform (frequency) Domains[3]. In spatial (pixel) domain, the watermark is inserted in the cover image changing pixels or image characteristics. The robustness against unauthorized alteration of a single bit in every consecutive 8-bits of length is enhanced by the incorporation of parity checking. Watermark message is cut into numerous pieces and each piece of message is inserted at different spots, hence, if a piece of message is lost in one spot, the error correct decoding can be employed to possibly retrieve the same information from other spots. Compared to spatial domain, frequency domain techniques are more applied. The objective of this technique is to insert the watermarks in the spectral coefficients of the image. Most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier

Transform (DFT), and Discrete Wavelet Transform (DWT). The Discrete Wavelet Transforms (DWT) and the Discrete Cosine Transforms (DCT). Now days these are being used with the combination of SVD, which altogether provides robustness.

In this research, some of the recent watermarking algorithms have been reviewed and a classification is proposed based on their intrinsic features, inserting methods and extraction forms. Discrete Cosine Transform (DCT) is like Discrete Fourier Transform (DFT) technique used for converting a signal into frequency components. The 2D-DCT of a given matrix gives the frequency coefficient in the form of another matrix. Watermarking with DCT techniques are robust as compared to spatial domain techniques. Such algorithms are robust on image processing operation like low pass filtering, brightness and contrast adjustment, blurring etc. On the other hand Discrete Wavelet Transform (DWT) is a mathematical tool used for decomposing any image. Wavelet transform provides both frequency and spatial description of an image. The wavelet transform decompose the image in four channels (LL, HL, LH and HH) with the same bandwidth thus creating a multi resolution perspective. Due to this advantage the watermark can embed in any of the frequency bands and on inverse transform the watermark will be distributed throughout the low and high frequencies as well as in the spatial domain. Singular Value Decomposition (SVD) is numerical analysis tool in linear algebra, which is being used in many applications of signal processing. It decomposes a matrix with a little error. It is used to provide robustness characteristics to the image. This thesis analyzed the robustness of hybrid digital image watermarking as compared to DCT, DWT, SVD methods watermarking.[4] Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of watermark. Peak Signal to Noise Ratio (PSNR, calculated in dB) which is based on Mean Square Error (MSE) is typically used to calculate imperceptibility. PSNR properties does not take into account image properties such as flat and textured regions. If, the watermark is embedded in textured regions and into edges, the PSNR is inadequate to measure its quality in this case. So, the Weighted PSNR (WPSNR) has been defined as an extension to PSNR. Hybrid watermarking method satisfies all requisites of an ideal watermarking scheme i.e., imperceptibility, robustness and good capacity along with robust against different kind of attacks such as Gaussian noise, salt & pepper attacks, JPEG compression, rotation through an angle etc. The DCT-SVD based method is very time consuming because it offers better capacity and imperceptibility. DWT-SVD method is also similar to DCT-SVD scheme except that the process was fast.

In this thesis, Proposed a novel method for RDH in encrypted images, for that method they do not “vacate room after encryption” as done previously but “reserve room before encryption with a traditional RDH algorithm[5], and thus it is easy for the data hider to reversibly embed data in the encrypted image. The proposed method can achieve real reversibility that is data extraction and image recoveries are error free. First up all they empty out room by embedding LSBs of some pixels into other pixels with a traditional RDH method and then encrypt the image, so the positions of these LSBs in the encrypted image can be used to embed data. Not only the proposed method separate data extraction from image decryption but also achieves excellent performance.

With the widespread use of networks, intellectual properties can be obtained and reproduced easily. This creates a high demand for content protection technique like watermarking, which is one of the most efficient ways to protect the digital properties in recent years. This paper reviews several aspects and techniques about digital watermarking.

The amount of data that can be embedded into audio is considerably low than amount that can be hidden in images, as audio signal has a dimension less than two-dimensional image files. Embedding additional information into audio sequence is a more tedious than images, due to dynamic supremacy of HAS than HVS.

Least Significant Bit Coding:

This simple approach in watermarking audio sequences is to embed watermark data by altering certain LSBs of the digital audio stream with low amplitude.

Phase coding:

The basic idea is to split the original audio stream into blocks and embed the whole watermark data sequence into the phase spectrum of the first block.

Quantization Method:

A scalar quantization scheme quantizes a sample value x and assign new value to the sample x based on the quantized sample value.

This thesis reviews various techniques for watermarking data files like text, image, audio and video. According to the paper, we can conclude that watermarking is a potential approach for protection of ownership rights on digital properties. According to different applications, there are different requirements of the watermarking system. However, it is hard to satisfy all the requirements at the same time. So, benchmark is used to evaluate and compare the performance of different watermarking systems.

Watermarking techniques can be broadly classified into two categories: Spatial and Transform domain methods. Spatial domain methods are less complex and not robust against various attacks as no transform is used in them.

Transform domain methods are robust as compared to spatial domain methods. This is due to the fact that when image is inverse transformed, watermark is distributed irregularly over the image, making the attacker difficult to read or modify. Due to the fact of localization in both spatial and frequency domain, wavelet transform is the most preferable transform among all other transforms.

The proposed method embeds watermark by decomposing the host image by the means of Discrete Wavelet Transform. The watermark used for embedding is a gray scale image. First, the reference image is formed and is used for watermark embedding. Also, we save this reference image for the extraction process. For embedding, SVD is applied on both reference and watermark images and the singular values of reference image is modified with the help of singular values of watermark image. Inverse wavelet transform is performed to reconstruct the watermarked image. The block diagram of the proposed watermarking technique is shown. Original image is not required for the extraction. Reference image is used for the watermark extraction. The objective of this semi blind watermark extraction is to obtain the estimate of the original watermark. For watermark extraction from watermarked image, original image is not required. Hence this extraction is called semi-blind.

III. METHODOLOGY AND PROPOSED WORK

In this proposal system Reverse image Transformation is used to hide an image to another image. In this system both are of same size, the input image and the target image. Here the input image which is to be hidden in a target image an LSB based technique is used. And it is encrypted with the target image. In this RDH-EI techniques the encrypted image is send to the cloud and it embed the data and remove the data whenever the user wants to download. At the user side it get the encrypted image, after decrypting the image the user can get the original image. Restore the original image from the encrypted image in a lossless way. The idea of RIT is exploited for RDH-EI, by which the user can outsource the encrypted image to the cloud in a form of plaintext and thus it will avoid the attention of the curious cloud is irrelevant with both sender and receiver, which is called a client free RDH-EI.

Proposed work is divided into three modules namely:-

- Content Owner,
- Data Hider,
- Receiver.

IV. CONCLUSION

Traditional techniques of reversible data hiding in encrypted image had some limitation, which are unable to protect image content, it can not protect the privacy of data, low hiding capacity and complex computations, clarity of the image will be poor, data compression is not efficient, some problem in the decoding section. Under such demands to overcome this kind of drawbacks proposes a novel framework of Data Hiding in Encrypted Image by Reversible Image Transformation (RIT), which can transform a secret image to a randomly selected target image for getting a encrypted image which is used as the encryption of secret image with good visual quality, and the secret image can be restored without any loss. It can protect the image content. So it is interesting to implement RDH in encrypted images (RDH-EI), by which the cloud server can reversibly embed data into the image but cannot get any knowledge about the image contents. Our further work includes improving the transformation and RDH methods, transmuting the two encrypted image (secret image) into only one target image and extend idea to the video or audio.

REFERENCES

[1] Z. Qian, and X. Zhang, “Reversible data hiding in encrypted image with distributed source encoding,” IEEE Trans. on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636-646, Apr. 2016.

[2] G.Sudheer and G.V. Sridhar, “Implementation of robust watermarking technique using SVD algorithm with GUI representation”, IJARCSMS - 2014.

[3] Y.Shantikumar Singh, B. Pushpa Devi and Kh. Manglem Singh Proposed, “A review of different techniques on Digital Image Watermarking Scheme”, IJER 2013.

[4] Yashovardhan Kelkar, Heena Shaikh and Mohd. Imran Khan Proposed, “Analysis of robustness of hybrid digital image watermarking technique under various attacks”, IJCSMC 2013.

[5] K.Ma, W.Zhang, X.Zhao, N.Yu, F.LI, “Reversible data hiding in encrypted images by reserving room before encryption”, IEEE Trans. On Information Forensics and Security, vol. 8, no. 3, pp. 553-562, Mar 2013.

[6] Baisa L. Gunjal, R.R. Manthalkar, “An Overview of Transform Domain Robust Digital Image Watermarking Algorithms”, Proposed CIS Journal, 2011.

[7] L.Robert and T.shanmugapriya, “A Study on Digital Watermaking Techniques”, Proposed IJRTE, 2009.

[8] G.Bhatnagar and B. Raman, “A new robust reference watermarking scheme based on DWT-SVD”, Proposed Computer Standards Interfaces, 2009.

[9] C. Jain, S. Arora, P. K. Panigrahi, “ A reliable SVD based watermarking scheme.”, Proposed ADSABS 2008.

[10] Amol R. Madane, K T. Talele and M.Shah, “ Watermark Logo in Digital Image using SWT”, Proposed IEEE, 2007.