ISSN XXXX XXXX © 2019 IJESC

Research Article Volume 9 Issue No.4

An Embedded Scheme for Data Hiding in Digital Images

Priyanka. D[1], Prabhakaran. S[2]
PG Scholar[1], Professor[2]
Nandha Engineering College, Erode, India

Abstract:
In this paper we will overview the data hiding techniques in digital images. The RNS based data embedded scheme is proposed, which converts secret information and image cover into residues. Since the residues represent the lowest levels of continues image tone that human eyes are not sensitive. The residues of cover image can be considered as redundancy, which are replaced by the embedded residual data without introducing perceptible distortions. It provides a additional manipulate the encrypted data when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes. A lossless compression method for encrypted gray image using progressive decomposition and rate compatible punctured turbo codes is developed Security with a set of modulus. The proposed scheme exploits by predicting the original pixel the original pixel values on the color channel differences. Secret embedding ownership of data in the contents if digital image is one way to establish and protect ownership of digital image.

Keyword: Residue number system, data hiding, information embedding.

1. INTRODUCTION

Data hiding is a method of hiding secret messages into cover media such that an unintended observer will not aware of the existence of the hidden messages. In this paper, 8-bit gray scale images are selected as the cover-media. These images are called cover-images. Cover –images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to quality of the stego-images. In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some sceneries that a content owner does not trust the processing service provider, the ability to

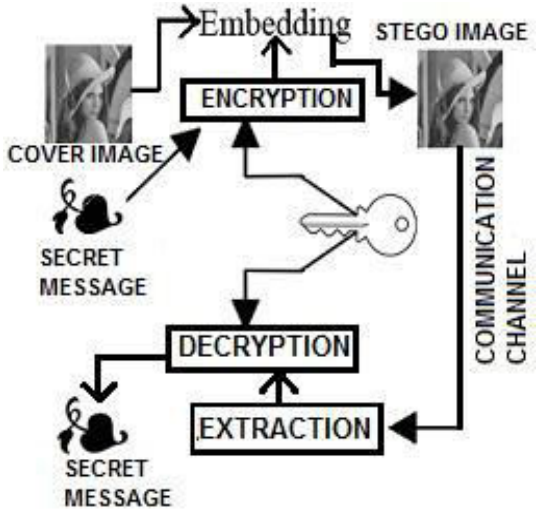

Figure.1. Block diagram of digital image

The popular saying ‘a picture is worth a thousand words’ was certainly true until last decade but, the growing research interests in the field of digital image processing during the last decade have changed this estimation about a picture. Now pictures in their digital representations speak much more than a thousand words, thanks to the digital image data hiding procedures. For example, the block diagram given in figure.1 explains the process of stego-image in which we generally embed some secret message into an innocuous looking simple image (called as the cover image) and create a Stego-image. The Stego-image visually seems to be indifferent from the original cover but hides the secret message inside it and is transmitted to the desired recipients over the communication channels without creating any suspicion in the minds of the intermediately sniffers or/and receivers. When the authorized recipient receives the image, they follow the extraction procedure to retrieve the secret message. To increase the secrecy or security of the hidden message there may some keys involved in this process of embedding and extraction. At the transmission end, during embedding, the message can suitably be encrypted using one or more encryption techniques. These encryption standards can be key based encryptions or non-key based and in key in based techniques, they again can be public or private or a mix. Depending upon the encryption method used during the embedding process, the receiver needs to execute certain decryption algorithms to retrieve the correct message.

2. TYPES OF DATA HIDING TECHNICS

Information hiding techniques are broadly classified into four categories such as, Covert channels, Steganography, Anonymity and Copyright marking [1-5]. The Steganographic procedures can be linguistic or technical whereas the copyright marking procedures can be robust or fragile. Watermarking is a type of robust copyright marking technique which can further be classified as perceptible or imperceptible watermarking. Figure.4 gives a complete classification of various data hiding techniques. A *covert channel* is a type of computer security attack that provides a channel for transfer of in a way that

violates the computer security policy. Robustness and imperceptibility are the important characteristics of a covert channel. *Linguistic Steganography* uses text as the cover media to hide the secret message whereas the *technical covert channels* work by exploiting the loopholes in the OS, network model, protocols etc. *Copyright marking* is a procedure that is used to protect the intellectual properties. In this method a logo or a mark is embedded into a piece of information to show the originality of the work. The copyright can be robust or fragile depending upon the requirement. *Fragile copyright marks* are used to prove manipulations as the fragile marks cannot resist manipulations and lost upon slightest modifications. *Robust copyright methods* are resistant against all sorts of statistical and other types of manipulations.

RDH in encrypted color images

The data encryption stage and the data embedding are presented in section. The decryption stage and the data extraction and original image recovery are discussed below.

2. 1 Encryption stage

We shall further consider color RGB images with L bit planes for each color plane (usually L = 8). The encrypted image is generated by using the standard exclusive-or based stream cipher encryption. Let C 2 fR; G;Bg be a color channel. The bit planes of the corresponding encrypted channel are computed as:

El = Cl _ rl

Where f1; :::;Lg is the current bit plane, is the exclusive-or operator and r is a pseudo random bit stream sequence generated using the encryption key. Note that a distinct r is used for each bit plane and channel (there is no correlation between pixels/channels after encryption). A unique bit stream sequence r should be used with each image in order to ensure the safety of the encrypted content. This is accomplished by either having a distinct encryption key for each image, or more commonly, by generating r by using a fixed key together with some randomly selected pixels/ bit plane values from the current image. These selected bits should not be altered neither by the encryption process, nor by the RDH scheme. The proposed data hiding scheme does not modify the first two LSB planes of the color channels (corresponding to l 2 f1; 2g, but they are encrypted), therefore the required values for computing r will be selected from this two planes and the selected bits will remain unchanged.

2.2 Data embedding stage

The data hider will insert a hidden data bit in a group of n pixel values from an encrypted color channel. He/she must first select between channels: G or RBs. The embedding into G ensures less embedding distortion (requiring a smaller value for n), while the embedding into R and B allows for higher embedding capacities. Next, the bit plane 2g $l \in \{3,...,L-2\}$ that will plane contain the hidden data is chosen. The range $\{3,...,L-2\}$g was selected because the first two LSB planes are used by the encryption scheme and the embedding into the MSB planes introduces unacceptable distortion. The selected channels are then split into the α, and β pixel sets. Only the α and β sets will contain hidden data. The pixels in set are kept unchanged and will be used to predict the values of the host pixels from α and β. Set _ is the first to be processed by the embedding scheme. A data hiding key is used to randomly distribute the pixel from _ into n pixel groups. The first groups of G will be used for embedding additional information: a 64 bit watermark identifier, the channels used for data hiding and the number of hidden bits. This additional information is necessary at the detection stage. The payload is hidden into the selected channels, one bit per group, either into the remaining groups of G, or into the ones of R and B. Both methods from [8] can be used for embedding. The selection of the method depends on the requirements for the hidden data. Thus, the separate method allows for the hidden data to be read and modified from the encrypted image, but the image can only be restored after decryption. For the joint method, the hidden data can be real and extracted from the decrypted host image.

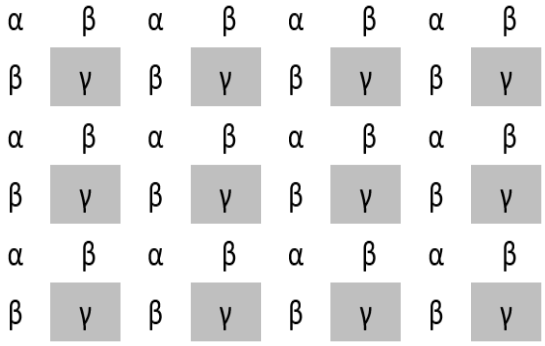

Figure.2. Distribution of pixels

If the required embedding capacity is not entirely provided by set _, the embedding process is repeated for set _. If the R channel was selected as host, then the embedding process can continue with the pixel values in B as well.

2.3 Decryption stage

The encryption key is used together with the selected LSB image values to generate the original r bit sequence used to encrypt the image. The image is then decrypted:

$C_l = E_l \oplus r$

where $C' \in R,G,$ is a decrypted color channel still containing the hidden data.

Characterizing Data Hiding Techniques

The techniques embed a message inside a cover; various features characterize the strengths and weaknesses of the methods. The relative importance of each feature depends on the application.

Hiding Capacity: Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.

Perceptual Transparency: The act of hiding the message in the cover necessitates some noise modulation or distortion of the cover image. It is important that the embedding occur without significant degradation or loss of perceptual quality of the cover. In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stego-image, the steganographic encoding has failed even if the attacker is unable to extract the message. Preserving perceptual transparency in an embedded watermark for copyright protection is also of paramount importance because the integrity of the original work must be maintained. For applications where the perceptual transparency of embedded data is not critical, allowing more distortion in the stego-image can increase hiding capacity, robustness, or both.

Robustness:
Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, loss compression, and conversion from digital to analog form and then reconversion back to digital form (such as in the case when a hard copy of a stego-image is printed and then a digital image is formed by subsequently scanning the hardcopy.) Robustness is critical in copyright protection watermarks because pirates will attempt to filter and destroy any watermarks embedded in images. Anti-watermarking software is already available on the Internet and have been shown effective in removing some watermarks. These techniques can also be used to destroy the message in a stego-image.

Tamper Resistance:
Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego-image, such as a pirate replacing a copyright mark with one claiming legal ownership. Applications that demand high robustness usually also demand a strong degree of tamper resistance. In a copyright protection application, achieving good tamper resistance can be difficult because a copyright is effective for many years and a watermark must remain resistant to tampering even when a pirate attempts to modify it using computing technology decades in the future.

Other Characteristics:
Computational complexity of encoding and decoding is another consideration and individual applications may have additional requirements. For example, for a copyright protection application, a watermark should be resistant to collusion attacks where many pirates work together to identify and destroy the mark,

Data Embedding
Current methods for the embedding of messages into image covers fall into three categories: Least-Significant Bit embedding (or simple embedding), transform techniques, and methods that employ perceptual masking.

Least-Significant Bit Encoding
A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest steganographic techniques embed the bits of the message directly into the least-significant bit plane of the cover image in a deterministic sequence. Modulating the least-significant bit does not result in a human perceptible difference because the amplitude of the change is small. Other techniques "process" the message with a pseudorandom noise sequence before or during insertion into the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods [10]. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image.


Figure.3. cover image

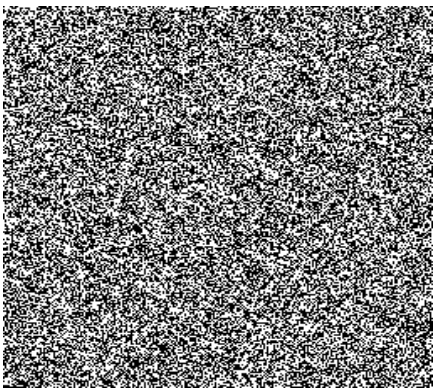
Figure.4. Difference image


Figure.5. Stego –image


Figure.6. Modified stego image

Spread-spectrum techniques and redundant encoding of the message can be employed in situations where robustness is critical. The watermark or message can be thought of as a narrowband signal encoded in a larger frequency band (the

cover). By spreading the energy of the embedded message across many frequency bands (such as by frequency hopping) the energy at any particular frequency band is reduced. Therefore the message becomes more difficult to detect modify without damaging the cover. Error correcting coding can be applied to the message during embedding to allow recovery even when some areas of the stego-image may be damaged or altered.

3. RESULTS AND DISCUSSION

In our experimental procedure we have used different set of cover and secret image. The experimental work of the proposed method formed stego-images by embedding secret image onto cover image using proposed random modified normal LSB replacement method and then compared the same images with normal LSB method. The difference of the stego image can hardly be distinguished after embedding. It is observed that human visual system(HVS) can hardly differentiate the original image and the stego-image and also the stego-images does not generate any suspicion. As in present proposed method a pseudorandom number generator is used to choose random pixels in an image by permuting the pixel indices with a secret key. The concept behind the proposed method is to devise a technique that enables secure data communication between sender and receiver. Furthermore, the secret messages were also retrieved successfully without encountering any loss of data. Most importantly, the modification of the cover image is not perceptible on the stego image at all and thus arouses no suspicion to third parties

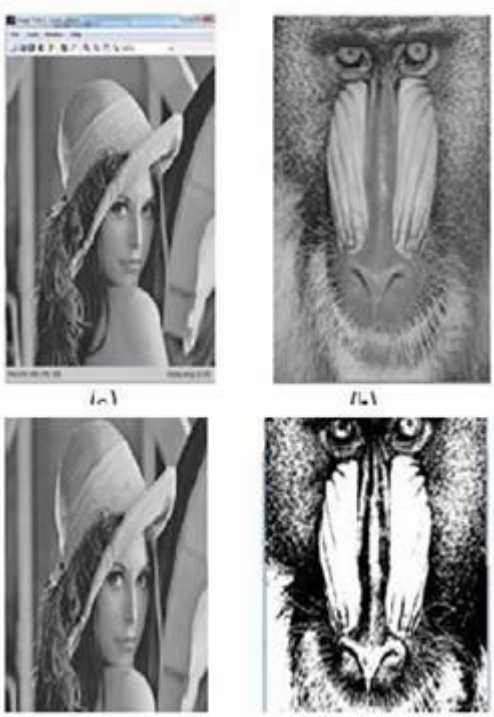

Figure.7. cover image and output image.

4. EXPERIMENTAL RESULTS

A series of experiments have been conducted to test the proposed method using many secret and target images. The presence of embedded data in covers can be detected by performing examination of the stego-image for distortion or excessive noise. Distortion in some cases can be visible under careful human observation. The known cover attacks simplify distortion analysis can be compared with a cover. Without affecting the perceptual quality of the image, destroying the embedded data can be a very difficult task, and entirely depends upon the method employed for data embedding.

5. CONCLUSION

The message to be protected is implanted in the cover file which can either be text, image or audio file. In steganography, LSB technique is applied in spatial domain to embed data in cover file. In this paper, we have compared the spatial domain technique The LSB Technique and Pseudo- Random Modified LSB Technique are applied on images to obtain secure stego-image which shows that PSNR of our Pseudo random modified LSB encoding is higher than PSNR of LSB encoding. The image resolution doesn't vary much when we insert the message into the image and the image is protected with the secret key. So, it is not possible to damage the data by any unauthorized person. This paper mainly enhances the security of the hidden data inserted in image deals with increasing the security of the message and increasing PSNR and reducing the distortion rate.

7. REFERENCES

[1]. X. Zhang, Let, vol. 18, pp. 255–258, 2011.”Reversible data hiding in encrypted images”, IEEE Signal Process.

[2]. B. Patra, J. C. Patra, 430-435, 2012 CRT-based fragile self recovery watermarking scheme for image authentication and recovery. International Symposium on Intelligent Signal Processing and Communications Systems.

[3]. W. Hong, T. Chen, and H.Wu, Lett., vol. 19, pp. 199–202, 2012, ”An improved reversible data hiding in encrypted images using side match”, IEEE Signal Process.

[4] Z.Wai1, S. Then, 2347-3878 Volume 1 Issue 2, October 2013”Data Hiding Technique Depended on pseudorandom Sequences”, International Journal of Scientific Engineering and Research (IJSER).

[5]. K. Maw. Zhang, X. Zha, N.Yu, and F. Li, o, vol. 8, pp. 553–568, 2013 ,”Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, IEEE Trans. Inf. Forensics Security.

[6]. X. Wu and W. Sun, ”High-capacity reversible data hiding in encrypted images by prediction error”, Signal Processing, pp. 387–400, 2014.

[7]. Y.-S. Kim, K. Kang and D.-W. Lim, , Appl. Math., vol. 9, pp. 2627–2636, 2015,”New Reversible Data Hiding Scheme for Encrypted Images using Lattices” .

[8]. Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu and B. Ma., IEEE Access, vol. 4, pp. 3210-3237, 2016, ”Reversible data hiding advances in the past two decades”.

[9]. X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, IEEE Trans. Cybernetics ,vol. 46, pp. 1132–1143, 2016,”High capacity reversible data hiding in encrypted images by patch-level sparse representation”,

[10]. I.-C Dragoi, H.-G. Coanda and D.Coltuc, in Proc.25th Eur. Conf. Signal. Process (EUSIPCO), pp. 2250 2254, 2017,” Improved Reversible Data Hiding in Encrypted Images Based on Reserving Room After Encryption and Pixel Prediction.