Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 6, June 2013, pg.209 – 215

RESEARCH ARTICLE

A Novel Steganographic Approach for Enhancing the Security of Images

Priya Thomas[1], Avanish Kumar Singh[2]

[1]Department of Computer Science & Engineering, Nehru College of Engineering & Research Center, Thrissur, Kerala, India

[2]Department of Computer Science & Engineering, Nehru College of Engineering & Research Center, Thrissur, Kerala, India

[1] *priyathomas1332@gmail.com;* [2] *aavi13@gmail.com*

Abstract— Internet users need to store, send or receive the secret data. The common way to do this is to transform the secret data into another form by the process called encryption. Here, the main drawback is if enough time is given the enemy is allowed to intercept and modify the messages. In order to avoid this we use the technique called steganography. Steganography is the method of storing information in a way that hides that information's existence and it can be used to carry out hidden exchanges. Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. This technique is commonly used for ensuring the secrecy of medical images, military images etc transmitted through the internet.

Key Terms: - Least Significant Bit (LSB) steganography; Hiding Behind Corners (HBC); Pixel-Value Differencing; security; steganalysis; statistical attacks

I. INTRODUCTION

Steganography is the art of embedding data by hiding that information's existence. The main purpose of steganography is to send secret or confidential messages under the cover of a carrier signal. It is generally accepted that any steganographic technique must possess two main properties: good imperceptibility and sufficient data capacity. The first property ensures that the embedded messages are difficult to detect, and the second implies efficiency in hidden communication. Steganography and cryptography aims at security, but both are different. The goal of cryptography is to communicate securely by changing the data into a form that an eavesdropper cannot understand. Steganography techniques, on the other hand, tend to hide the presence of the message and make it difficult for an observer to figure out the possibility of occurrence of the message. Here a novel scheme is proposed which combines encryption and steganography in a single step. Thus the reliability of the image as well as the data to be transmitted is ensured. This technique embeds data in an imperceptible way and restores the image with lesser distortions after data extraction. The method of embedding secret data into an image has gained importance in military as well as surveillance applications. The success of this process requires the development of robust steganographic algorithm in order to embed the data in an imperceptible manner as well as to extract the secret data with no loss. Thus a new steganographic method has been presented, which can securely embed data and efficiently extract data by preserving the secrecy and confidentiality.

II. EXISTING METHODS

Many techniques have been proposed to perform image steganography. The main design criterion for steganographic algorithms includes the level of invisibility, robustness against various attacks, imperceptibility, payload capacity etc. The novel scheme incorporates the positive aspects from the existing techniques and introduces an efficient and highly secure version.

Reversible data hiding method was introduced as an approach for data hiding. J.Tian *et al.* proposed a hiding method called difference expansion technique [1]. In that method, one bit can be embedded into two consecutive pixels. So the maximum embedding capacity is 0.5 bpp. However, the difference expansion based reversible data hiding methods have to double the differences between pixels. So larger distortion occurs and may not be suitable for applications where high quality images are demanded. K. Hempstalk *et al.* proposed another technique, Hiding Behind Corners (HBC) [2] which used a technique called Filter First that eliminates the need to provide any extra information such as original image, yet ensures that the same pixels are used for hiding and retrieval. FilterFirst [3] used an edge-detecting filter, such as the Laplace formula [4], to find the areas of the image where there are pixels that are the least like their neighbours. The weaknesses of Filter First were that it was not secure, as an attacker can repeat the filtering process. Ni *et al.* later introduced a novel histogram-shifting [5] reversible data hiding technique. In that method, pixel values were modified one greyscale value at most and thus, a high quality stego image could be achieved. However, the payload of the method was relatively low. The analysis based on several parameters showed that the payload in smooth regions is not only much higher than that of complex regions, but the distortion caused by data embedding is also smaller than that of the complex regions.

K. M. Singh *et al.* introduced a technique called Hiding Secret Message in Edges of the Image [6]**.** Here a new least significant bit embedding algorithm for hiding secret messages in non-adjacent pixel locations of edges of images was proposed. Here the messages are hidden in regions which are least like their neighbouring pixels i.e, regions that contain edges, corners, thin lines etc so that an attacker will have less suspicion of the presence of message bits in edges. One common disadvantage of LSB embedding was that it created an imbalance between the neighbouring pixels. It also limits the length of the secret message to be embedded. Moreover the embedding capacity was relatively low. C. M. Wang *et al.* [7] proposed a high quality steganographic method with PVD and Modulus function [8]. Here, the difference value between two consecutive pixels was computed and then their remainder was calculated by the modulus operation. The secret data was embedded into the two pixels by modifying their remainder. The hiding capacity of the two consecutive pixels depends upon the difference value taken. However unusual steps in the histogram of pixel differences reveal the presence of a secret message. An analyst can even estimate the length of hidden bits from the histogram. C. H. Yang *et al.* introduced the technique, Adaptive Data Hiding in Edge areas of image with Spatial LSB Domain Systems (AE-LSB) [9]**.** The difference value of two consecutive pixels estimates how many secret bits could be embedded into the two pixels. The readjusting phase ensures that the two consecutive pixels belong to the same level both before and after embedding. AE-LSB provides better capacity but is vulnerable to attack by RS steganalysis. It also has a characteristic of imperceptibility. But here the less smooth regions would get contaminated due to its lesser modification rate. Luo *et al.* proposed a new reversible data hiding method based on interpolation technique [10] which concealed data into interpolation errors. Instead of using the nearest neighbour interpolation technique, they offered a feasible image interpolation algorithm to obtain the interpolation errors. The pixels with larger prediction errors not only provide no payload, but also cause distortion since they have to be shifted. W. Luo *et al.* proposed an adaptive scheme Edge adaptive image steganography based on LSB Matching Revisited (LSBMR) [11] where one can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. The new scheme can enhance the security significantly compared with typical LSB-based approaches [12] as well as their edge adaptive ones.

III. PROPOSED SYSTEM

Existing systems like LSBMR embeds data in an image in a secure manner. The hidden data is secure against all type of attacks. Here the data is completely safe. But the image itself is not protected. Application like medical imaging highly demands the security of image as well as data. Surveillance and military application demands the same. So in order to provide security to the data as well as the image the novel scheme will first embed data into image using LSBMR, and then encrypt it using AES. At the receiver side the receiver must first decrypt image using the key and finally the data can be extracted using the data hiding key. Hence the image as well as the secret data will be successfully transmitted and extracted.

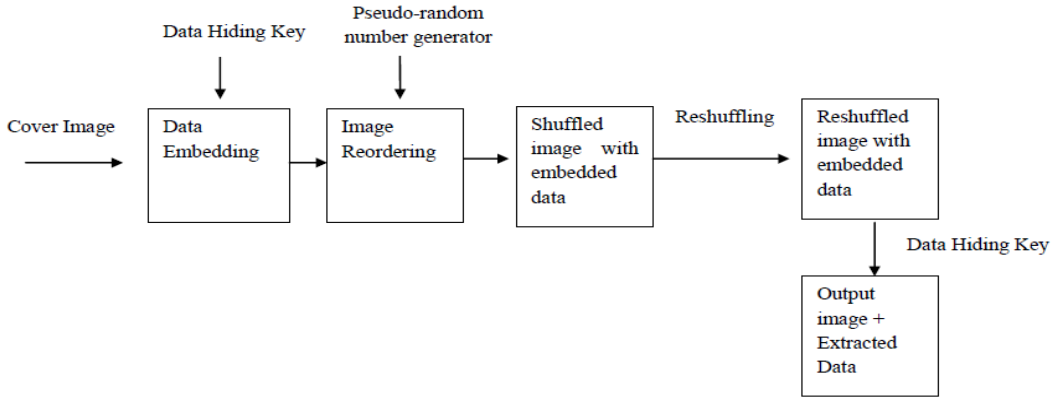

Fig. 1 System Architecture

A. Data Hiding

First step in data hiding will suitably selects the cover image to embed the data and second step will select appropriate region in the cover image for securely embedding secret data. The selection of input image is an important design criterion as it contributes much to data hiding. The second step divides the cover image of size mxn into non-overlapping blocks of B_Z x B_Z pixels. The resulting image is rearranged as a bitmap B by using raster scanning. And then the vector is divided into non-overlapping embedding units with every two consecutive pixels (x_i , x_{i+1}) where i= 1,2,3,...mn-1. Two benefits can be obtained by this approach. First, it can prevent the detector from getting the correct embedding units without the key key1, thus improving the security. Furthermore, both horizontal and vertical edges within the cover image can be used for data embedding.

The data embedding is performed according to the scheme of LSBMR [10] where secret bits can be embedded into each embedding unit by manipulating the LSB of the cover image. Therefore, for a given secret message M and a password P the threshold T for region selection can be determined as follows. The length of the secret message and password are used for region selection. Based on these lengths the RGB components of the input image are modified. If any region is insufficient to occupy the data, another region will be selected which satisfies the design criterion. The data embedding will consider the ratio of RGB components in the cover image and hence the quality is completely ensured. Moreover the secret data is password protected and hence cannot be extracted by any means without correct knowledge of the password as well as the length of the data and password. After data hiding, the post processing operations are done as final step. Here the resulting image is divided into non-overlapping B_Z x B_Z blocks. By proper knowledge of the requirements the secret message can be recovered fully and the image can be returned without any distortions.

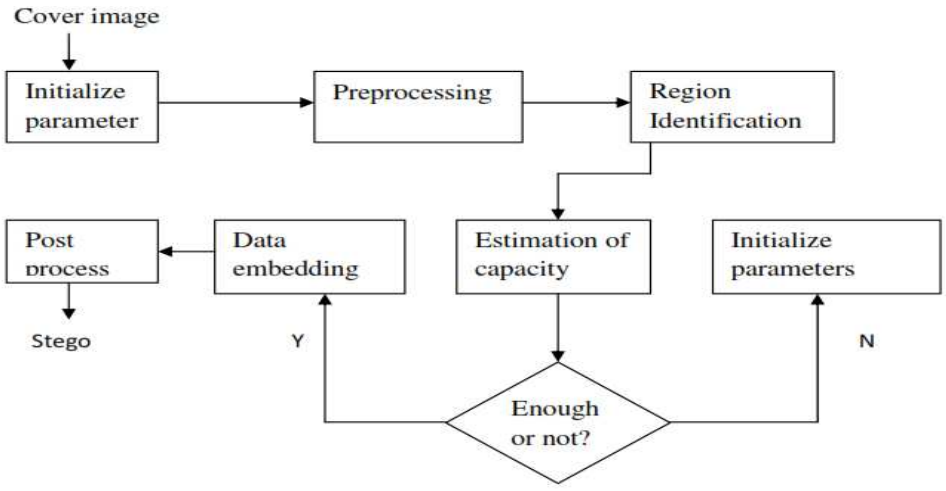

Fig. 2 Data embedding

B. Image Reordering

The use of computer networks for data transmissions has increased the need of security. The data embedding process is common. So steganalysis also has gained much popularity. The data hiding techniques are

continuously manipulated to extract the hidden data. So here we are introducing an additional feature which reorders the cover image in such a way an attacker will not be able to detect the hidden data by simply manipulating the image. The image reordering phase includes two sub processes: image splitting and image reshuffling.

Image splitting will divide the input image into MxN sized chunks. The image chunks can be of same or different dimensions. The smaller the size of chunks, the higher is the level of security. The chunks will be reordered in the second phase. The reshuffling phase will reorders the chunks in a random manner. Here we use a pseudo random number generator to generate the random series. The generated series will line up the image chunks in a desired manner. The final output will be in the form of a shuffled image. The main advantage of image shuffling is that an attacker will not be able to exploit the statistical features of the image to extract data. The hidden data will not be visible manually or statistically. Thus the data will be highly secure. The data hiding algorithm usually embeds the secret data in the LSB of the cover image. So the shuffling phase will change the LSB of the output image. So the attacker will not be able to guess the existence of data in the image. Moreover, the image can also be made secure than exposing it as such unlike the previous approaches. The steps in image reordering include image pre-processing, image splitting, image ordering etc as shown in fig 3.

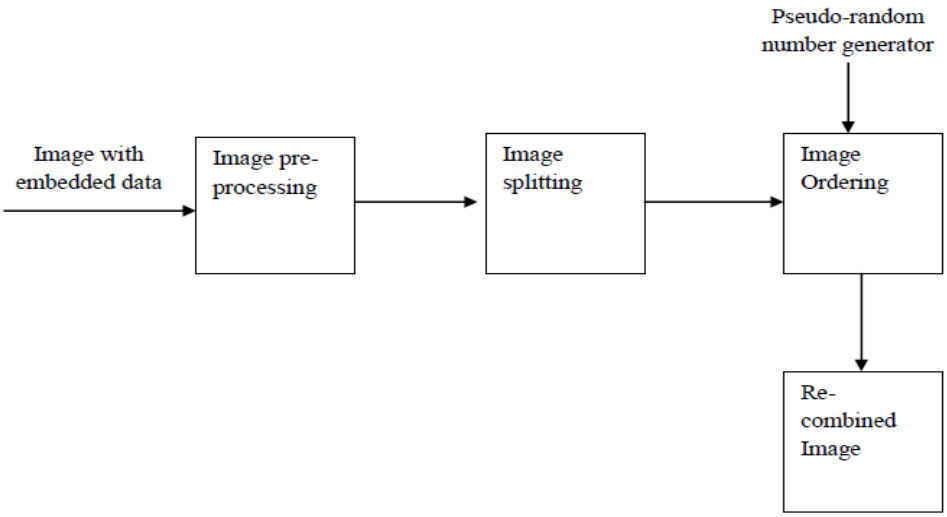

Fig. 3 Image Reordering

C. Image Reshuffling

The shuffled image containing embedded data is transmitted to the receiver. As the data and image are protected the reliability of data as well as image is guaranteed. The received image should be re-shuffled to extract data successfully. The reshuffling phase will reorder the image and will combine the image in an orderly manner. Thus the transmitted image could be completely recovered. The data extraction process should be performed to recover the image as such. The image with secret data can be transmitted to desired location to extract data if required.

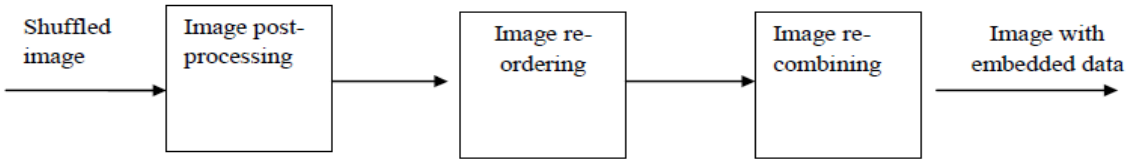

Fig. 4 Image Reshuffling

D. Data Extraction

The decrypted image with embedded data is subjected to feature extraction phase. The receiver must first enter the password to start extraction procedure. First we divide the stego image is divided into B_Z x B_Z blocks. The resulting image is rearranged as a row vector V'. Finally, we get the embedding units by dividing V' into

non-overlapping blocks with two consecutive pixels. The image must be reshuffled to start extraction process. We travel the embedding units in the reverse manner and extract the embedded data by right shifting the RGB components. The secret message embedded into the image will be extracted successfully if the password matches. The length of the message will be extracted first from the left most bit. The extraction loop will iterate until the complete message is extracted. The extraction process depends on the length of the secret message embedded. For each qualified embedding unit, say,

(x_i', x_{i+1}') where,

$|x_i', x_i'_{+1}| <= T,$

We extract the secret bits by right shifting. Thus the extraction phase will retain the quality of the original image as such after data extraction. If the password matches and the extraction were successful the embedded message will be retrieved. Thus the secrecy of the embedded data is ensured.

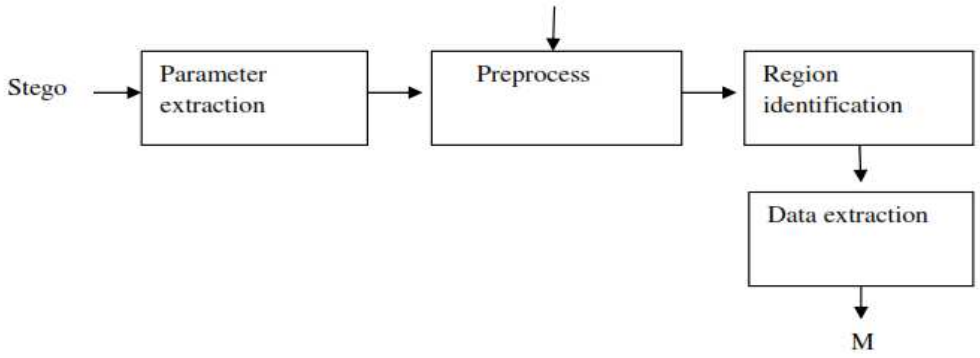

Fig. 5 Data Extraction

IV. EXPERIMENTAL RESULTS

In existing method the level of security was low compared to the proposed method. The existing techniques were slow compared to the algorithms used in our method. The proposed method completely hides the data in the image and reorders the image before transmission. The security of the data as well as the image is ensured in our method. The input image and the output image are exactly similar with lesser distortions compared to existing techniques as shown in the figure below.

Fig. 6 a) Cover image

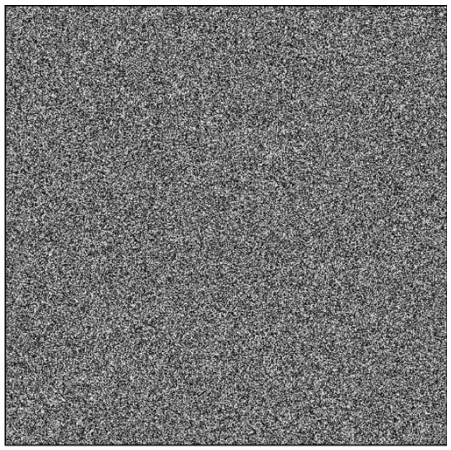

Fig. 6 b) LSB of stego

Fig. 6 c) Final version after data extraction

The existing system data hiding algorithms takes more execution time. Here we use fast effective algorithms for data hiding as well as encryption. So we can reduce the execution time for the encryption process. The security of the existing system is comparatively high than the existing techniques. The level of security is enhanced in our proposed system compared to the existing methods. The comparison graph is shown below.

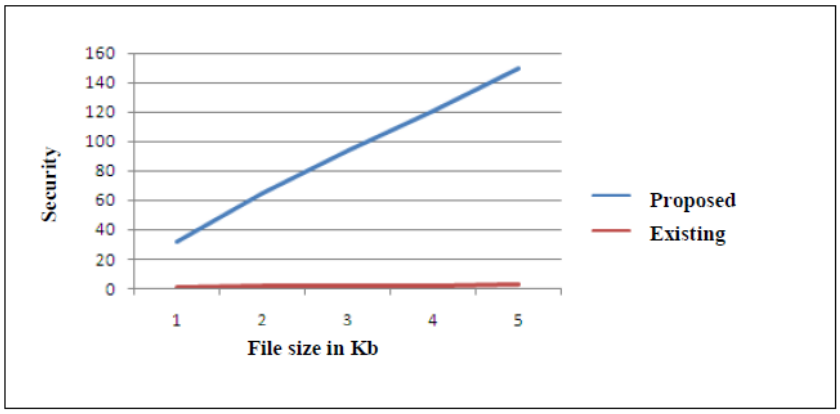

Fig. 8 Security levels for existing and proposed system

V. CONCLUSIONS

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. For embedding secret information in images, there exists variety of steganographic techniques. Some of them are more complex than others and all of them have their own respective strong and weak points. Some applications may require absolute invisibility of the secret information, while others may require a larger secret message to be hidden into an image. Usually there exist some smooth regions in all natural images, which may cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If we are embedding a message in these regions, the LSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. To protect the image along with data, the novel scheme first embeds the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. The embedded image is reordered to remove the dependencies between pixels in cover image and stego image. Thus the confidentiality of the message and data is assured. This mechanism highly improve the confidentiality and reliability of the image and hence widely used for medical imaging and military applications.

REFERENCES

[1] J. Tian, "Reversible data embedding using a difference expansion." IEEE Transactions on Circuits and Systems for Video Technology, 13, 8, PP 890–896, 2003.

[2] W. Bender, D. Gruhl, N. Morimoto, & A.Lu, "Techniques for data hiding", IBM Systems Journal, 35, PP 210-224, 2002.

[3] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, 4, 2, PP 127-135, 2001.
[4] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," Proceedings of the IEEE , Hamilton, New Zealand, 2006.
[5] B. Dunbar, L.H. Chen, "Steganographic techniques and their use in an Open-Systems environment", Proceedings of SANS, 2006.
[6] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, "Reversible data hiding" , IEEE Transactions on Circuits and Systems for Video Technology , 16 , 3 ,PP 354–362,2006.
[7] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, " High quality steganographic method with pixel-value differencing and modulus function," Science Direct The Journal of Systems and Software, 2007.
[8] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun. "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Transactions on Information Forensics Security, 3, 3, PP 488–497, 2008.
[9] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, "Reversible image watermarking using interpolation technique," IEEE Transactions on Information Forensics and Security , 5 ,1, PP 187–193, 2010.
[10] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," Proceedings of International Conference on Information and Communication Technology, PP 238–241, 2007.
[11] N.F. Johnson, & S. Jajodia, "Exploring Steganography: Seeing the Unseen", Proceedings of the 2nd Information Hiding Workshop, 12 ,4 , PP 120-128, 2007.
[12] L.M. Marvel, C.G. Boncelet , & C. Retter, "Spread Spectrum Steganography", IEEE Transactions on image processing, 8,8, PP 160-178, 2007.

