International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.11, November 2015 DOI:10.15693/ijaist/2015.v4i2.146-150

Image Hiding Technique Using Grey Prediction Model and Grey Relational Analysis

Joshi. K
M.E. Communication and Networking, National Engineering College, Kovilpatti, India.

Rajagopal. S
Asst Professor, Dept. of IT, National Engineering College, Kovilpatti, India.

***Abstract*— Various image hiding algorithm cannot maintain a good balance of capacity, invisibility and robustness. These images usually contain private or confidential information so that they should be protected from leakages during transmissions. Recently, many methods have been proposed for securing image transmission, for which two common approaches are image encryption and image hiding. So in this project, a new technique of color image hiding algorithm based on grey prediction model and grey relational analysis in the Discrete Cosine Transform (DCT) domain is proposed. First, this algorithm compresses the secret image losslessly based on the improved grey prediction model. It then chooses the rich texture block in the cover image as the embedding regions using Double-dimension Grey Relational Analysis (DGRA). Finally, it embeds the compressed secret bits streams into the DCT domain mid-frequency coefficients, which is chosen as the texture block using Double-Dimension Grey Correlation Degree (DGCD). Then the secret image is securely transmitted and at the receiver side the secret image is retrieved from the cover image. Finally, the PSNR is calculated for compressed image and stego image, RMSE is calculated for the prediction image and the original image and the Normalized Correlation (NC) is calculated to evaluate the similarity between the original and the extracted secret image. This method provides an adequate balance between invisibility, capacity and robustness.**

Keywords— DCT, DGCD, image hiding, DGRA, Grey Prediction Model.

I. INTRODUCTION

The development of image Steganography is used in various organizations to communicate between its members and used for communication between members of the military or intelligence agents of companies to hide secret messages or secret image. The main aim of Steganography is to avoid drawing attention to the transmission of hidden information. The main terminologies used in the Steganography are, the cover message, secret message, secret key and embedding algorithm. The cover message is the carrier of the message such as image, video, audio, text, or other digital media. The secret message is the information which is needed to be hidden in the suitable digital media. The secret key is usually used to embed the message depending on the hiding algorithms. The embedding algorithm is used to embed the secret information in the cover message.

To deliver the information secretly, traditional cryptography algorithms mainly uses a replacing or scrambling of the information bits or secret information bits to change the features of the secret information. The cipher text gives a stream of meaningless codes so that the intruder simply destroy them or easily attack and try to recover them which causes serious effects to information communication. To avoid this problem, image hiding technique mainly focuses to hide coded information into another host which makes hard to attacker to retrieve the secret information.

Several methods have been introduced to avoid the problem in image hiding techniques. Image hiding is a method which hides the secret image or confidential image into the cover image so that no one can find the existence of the secret image or data. Various existing data hiding methods use the techniques of LSB substitution [9], recursive histogram modification [1], difference expansion [3],Inverted pattern approach using LSB substitution [4], wavelet transform, discrete cosine transform, reversible data hiding [5], LSB substitution using Genetic algorithm [9], reversible watermarking algorithm [2], Difference expansion based reversible data hiding [8], the algorithm based on spatial domain [10-12] have large capacity but the robustness is unsatisfactory, the algorithm based on transform domain [13-15] have good robustness and invisibility but the hiding capacity is low. Therefore, information hiding mainly focuses on invisibility, robustness and hiding capacity.

In this paper a new method of image information hiding based on Grey Prediction and grey relational analysis using the Discrete Cosine Transform (DCT) domain is proposed. The secret image is compressed losslessly based on improved grey prediction model is described in section III. Section IV shows the procedure used to choose the rich texture block in the cover are chosen as the embedding region to embed the secret information bits using the double-dimension grey relational analysis (DGRA). Section IV explains the Embedding of Secret information bits. Section II explains the proposed work to embed the compressed bits in the DCT domain mid-frequency coefficients which is chosen by the block using Double Dimension Grey Correlation Degree (DGCD).

II.PROPOSED METHODOLOGY

The proposed method consists of two stages as shown in the block diagram of Fig. 1: 1) Image Compression based on Grey Prediction Model and 2) Choosing of rich texture block based on Double-Dimension Grey Relational Analysis. 3) Embedding the secret information bits.

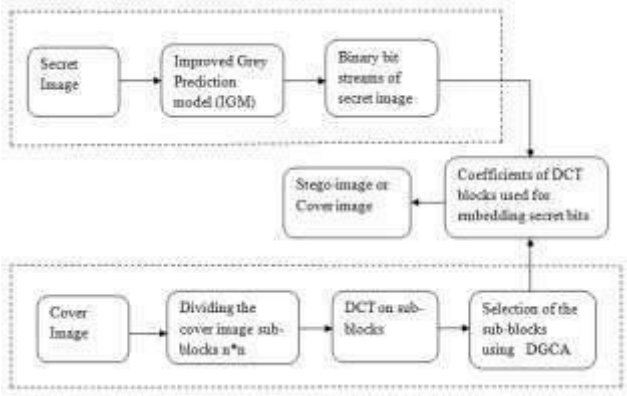

Figure 1. Block Diagram of the Proposed Method

In the first stage the secret image is compressed by a lossless called improved grey prediction model (IGM) to form the binary bit streams using the code table. Then the secret information binary bit streams are compressed using Run length Encoding Compression technique. In the second stage, the cover image is divided in to size of n*n block, then DCT domain is applied to form the blocks of DCT coefficients. The Grey Correlation Degree is calculated using the DCT coefficients from that the Double-Dimension Grey Correlation Degree (DGCD) is calculated. Using the DGCD, the rich texture block is selected and the Secret binary information bits are embedded in the selected block. Finally, the PSNR is calculated for compressed image and stego image, RMSE is calculated for the prediction image and the original image calculated and the Normalized Correlation (NC) is calculated to evaluate the similarity between the original and the extracted secret image

III. IMAGE COMPRESSION BASED ON GREY PREDICTION MODEL

Image compression technique is mainly classified into two types such as lossless compression and lossy compression. Some images such as medical images, satellite images, geographical images and military images contains the secret information which needs to completely reflect the original information at the receiver side. So this application uses a lossless compression to reduce the redundant data. In this paper a new method of image compression called Grey Prediction Model to compress the secret image.

A. Prediction of Adjacent Pixel Values

Consider the image is a blocks of pixels, IGM (Improved Grey Prediction Model) has a more accurate prediction results for the pixels in the block. For example the prediction value is calculated by considering the first three original values of a block and predicting the fourth block value. Likewise all the block values of an image are calculated sequentially. From the predicted values, the prediction error is calculated by subtracting the original value with predicted value to gives a prediction error.

B. Encoding the Prediction Error

The prediction errors are encoded by using the coding table with the combination of paragraph identity codes and segment code corresponding to the paragraph codes to give the binary bit streams containing the secret information. The maximum in the paragraph identification code is determined by the actual maximum of the absolute value of the prediction error. The total number of bits after error coding is smaller than the original image. After all the prediction error are coded in to binary bit streams it should be compressed using Run length encoding compression technique. The compression ratio (Cr) is defined as,

Cr = size before compression / size after compression. (1)

Now the compressed binary bit streams containing the secret information is ready to embed in the rich texture block of the cover image.

IV. SELECTION OF RICH TEXTURE BLOCK USING DGRA

Grey Relational Analysis is widely used in data sequence relevance, image matching, image texture analysis etc. It is used color images, because of the high data redundancy, the rich texture block and the similarity in pixel values at corresponding positions of the R, G, B component is calculated using DGRA (Double Dimension Grey Relational Analysis).

*C. Dividing the Cover Image into N*N and applying DCT Domain*

The cover image is divided into the block size of n*n (16*16) and the Discrete Cosine Transform (DCT) domain is applied to get the DCT coefficients. Then the average of all the R, G, B component of the DCT coefficients to get the Grey Correlation Coefficients (GCC). The GCC is calculated using the formula,

$$GCC(dx_{0j}, dx_{ij}) = \frac{\min\min\left|dx_{0j} - dx_{ij}\right| + \varepsilon \max\max\left|dx_{0j} - dx_{ij}\right|}{\left|dx_{0j} - dx_{ij}\right| + \varepsilon \max_{i}\max_{j}\left|dx_{0j} - dx_{ij}\right|} \quad (2)$$

Where, $\{1 \le i,j \le N\}$ and ε is resolution ratio(0,1). Using the Grey Correlation Coefficient (GCC), the Grey Correlation Degree (GCD) is calculated using the formula,

$$GCD(X_0, X_i) = \frac{1}{n}\sum_{j=1}^{n} GCC(dx_{0j}, dx_{1j}) \quad (3)$$

The Grey Correlation Degree (GCD) is calculated in horizontal, vertical and diagonal directions of the GCC of DCT coefficient matrix. It should be noted that when

calculating GCD_D, we choose the two longest diagonal sequence of x and the sequence with 64 elements after zig-zag scans for this block as contrast sequence.

D. Selection Rich Texture Block using the DGCD

According to direction sensitivity to the image texture, the double-dimension grey correlation degree (DGCD) is defined as,

$$DGCD = GCD_H + GCD_V + GCD_D \quad (4)$$

Where, GCD_H, GCD_V and GCD_D are the average grey correlation degree at horizontal, vertical and diagonal direction respectively. Then the rich texture block is found out by comparing the DGCD with Threshold (T). So if the DGCD>T, then it is consider as a smooth block and it is neglected. If DGCD < T, then that block is chosen as a rich texture block for embedding.

V.EMBEDDING THE SECRET INFORMATION BITS

The secret information bit streams are embedded in the mid frequencies of DCT coefficients of the embedded block. The following two conditions exist for embedding the secret information bits:

1. Secret bit str(r)=0 ,then
   EmbedBlockDCT(k,n)=min{EmbedBlockDCT(k,n), EmbedBlockDCT(k,n+1)} (or)
   EmbedBlockDCT(K,n+1)=max{EmbedBlockDCT(k,n), EmbedBlockDCT(k,n+1)}
2. Secret bit str(r)=1, then
   EmbedBlockDCT(k,n)=max{EmbedBlockDCT(k,n), EmbedBlockDCT(k,n+1) (or)
   EmbedBlockDCT(k,n+1)=min{EmbedBlockDCT(k,n), EmbedBlockDCT(k,n+1)}

Then the secret information bits, the first row and column values of original image which is used to extract the image using the prediction error, image size, error compression method and the parameter values are embedded in the rich texture block which is used to retrieve the original secret image at the receiver side. Finally, the stego image is formed which same as that of the cover image is taken at the initial stage.

VI .Performance Analysis

The performance of the image can be found by the Root Mean Square Error value (RMSE), the Peak Signal to Noise ratio value (PSNR) and the Normalized Correlation (NC) are the three metrics used to compare image compression, quality of an image before and after extraction.

The Root Mean Square Error (**RMSE**) (also called the root mean square deviation, RMSD) is a frequently used as measure of the difference between values predicted by a model and the values actually observed.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n} (X_{obs,i} - X_{model,i})^2}{n}} \quad (5)$$

Where, Xact,i is the actual pixel values of an image
Xmod,i is the predicted pixel values of an image.

The **PSNR**, peak signal-to-noise ratio, in decibels, between two images is defined as the ratio used as a quality measurement between the original and a compressed image. Here the PSNR is calculated for cover image before and after embedding and secret image before and after embedding. Higher the PSNR, better the quality of the compressed or reconstructed image. The PSNR is represented as a following equation.

$$PSNR = 10 \log_{10}\left(\frac{R^2}{RMSE}\right) \quad (6)$$

Where, R is the fluctuation in the input image.

The Normalized Correlation (**NC**) is defined to evaluate the similarity between the original secret image in the initial stage and the extracted secret image in the receiver side. Here the NC is calculated for cover image before and after embedding and secret image before and after embedding.

$$NC(X, X') = \frac{\sum_{m,n} X(m,n)\, X'(m,n)}{\sqrt{\sum_{m,n} (X(m,n))^2 \, (X'(m,n))^2}} \quad (7)$$

Where, m and n represents the number of image rows and columns. X (m,n) stands for grey intensity at the pixel (m,n) of the original image. X`(m,n) stands for the grey intensity at the pixel (m,n) of the embedded image.

VII. RESULTS AND DISCUSSION

An experiment has been done to examine the proposed methodology using a sets of secret and target image with the size of 380×380 or 500×500 or 400×400 etc. Finally it, shows the decompressed secret image which is same as that of the preselected target or cover image and the quality metric is verified using the RMSE, NC and PSNR values between the images.

(a)

(b)

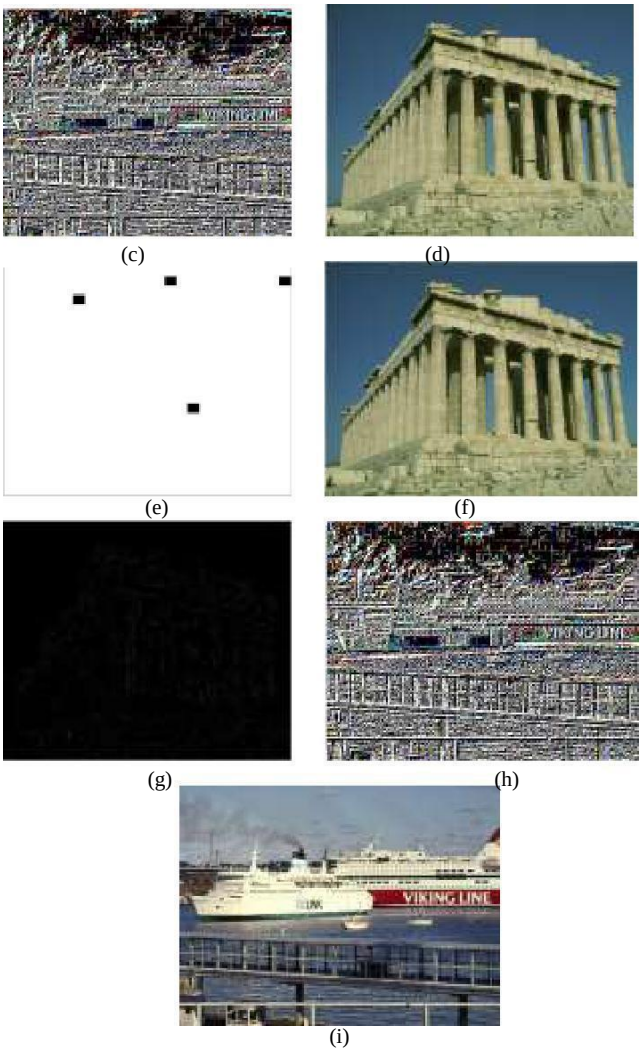

Figure 3 shows the experimental results image hiding technique using IGM and DGRA

An example shows the experimental results in Fig. 3; Fig. 3(a) shows the input secret image and fig. 3(d) the target or cover image. The target image is of block size 16×16. The Fig. 3(b) shows the predicted values of the secret image using IGM is represented in the form of image with an RMSE of 19.7395. Fig. 3(c) shows the prediction error of an secret image which is in uncompressed stage. The Fig. 3(e) shows chosen blocks for embedding the secret image bits using DGRA and the Fig. 3(f) shows the stego image which is same as that of the cover image after embedding the secret bits with PSNR of 30.8004 and NC of 0.99814. Fig. 3(g) shows the difference between the target image and stego image after embedding the secret information bits and the Fig. 3(h) shows the prediction error in decompressed stage which is used to extract the secret image. Finally, Fig. 3(i) shows the extracted secret image from stego image after decompression with PSNR of 31.2772 and NC of 0.99914.

VIII. CONCLUSION

Finally, a blind color image information hiding algorithm based on grey prediction and grey relational analysis in DCT domain is proposed. Meanwhile the blind information hiding is more confusing to the attackers. Here the secret image is compressed using the improved grey prediction model and it is converted to binary bit streams, then the appropriate blocks chosen for embedding the secret binary bit streams using the Double Dimension Grey Relational Analysis (DGRA). Finally, the stego image is created and at the receiver side the original secret image is extracted from the stego image using the retrieved embedded information and the quality of an image is verified using the performance metric such as RMSE, PSNR and NC for the image before and after embedding for both secret and cover image.

REFERENCES

[1] Zhang, X. Hu, X. Li, and N. Yu, "**Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression**," IEEE Trans. Image Process., vol. 22, no. 7, pp. 2775–2785, Jul. 2013.

[2] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "**Reversible watermarking algorithm using sorting and prediction,"** IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[3] Y. Hu, H.-K. Lee, K. Chen, and J. Li, "**Difference expansion based reversible data hiding using two embedding directions,"** IEEE Trans. Multimedia, vol. 10, no. 8, pp. 1500– 1512, Dec. 2008

[4] C. H. Yang, "**Inverted pattern approach to improve image quality of information hiding by LSB substitution**," *Pattern Recog.*, vol. 41, no. 8, pp. 2674–2683, 2008.

[5] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "**Reversible hiding in DCT-based compressed images**," *Inf. Sci., vol. 177, no. 13,* pp. 2768–2786, 2007.

[6] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su**, "Reversible data hiding**," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[7] C. K. Chan and L. M. Cheng, "**Hiding data in images by simple LSB substitution,"** Pattern Recognition.., vol. 37, pp. 469–474, Mar. 2004.

[8] J. Tian, "**Reversible data embedding using a difference expansion,"** IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[9] R. Z. Wang, C. F. Lin, and J. C. Lin, "**Image hiding by optimal LSB substitution and genetic algorithm**," *Pattern Recog., vol. 34, no. 3,* pp. 671–683, 2001.

[10] CHANG C C, HSIEH Y P, LIN C Y. ***Lossless Data Embedding With High Embedding Capacity Based on De-Clustering for VQ-Compressed Codes***. IEEE Transactions on Information Forensics and Security, 2007: 341-349.

[11] LI Changcheng, XU Wei, MENG Liang, *et al.* ***Realization of a LSB Information Hiding Algorithm Based on Lifting Wavelet Transform Image***, August 19-22, 2011. Jilin, China. IEEE Computer Society, 2011: 1015- 1018.

[12] KANG Xiaojun, DONG Lijun, WANG Yun***. Research on an Information Hiding Algorithm Based on Most Significant Bit in Image***, October 22-24, 2010. Taiyuan, China. IEEE Computer Society, 2010: 372-374.

[13] LIU Jinhua, SHE Kun. ***Quantization-Based Robust Image Watermarking Using the Dual Tree Complex Wavelet Transform***. China Communications, 2010: 1-6.

Authors Profile

K.Joshi received the **B.E.** degree in Electronics and Communication engineering from the K.L.N College of Engineering, Madurai, Anna University, Chennai, India, in 2012. Currently doing **M.E.** Communication and Networking in National Engineering College, Kovilpatti, India, Anna University, Chennai, India. His research interest includes Image processing, Security in image processing, Image compression.

S.Rajagopal (Sankarasubbu Rajagopal) obtained his Bachelor's degree in Electronics and Communication Engineering from Anna University (P.S.R Engineering College, Sivakasi in 2007). Then he obtained his Master's degree in Computer and Communication from Anna University (National Engineering College, Kovilpatti in 2009). Currently, he is a Assistant Professor at the Department of Information Technology, National Engineering College, Kovilpatti. His specializations include real time video processing, Video Analytics, Video Encryption, Video compression.

[14] YOU Xinge, DU Liang, CHEUNG Yiuming, *et al*. ***A Blind Watermarking Scheme Using New Non-Tensor Product Wavelet Filter Banks***. IEEE Transactions on Image Processing, 2010: 3271-3284.

[15] JIAO Jianquan***. Research on Information Hiding Technology on DCT Domain Based on Grey System Theory***. 2008, Zhengzhou, China communication.