Implementation of XOR and Edge Identification Method in Steganography

Permella Abishai Jasper
Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad

D.Jayanthi
Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad

N.Arun Vignesh
Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad

K.G. Maheshwari
Department of IT, Institute of Road and Transport Technology, Erode, Tamil Nadu

Abstract - In this paper, a novel image steganography algorithm that combines the strengths of edge detection and XOR coding, to conceal a secret message either in the spatial domain or an Integer Wavelet Transform (IWT) based transform domain of the cover image is presented. Edge detection and XOR coding are used in to conceal the secret message. Edge detection enables the identification of sharp edges in the cover image and this when embedding results in good image quality. Edge detection method presented here is capable of estimating the exact edge intensities for both the cover and stego images (before and after embedding the message), which is essential when extracting the message. The XOR coding, on the other hand, is a simple, yet effective, process that helps in reducing differences between the cover and stego images. Experimental results are observed using XILINX ISE and demonstrated that the proposed method has achieved better imperceptibility results than other popular steganography methods.

Keywords - Image Steganography, Human Visual System (HVS), EDGE detection and XOR Coding.

I. INTRODUCTION

Steganography is an art of hiding information in a way that prevents the detection of hidden messages and this is achieved by hiding one piece of information within another piece of innocent-looking information. There are several methods of embedding data, such as spatial and time domain methods, Transform domain methods and fractal coding methods. These methods hide/embed information in different types of media such as text, image, audio, video, etc. Varieties of different file formats, digital images are considered the most popular types of carriers because of their size and frequency of distribution. Image steganography is the steganography subdivision where digital images are used as information carrier file formats. The joint image format (JPEG), the graphics exchange format (GIF), the bitmap (BMP) image format and the Portable Network Graphics (PNG) format are the most popular image file formats. Share on the Internet. Steganography is the art of hiding messages in a medium called a cover object in such a way that
the existence of the message is undetectable. Imperceptibility is clearly the most important requirement. The cover object can be a digital image, an audio file or a video archive. The secret message called payload could be plain text, an image, a video file or an audio. Steganographic methods are classified in the domain spatial domain and domain incorporation Embedding In the frequency domain, images are transformed into frequency components DCT, FFT or DWT and then the messages are embedded in the bit level or in the block level. In Space domain LSB replacement is the most widely used data hiding method. However, most of the LSB techniques are prone to seizures. Due to the low computational complexity and high This work is mainly concerned with the LSB steganography method.

Imperceptibility is an essential requirement for steganography techniques, which reflects the ability of these techniques in maintaining the visual quality of the produced stego images. It is well-known that the HVS is less sensitive to changes in sharp areas of images compared to smooth areas. The first steganography method designed based on this fact was the Pixel-value differencing (PVD), which attempts to embed into sharp areas. The original PVD algorithm introduced by Wu and Tsai (2003) converts the 2D image into a 1D vector. The number of bits that can be used for embedding in each pixel is calculated based on the difference between that pixel and its neighbour. Thus, more bits are to be embedded in a pixel if its grey level is noticeably different from that of its neighboring pixel. This method, however, only considers differences in one dimension (either horizontal or vertical), which does not guarantee that all edges are identified.

II. LITERATURE SURVEY

Since the early stages of the human civilization, there has been an increased interest in information security, particularly the protection and privacy of communications (Pal & Pramanik, 2013). In modern societies, the excessive use of electronic data has made protection from malicious users more difficult (Grover & Mohapatra, 2013). Information hiding has emerged as an effective solution to this problem (Wu & Tsai, 2003; Wu, Lee, Tsai, Chu, & Chen, 2009).

Steganography is a kind of information hiding, in which a secret message is concealed within digital media (image, audio, video or text data) (Bassil, 2012; Cheddad, Condell, Curran, & Mc Kevitt, 2010). This property distinguishes steganography from other information security techniques (Modi, Islam, & Gupta, 2013). For instance, in cryptography, the message that needs to be transferred is encrypted to prevent intruders from understanding it. Hence, people can recognize the existence of the message, however it cannot be understood without decryption (Bassil, 2012; Cheddad et al., 2010; Verma, 2011).

As opposed to data concealing, steganalysis was initially designed to distinguish whether a given digital media has a secret message embedded in it. Moreover, some steganalysis methods may determine the type of steganography technique or estimate the length of the secret message (Li, He, Huang, & Shi, 2011). In term of security measurement, steganalysis has been utilized to evaluate the efficiency of steganography techniques from a security point of view (Geetha, Ishwarya, & Kamaraj, 2010). Steganalysis methods can be performed either by using image processing operation or by implementing methods that analyze the statistical features of the stego image structure, such as first order statistics (histogram) or second order statistics (correlations between pixels) (Cheddad et al., 2010). Ziou and Jafari suggested five requirements for steganalysis methods: (1) detection of the existence or absence of an embedded message in a given image, (2) identification of the steganographic method that have been used to hide the secret message, (3) approximation of the hidden message length or location and (4) extraction of the secret message (Ziou & Jafari, 2014).

In order to enhance the embedding efficiency, coding methods (mainly matrix encoding) have been introduced with the aim of minimizing the modifications created by embedding the message (Crandall, 1998; Hou, Lu, Tsai, & Tzeng, 2011).
In this paper, we propose a functional and simple image steganography method that is based on identifying edge locations on the cover image and incorporates an XOR coding function. The XOR function, which has a lower computation complexity compared to other matrix encoding methods, adds some security and reduces the distortion caused by embedding the message. Embedding in both spatial and wavelet transformed domains has been implemented.

III. RELATED WORK

Wavelet transform

Transform domain embedding methods provide a higher level of robustness, particularly when applying some image processing operations, compared to spatial domain methods. One of the most popular transforms is the Discrete Wavelet Transform (DWT) (Baby, Thomas, Augustine, George, & Michael, 2015; Thanikaiselvan et al., 2014). The Wavelet transform requires less computational cost compared to DCT and FFT (Fourier Transform) and offers sub-representations of the image that can be considered related to how the human visual system (HVS) perceives images. Generally, the wavelet transform allows embedding data in high frequency regions where the HVS cannot distinguish modifications compared to uniform regions with low frequency (Sharma & Swami, 2013). When DWT is performed to an image it is divided into 4 sub-bands: Low–Low (LL), Low–High (LH), High–Low (HL) and High–High (HH) frequency sub-bands, as shown in Fig. 1. The low frequency sub-band represents coarse information of pixels, while the high frequency sub-bands represent the edge information (Sharma & Swami, 2013). Hiding Information in the high frequency sub-bands (LH, HL, and HH) increases the robustness and ensures the visual quality, where the HVS is less sensitive to modifications in these sub-bands. The Integer Wavelet Transform (IWT) maps integers to integers and allows the construction of lossless compression to exactly retrieve the original data (Thanikaiselvan et al., 2014).

EDGE detection in steganography.

The utilization of edge detection in image steganography has been considered by a number of researchers. Due to sensitivity of the human eye to changes in smooth areas of the image compared to sharp contrast areas, it is logical to focus on sharp edges when embedding the secret message. However, the main obstacle to applying traditional edge detection methods in image steganography is the correct identification of edge pixels in the stego image S that need to exactly match the original edge pixels in the cover image C. This problem arises from the fact that the embedding process introduces minor changes to the stego image, which may make the produced stego image not identical with the cover image, and this can affect the message extraction process. Some of the existing edge-based steganography methods suggested certain solutions to overcome this problem. An edge image is created by performing Canny and fuzzy edge detection methods. The cover is then distributed into blocks of n pixels. The first pixel of each block is changed to represent the status of (n − 1) pixels if it is considered as edge pixel. LSB technique is used to embed x bits into non-edge pixels and y bits into edge pixels. The main drawback of this method is the unwanted modification that are created in the stego image because the method replaces (n − 1) bits from the first pixel of each block.

Coding theory.

Enhancing the embedding efficiency has been the focus of many steganography algorithms, as minimizing the amount of changes in the image when embedding (embedding rate) will enable the embedding of bigger messages. Crandall’s method utilizes the XOR function to conceal 2 bits of message into a block of 3 pixels. The F5 steganography algorithm, proposed by Westfeld (2001), is the first execution of matrix encoding to increase the capacity of embedding data as well as to minimize the change of DCT coefficients. This method has become well-known because it integrated the Hamming code with the transform domain implementation, which can embed k bits of the secret data in 2k − 1 cover bits by changing at most one bit only. As a result, this method has a limited embedding capacity, for example when k = 3, the method only embeds 3 bits in every 7 bits of the cover image.
IV. PROPOSED SYSTEM

The spatial domain algorithm
Identification of edges

The edge image generated by traditional edge detection methods is usually sensitive to changes in the original gray image, even if the changes are minor or not significant. This property limits the utilization of edge detection in steganography, as concealing the message would introduce some changes to the original image. Thus, embedding in pixels identified by one of the existing edge detection methods, such as Canny, cannot guarantee the identification of the exact edge intensities for the cover and stego images.

Here a simple new way to discover the edge (sharp) regions of the cover image, such that the two edge images generated using the original cover image and the stego image are identical is proposed. This will enable the correct extraction of the concealed message from the stego image. The algorithm starts by dividing the image into non-overlapping blocks that would be individually evaluated for inclusion of edges. The key idea behind preserving the same edge image is not to embed in the pixels that are used to calculate the edge strength, which are the outer pixels of the block.

Below are the detailed implementation steps.

Step 1: Divide the image C into non-overlapping blocks of the size n × n.

Step 2: Compute the absolute mean difference between the left and right columns of the block (magnitude of vertical edge). Repeat for horizontal, first diagonal and second diagonal edges. Fig. 3(a) shows the specific pixels used to calculate the edges for the 3 × 3 block.

Step 3: Find the maximum of the four values and assign it to e. If e > Th, then the block is considered to be an edge block, otherwise it is not an edge block. Construct E that contains the calculated e value of each of the edge blocks, and 0 for non-edge blocks. A binary edge image can also be constructed, which contains 1 for edge blocks and 0 for non-edge blocks.

Step 4: For the edge blocks, embed in the shaded 5 pixels.

Message embedding

The flow diagram of our proposed method is illustrated in Fig. 1. The data embedding process begins with reading the cover image and the secret message. A high threshold (96) is initially considered, which is then adjusted based on the number of pixels needed for embedding (identified by the generated binary edge image) and the message length, according to the following condition:

\[ \text{no. of edge pixels} \geq \left(4 \times \text{Message Length}/3\right) \]

For the given threshold value, if (no. of edge pixels ≥ (4 * Message Length)/3)) then the discovered area is enough to embed the secret message.

The embedding process is performed on the detected edge locations using the proposed XOR coding. This method partitions the index table into groups of four pixels and encodes three message bits into the pixels of each group. The XOR operation ensures that the secret message is concealed into the cover with minimum number of pixel changes. Thus, the three secret bits m1, m2, and m3 are embedded in the four LSBs p1, p2, p3, and p4 (one bit for each edge pixel) according to the following procedure:

1. Perform the following three XOR operations:
   \[ k1 = p1 \oplus p2 \]
   \[ k2 = p3 \oplus p4 \]
   \[ k3 = p1 \oplus p3 \]
2. To embed the three secret bits m1, m2, and m3, the three calculated bits k1, k2, and k3 are compared with the secret message bits m1, m2, and m3. The result of this comparison, which can take one of eight possibilities, determines which of the four bits p1, p2, p3, and p4 have to be modified. We will refer to the new four bits of the stego image as q1, q2, q3, and q4. The table indicates that embedding 3 message bits
into 4 cover bits will cause an average modification of 1.25 bits.

3. The threshold value should also be embedded, as it is needed by the extraction process. In this algorithm, the threshold value is embedded into the last pixel of the cover image.

**Message extraction**

The extraction process is easier and faster than the embedding process. Fig. 6 represents the flow diagram of the extraction process. It starts by retrieving the threshold value. The edge blocks of the stego image are then identified using the retrieved threshold, which will return the same edge image as the one obtained using the cover image. This will be followed by dividing the LSBs of the edge pixels into groups of four. Finally, for each of the four stego edge bits q1, q2, q3, and q4 the XOR operations listed below are used to retrieve three message bits m1, m2, and m3

\[
\begin{align*}
    m1 &= q1 \oplus q2 \\
    m2 &= q3 \oplus q4 \\
    m3 &= q1 \oplus q3
\end{align*}
\]

When considering any combination of m1, m2, m3, p1, p2, p3, and p4 to verify the embedding and extraction processes, one can find that the extraction process truly restores the original message.

**Embedding and extraction of n bits per coefficient of the Integer Wavelet Transform Domain**

The proposed Integer Wavelet Transform (IWT) based embedding process starts by converting the cover image to the frequency domain using IWT. Since the HVS is sensitive to small modification into the lower frequency band compared to the higher frequency, the secret data is embedded only in the high frequency sub-bands of the IWT domain to achieve a high robustness and imperceptibility results. In other words, data hiding is carried out in the three sub-bands HH, LH and HL (the LL sub-band is excluded). Similar to the spatial domain embedding, the XOR operation is also utilized here.

The embedding process begins with HH sub-band and identify the edge coefficients to start embedding with the strongest edges to the weakest edges. If the HH sub-band is not enough to embed the secret message, then the process moves to the LH sub-band, and then to the HL sub-band.

The implementation of the embedding process is explained in the following steps:

1. Read the cover image and the secret message.
2. Apply the First-Level of IWT on the cover image to decompose the cover image into four sub-bands (LL, HL, LH and HH).
3. Identify edge regions in the high frequency sub-bands (LL, HL, LH and HH). To increase the embedding payload of the wavelet transform method, n LSB from each edge coefficients are utilized in embedding. A higher threshold value (Th) is initialized, which is then decreased based on the number of coefficients needed for embedding and the message length. To identify the edge regions, HH sub-band is divided into non-overlapping blocks of 3 × 3 coefficients as shown in Fig. 3(b). For each block, the average value (avg) of the four non-shaded coefficients (Pi−1,j−1, Pi−1,j+1, Pi+1,j−1, Pi+1,j+1) is calculated. Finally, if the average value (avg) ≥ Threshold, the block is selected for embedding.

The extraction process begins with retrieving the threshold value to apply the edge detection method. Edge detection method is performed on the high frequency sub-bands by dividing the sub-band into non-overlapping blocks of size 3 × 3 to identify the edge area that has been utilized in the embedding process. For each of the three high frequency sub-band (HH, LH and HL), edge blocks are arranged into five groups according to the edge strength. Then, the XOR extraction operations are performed to retrieve n bits from each group.

**IV. EXPERIMENTAL RESULTS**

The Design is written in Verilog HDL Modules and has been successfully simulated and verified using Isim and synthesized using Xilinx ISE 13.2.
XOR embedding process hides two information signals (audio and ECG) into cover image. The proposed image steganography aims in developing a stego process, imperceptible and with high payload capacity. At first the scaled sampled are convolved using XOR coding to reduce size of information and to increase security of the process. The main contribution of the proposed method is introducing new and efficient edge detection algorithm using non-overlapping blocks that estimates the same edge intensities for the cover and stego images is determined in this project and has achieved better imperceptibility results than other popular steganography methods.

REFERENCES
1. Al-Dmour, H., Ali, N., & Al-Ani, A. (2015). An efficient hybrid steganography method based on edge adaptive and tree based parity check. In Multimedia modeling (mmm 2015) (pp. 1–12). Springer-Verlag.
2. Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. Procedia Computer Science, 46, 612–618.
3. Bandypadhyay, D., Dasgupta, K., Mandal, J., & Dutta, P. (2014). A novel secure image steganography method based on chaos theory in spatial domain. International Journal of Security, Privacy and Trust Management (IJSPTM), 3(1), 11–22.
4. Bas, P. & Furon, T. (2007). Bows-2. http://bows2.ec-lille.fr/.
5. Bassil, Y. (2012). Article: image steganography based on a parameterized canny edge detection algorithm. International Journal of Computer Applications., 60(4), 35–40.
6. Chan, C.-S., & Chang, C.-Y. (2010). Hiding data in parity check bit. In Proceedings of the 4th international conference on uniquitous information management and communication 2010 (icuime 2010). (pp. 359–363). ACM.
7. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: survey and analysis of current methods. Signal Processing, 90(3), 727–752.
8. Chen, W.-J., Chang, C.-C., & Le, T. (2010). High payload steganography mechanism using hybrid edge detector. Expert Systems with applications., 37(4), 3292–3301.
9. Crandall, R. (1998). Some notes on steganography. Posted on steganography mailing list.
10. Geetha, S., Ishawarya, N., & Kamaraj, N. (2010). Audio steganalysis with hausdorff distance higher order statistics using a rule based decision tree paradigm. Expert Systems with Applications., 37(12), 7469–7482.
11. Ghebleh, M., & Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898–1907.
Advanced computing, networking and security (adcons), 2013 (pp. 238–242). IEEE.
12. Hou, C.-L., Lu, C., Tsai, S.-C., & Tzeng, W.-G. (2011). An optimal data hiding scheme with tree-based parity check. IEEE Transactions on Image Processing, 20(3), 880–886.
13. Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. International Journal of advanced Science and Technology. Vol., 54, 113–123.
14. Ioannidou, A., Halkidis, S. T., & Stephanides, G. (2012). A novel technique for image steganography based on a high payload method and edge detection. Expert Systems with Applications., 39(14), 11517–11524.
15. Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications., 41(14), 6123–6130.
16. Lee, Y.-P., Lee, J.-C., Chen, W.-K., Chang, K.-C., Su, I.-J., & Chang, C.-P. (2012). Highpayload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences, 191, 214–225.
17. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing. Vol., 2(2), 142–172.
18. Li, B., Huang, J., & Shi, Y. Q. (2008). Textural features based universal steganalysis. In Electronic imaging 2008 (pp. 1201–1212). International Society for Optics and Photonics.
19. Li, L., Luo, B., Li, Q., & Fang, X. (2009). A color images steganography method by multiple embedding strategy based on sobel operator. In Multimedia information networking and security, 2009. mines’09. international conference on: 2 (pp. 118–121). IEEE.
