Implementation of Xor and Edge Identification Method in Steganography

Permella Abishai Jasper, D.Jayanthi, N.Arun Vignesh, K.G.Maheshwari,

Abstract: In this paper, a novel imagesteganography 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 stegno 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 stegno 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 Spatial and time domain methods, Transform domain methods and fractal coding methods are the several methods of embedding data. These methods hide / embed information in different types of media such as video, audio, image, text, etc. Varieties of different file formats, digital images are considered the most popular type 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.

Manuscript published on 30 September 2019.
* Correspondence Author (s)
Permella Abishai Jasper, Dept. of E.C.E, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad.
D.Jayanthi, Dept. of E.C.E, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad
N.Arun Vignesh, Dept. of E.C.E, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad

The secret message called payload could be plain text, an image, a video file or an audio. Steganography 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 stegano 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 neighbouring 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 stegno 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 stegano graphic 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).

Table 1
Differentiation between image steganography schemes in spatial and transform doamins.

Domain	Advantages	Disadvantages
Spatial Domain	High embedding capacity Shorter computational time High controllable imperceptibility	Vulnerable to geometric attacks.
Transform Domain	Robustness against attacks such as Geometric attacks and compression	High computational time Limited embedding capacity Lower controllable imperceptibility

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 useful and basic picture steganography technique that depends on recognizing edge areas on the cover picture and joins a XOR coding capacity. The XOR work, which has a lower calculation multifaceted nature contrasted with other grid encoding techniques, includes some security and lessens the bending caused by installing the message. Implanting in both spatial and wavelet changed spaces has been executed.

III.RELATED WORK

Wavelet transform

Change space implanting techniques give a larger amount of strength, especially while applying some picture handling activities, contrasted with spatial area strategies. A standout amongst the most mainstream changes is the Discrete Wavelet Transform (DWT) (Baby, Thomas, Augustine, George, and Michael, 2015; Thanikaiselvan et al., 2014). The Wavelet change requires less computational expense contrasted with DCT and FFT (Fourier Transform) and offers sub-portrayals of the picture that can be viewed as identified with how the human visual framework (HVS) sees pictures. By and large, the wavelet change permits inserting information in high recurrence districts where the HVS can't recognize alterations contrasted with uniform areas with low recurrence (Sharma and Swami,2013). At the point when DWT is performed to a picture it is separated into 4 sub-groups: Low– Low (LL), Low– High (LH), High– Low (HL) and High– High (HH) recurrence sub-groups, as appeared in Fig. 1. The low recurrence sub-band speaks to coarse data of pixels, while the high recurrence sub-groups speak to the edge data (Sharma and Swami, 2013).

Concealing Information in the high recurrence sub-groups (LH, HL, and HH) builds the vigor and guarantees the visual quality, where the HVS is less delicate to alterations in these sub-groups. The Integer Wavelet Transform (IWT) maps whole numbers to whole numbers and enables the development of lossless pressure to precisely recover the first information (Thanikaiselvan et al., 2014).

EDGE detection in steganography

The usage of edge identification in picture steganography has been considered by various scientists. Because of affectability of the human eye to changes in smooth regions of the picture contrasted with sharp difference zones, it is sensible to concentrate on sharp edges while implanting the mystery message. In any case, the primary snag to applying conventional edge discovery techniques in picture steganography is the right ID of edge pixels in the stegno picture S that need to precisely coordinate the first edge pixels in the cover picture C. This issue emerges from the way that the implanting procedure acquaints minor changes with the stegno picture, which may make the created stegno picture not indistinguishable with the cover picture, and this can influence the message extraction process.

A portion of the current edge-based steganography techniques proposed certain answers for conquer this issue. An edge picture is made by performing Canny and fluffy edge recognition strategies. The cover is then conveyed into squares of n pixels. The principal pixel of each square is changed to speak to the status of $(n - 1)$ pixels on the off chance that it is considered as edge pixel. LSB strategy is utilized to insert x bits into non-edge pixels and y bits into edge pixels. The principle downside of this strategy is the undesirable adjustment that are made in the stegno picture in light of the fact that the technique replaces $(n - 1)$ bits from the main pixel of each square.

Coding theory

Upgrading the implanting productivity has been the focal point of numerous steganography calculations, as limiting the measure of changes in the picture while inserting (installing rate) will empower the installing of greater messages. Crandall's technique uses the XOR capacity to cover 2 bits of message into a square of 3 pixels. The F5 steganography calculation, proposed by Westfeld (2001), is the principal execution of grid encoding to build the limit of installing information and in addition to limit the difference in DCT coefficients. This strategy has turned out to be outstanding on the grounds that it incorporated the Hamming code with the change area execution, which can install k bits of the mystery information in $2k - 1$ cover bits by changing at most one piece as it were. Accordingly, this technique has a constrained inserting limit, for instance when $k = 3$, the strategy just implants 3 bits in each 7 bits of the cover picture.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV.PROPOSED SYSTEM

The spatial domain algorithm

Identification of edges:

The edge picture created by conventional edge identification techniques is normally delicate to changes in the first dark picture, regardless of whether the progressions are minor or not huge

This property restrains the use of edge location in steganography, as covering the message would acquaint a few changes with the first picture. Along these lines, implanting in pixels distinguished by one of the current edge discovery strategies, for example, Canny, can't ensure the ID of the correct edge powers for the cover and stegno pictures. Here a basic better approach to find the edge (sharp) locales of the cover picture, to such an extent that the two edge pictures created utilizing the first cover picture and the stegno picture are indistinguishable is proposed. This will empower the right extraction of the disguised message from the stegno picture. The calculation begins by partitioning the picture into non-covering hinders that would be separately assessed for incorporation of edges. The key thought behind protecting a similar edge picture isn't to insert in the pixels that are utilized to figure the edge quality, which are the external pixels of the

square.Below are the detailed implementation steps.Sources of info: Cover picture (C), square size (n × n, which is required here to be 3 × 3), limit(Th runs somewhere in the range of 4 and 96)Yield: edge picture with edge greatness (E) Step 1: Divide the picture C into non-covering squares of the size n × n.

Step 2: Compute without a doubt the mean distinction between the left and right segments of the square (greatness of vertical edge). Rehash for even, first slanting and second corner to corner edges. Fig. 3(a) demonstrates the explicit pixels used to compute the edges for the 3 × 3 square.

Stage 3: Find the most extreme of the four qualities and allot it to e. On the off chance that e > Th, the square is viewed as an edge square, else it's anything but an edge square. Build E that contains the determined estimation of every one of the edge squares, and 0 for non-edge squares. A paired edge picture can likewise be built, which contains 1 for edge squares and 0 for non-edge squares.

Stage 4: For the edge squares, install in the shaded 5 pixels.

Message installing:

The stream graph of our proposed strategy is shown in Fig. 1. The information installing process starts with perusing the cover picture and the mystery message. A high edge (96) is at first considered, which is then balanced

dependent on the quantity of pixels required for installing (distinguished by the produced double edge picture) and the message length, as per the accompanying condition:

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

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:

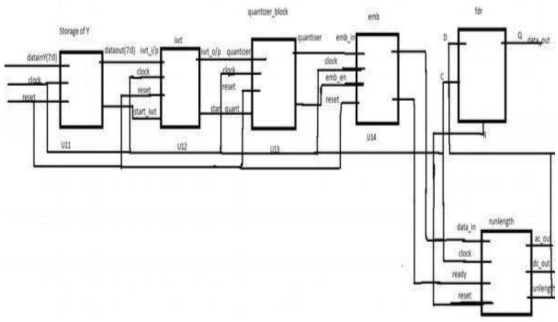


Fig. 1. Block Diagram of message Embedding For the given threshold value, if (no. of edge pixels=(4 ∗

Message Length)/3)) then the

discovered area is enough to embed the secret message.

The embedding system is performed on the perceived edge regions using the proposed XOR coding. This procedure sections the document table into social events of four pixels and encodes three message bits into the pixels of each get-together.

The XOR action ensures that the riddle message is masked into the cover with slightest number of pixel changes. In this way, the three puzzle bits m1, m2, and m3 are embedded in the four LSBs p1, p2, p3, and p4 (one piece for each edge pixel) as demonstrated by the going with methodology.

1. Play out the accompanying three XOR activities
   $k1 = p1 \oplus p2$
   $k2 = p3 \oplus p4$
   $k3 = p1 \oplus p3$
2. To embed the three puzzle bits m1, m2, and m3, the three decided bits k1, k2 and k3 are differentiated and the secret message bits m1, m2, and m3. The delayed consequence of this examination, which can take one of eight possible results, makes sense of which of the four bits p1, p2, p3, and p4 must be modified.

We will imply the new four bits of the stegno picture as q1, q2, q3, and q4. The table demonstrates that implanting 3 message bits1. Play out the going with three XOR activities

$k1 = p1 \oplus p2$

$k2 = p3 \oplus p4$

$k3 = p1 \oplus p3$.

To embed the three riddle bits m1, m2, and m3, the three decided bits k1, k2 and k3 are differentiated and the puzzle message bits m1, m2, and m3. The result of this relationship, which can take one of eight possible results, makes sense of which of the four bits p1, p2, p3, and p4 must be modified. We will insinuate the new four bits of the stegno picture as q1, q2, q3, and q4. The table exhibits that introducing 3 message bitsinto 4 cover bits will cause a normal alteration of 1.25 bits.

3. The limit esteem ought to likewise be implanted, as it is required by the extraction procedure. In this calculation, the edge esteem is installed into the last pixel of the cover picture.

Retrieval Number: F13930986S319/2019©BEIESP
DOI:10.35940/ijeat.F1393.0986S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Message extraction:

The extraction procedure is simpler and quicker than the inserting procedure. Fig. 6 speaks to the stream graph of the extraction procedure. It begins by recovering the limit esteem. The edge squares of the stegno picture are then recognized utilizing the recovered edge, which will restore a similar edge picture as the one got utilizing the cover picture. This will be trailed by isolating the LSBs of the edge pixels into gatherings of four.

At last, for every one of the four stegno edge bits q1, q2, q3, and q4 the XOR activities recorded beneath are utilized to recover three message bits m1, m2, and m3

$$m1 = q1 \oplus q2$$
$$m2 = q3 \oplus q4$$
$$m3 = q1 \oplus q3$$

While thinking about any mix of m1, m2, m3, p1, p2, p3, and p4 to confirm the inserting and extraction forms, one can find that the extraction procedure really re-establishes the first message. Inserting and extraction of n bits per coefficient of the Integer Wavelet Transform Domain.The proposed Integer Wavelet Transform (IWT) based inserting process begins by changing over the cover picture to the recurrence area utilizing IWT. Since the HVS is delicate to little alteration into the lower recurrence band contrasted with the higher recurrence, the mystery information is inserted just in the high recurrence sub-groups of the IWT area to accomplish a high power and intangibility results.

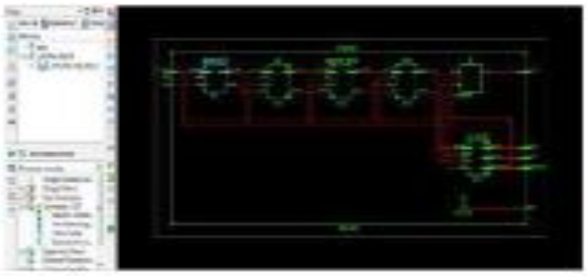
At the end of the day, information stowing away is completed in the three sub-groups HH, LH and HL (the LL sub-band is avoided). Like the spatial space implanting, the XOR task is likewise used here.The installing procedure starts with HH sub-band and distinguish the edge coefficients to begin implanting with the most grounded edges to the weakest edges. In the event that the HH sub-band isn't sufficient to implant the mystery message, at that point the procedure moves to the LH sub-band, and after that to the HL sub-band. The usage of the installing procedure is clarified in the accompanying advances.

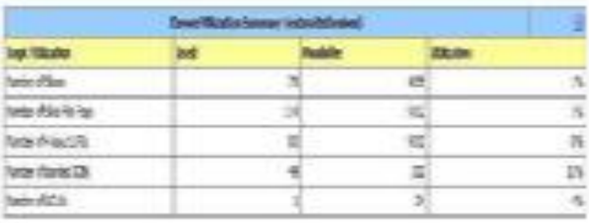
Read the cover image and the secret message and applied the First-Level of IWT on the cover image to decompose the cover image into four sub-bands (LL, HL, LH and HH).Identified edge areas in the high recurrence sub-groups (LL, HL, LH and HH). To build the installing payload of the wavelet change strategy, n LSB from each edge coefficients are used in inserting. A higher limit esteem (Th) is instated, which is then diminished dependent on the quantity of coefficients required for installing and the message length. To distinguish the edge areas, HH sub-band is partitioned into non-covering squares of 33 coefficients as shown in Fig. 3(b). For each block, the average value (avg) of the four non-shaded coefficients ($P_{i-1,j-1}$, $P_{i-1,j+1}$, $P_{i+1,j-1}$, $P_{i+1,j+1}$) is calculated. Finally, if the average value (avg) ≥ Threshold, the block is selected for embedding.The extraction procedure starts with recovering the limit an incentive to apply the edge identification technique.

Edge location strategy is performed on the high recurrence sub-groups by separating the sub-band into non-covering squares of size 3 × 3 to distinguish the edge zone that has been used in the installing procedure. For every one of the three high recurrence sub-band (HH, LH and HL), edge squares are organized into five gatherings as per the edge quality. At that point, the XOR extraction activities are performed to recover n bits from each gathering.

V.EXPERIMENTAL RESULTS:

The Design is written in Verilog HDL Modules and has been successfully simulated and verified using modelsim and synthesized using Xilinx ISE 13.2





Retrieval Number: F13930986S319/2019©BEIESP
DOI:10.35940/ijeat.F1393.0986S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

VI.CONCLUSION:

XOR installing process conceals two data signals (sound and ECG) into cover picture. The proposed picture steganography points in building up astegno procedure, indistinct and with high payload limit. At first the scaled tested are convolved utilizing XOR coding to decrease size of data and to build security of the procedure. The primary commitment of the proposed strategy is presenting new and effective edge recognition calculation utilizing non-covering obstructs that assesses a similar edge forces for the cover and stegno pictures is resolved in this venture and has accomplished preferred intangibility results over other prominent steganography strategies

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. Bandyopadhyay, 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
7. conference on uniquitous information management and communication 2010 (icuimc 2010). (pp. 359–363). ACM.
8. 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.
9. 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.
10. Crandall, R. (1998). Some notes on steganography. Posted on steganography mailing list.
11. Geetha, S., Ishwarya, 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.
12. Ghebleh, M., & Kanso, A. (2014). A robust chaotic algorithm for digital image steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6), 1898– 1907.
13. Grover, N., & Mohapatra, A. (2013). Digital image authentication model based on edge adaptive steganography. In 2nd international conference on Advanced computing, networking and security (adcons), 2013 (pp. 238–242). IEEE.
14. 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.
15. Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. International Journal of advanced Science and Technology. Vol., 54, 113–123.
16. 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.
17. Kanan, H. R., & Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable
18. visual image quality based on a genetic algorithm. Expert Systems with Applications., 41(14), 6123–6130.
19. 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
20. 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.
21. 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.
22. 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,
23. 2009. mines'09. international conference on: 2 (pp. 118–121). IEEE.

.