Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Reversible Data Hiding for Lossless Image and Data Recovery

Bhagyashri S. Jatte, Asst. Prof. A.S. Deshpande
Electronics & Comm. Department
JSPM's Imperial College of engineering Wagholi
University of Pune, Maharashtra, India

Abstract— presently, there are a unit numerous issues of information hacking. There are a unit type of techniques to stay up info security. This paper presents a reversible knowledge concealment using a replacement chaotic rule for image cryptography mistreatment numerous ways in which. this method proposes the development of protection system throughout that the initial cowl is also losslessly recovered. once image cryptography, info hider will conceal the secrete info into the careful coefficients that unit of measurement reserved before cryptography. we tend to tend to review sample cases where watermarking has been deployed. Although cryptography achieves positive security effects, they produce the messages unreadable and meaningless . the knowledge concealment technique uses the accommodative LSB replacement rule for concealing secrete message bits into the encrypted image. throughout this planned technique, we tend to tend to engraft info by reserving house before cryptography with a standard RDH rule. The planned technique can extract the additional info and recover the initial image content with none error and offers higher performance over other ways.

Keywords— Encrypted image, new chaotic system, reversible info concealment, image recovery, least vital bit.

I. INTRODUCTION

The word cryptography comes from the Greek words κρυπτο (hidden) and γραφη (writing). Interestingly enough, cryptography is that the art of hidden writing. Generally, of us study of cryptography as a result of the art of mangling knowledge into apparent unintelligibility in Associate in Nursing passing manner allowing secret technique of unmingling. The essential service provided by cryptography is that the power to send knowledge between participants in Associate in Nursing passing methodology that forestalls others from reading it. Throughout this paper, we\'ll discuss on the kind of cryptography that is supported representing knowledge as numbers and mathematically manipulating those numbers. Info concealment is also a form of steganography, embeds info into digital image or audio for the aim of identification and copyright. Several constraints a bit like the number of data to be hidden, the need for invariability of these info have a bearing on this methodology. To a lower place this conditions, a symbol is subject to distortions, e.g., lossy compression. We tend to tend to explore every ancient and novel techniques for addressing the data-hiding methodology and live these techniques in light-weight of three applications: copyright protection, tamper proofing, and augmentation info embedding.

In recent years, many RDH techniques have emerged in recent years. Fridrich et al. [1] created a general framework for RDH. By initial extracting compressible choices of original cowl thus pressure them losslessly, spare space is also saved for embedding auxiliary info. A further well-liked technique relies on distinction enlargement (DE) [3], throughout that the excellence of each component cluster is enlarged , e.g., magnified by 2, then the little quantity vital bits (lsbs) of the excellence unit of measurement all-zero and could be used for embedding messages. Another promising strategy for RDH is bar graph shift (HS) [4], throughout that space is saved for info embedding by shifting the bins of bar graph of gray values.

A. Choices of data concealment

1. The host signal need to be non objectionally degraded and thus the embedded info need to be minimally perceptible. (The goal is for the knowledge to remain hidden. As any magician will tell you, it's potential for one issue to be hidden whereas it remains in plain sight; you simply keep the person from looking at it. We'll use the words hidden, inaudible, imperceivable, associated invisible to mean that Associate in nursing observer does not notice the presence of the knowledge, albeit they are perceptible.)
2. The embedded info need to be directly encoded into the media, rather than into a header or wrapper, so as that the knowledge keep intact across varied record formats.
3. Asymmetrical secret writing of the embedded info is fascinating, since the aim of data concealment is to remain the knowledge at intervals the host signal, but not basically to create the knowledge powerful to access.
4. Error correction coding1 need to be accustomed guarantee info integrity. It's inevitable that there will be some degradation to the embedded information once the host signal is modified.

5. The embedded information need to be self-clocking or each that means re-entrant. This ensures that the embedded info is also recovered once exclusively fragments of the host signal unit of measurement out there, e.g., if a line is extracted from associate interview, info embedded at intervals the section is also recovered. This feature to boot facilitates automatic decoding of the hidden information, since there is not any need to be compelled to envision the initial host signal.

B. Applications of information concealment

Trade-offs exists between the quantity of embedded information and thus the degree of immunity to host signal Modification. By confining the degree of host signal degradation, a data-hiding technique can operate with either high embedded rate, or high resistance to modification, but not every. Reciprocally can increase, the other ought to decrease. Whereas this might be shown mathematically for a couple of data-hiding systems sort of a selection spectrum, it seems to hold true for all data-hiding systems. In any system, you will trade metric for robustness by exploiting redundancy. The quantity of embedded info and thus the degree of host signal modification vary from application to application. Consequently, different techniques unit of measurement used for numerous applications. Several prospective applications of data concealment unit of measurement mentioned throughout this section. Associate application that wants a nominal amount of embedded info is that the position of a digital water mark. The embedded info unit of measurement accustomed place a symbol of possession at intervals the host signal, serving constant purpose as associate author's signature or a company emblem. Since the info is of a vital nature and thus the signal would possibly face intelligent and intentional makes a shot to destroy or deduct it, the key writing techniques used ought to be proof against a decent quite potential modifications. A second application for info concealment is tamper-proofing. It's accustomed indicate that the host signal has been modified from its authored state. Modification to the embedded info indicates that the host signal has been changed in a very means. A third application, feature location, wants further info to be embedded. Throughout this application, the embedded info unit of measurement hidden in specific locations among an image. It permits one to identify individual content choices, e.g., the name of the person on the left versus the right aspect of an image. Typically, feature location info are not subject to intentional removal. However, it's expected that the host signal can be subjected to a specific degree of modification, e.g., footage unit of measurement routinely modified by scaling, cropping, and tone scale improvement. As a result, feature location info concealment techniques ought to be proof against geometrical and non-geometrical modifications of variety signal.

II. OTHER WAYS FOR INFORMATION CONCEALMENT

A. Reversible info Embedding using a distinction enlargement

Throughout this method, we tend to generalize the plan of action in our previous paper using a decompression rule as a result of the key writing theme for embedding info and prove that the generalized codes can reach the rate–distortion bound as long as a result of the compression rule reaches entropy. By the planned binary codes, we tend to enhance three rdh schemes that use binary feature sequence as covers, i.e., associate as theme for spatial footage, one theme for jpeg footage, and a pattern substitution theme for binary footage. The experimental results show that the novel codes can significantly reduce the embedding distortion.

Data-Embedding Algorithm[3].

In a digital image, one can select some expandable distinction values of pixels, and engraft one bit into each of them. To extract the embedded info and restore the initial values, the decoder should apprehend that distinction values area unit chosen for the primary State. To facilitate it, we\'d wish to engraft such location data, such the decoder could access and use it for decoding. For this purpose, we\'ll turn out and engraft a location map, that contains things data of all chosen expandable distinction values. What\'s additional, the Decipher should apprehend where (from that distinction values) to collect and decipher things map. Once the primary State, the enlarged distinction value might not be expandable. On the decoder aspect, to examine whether or not is expandable does not tell whether or not or not the initial has been chosen for the primary State throughout embedding. As we know, the enlarged distinction value is changeable, that the decoder could examine each changeable distinction value. Like many image method techniques, the encoder serves for the decoder, at intervals the primary State technique, the encoder will take all changeable distinction values as a result of the embedding house, so as that the Decipher will use constant info to decipher. Throughout info embedding, we'll modify all changeable distinction values, by either adding a greenhorn LSB (via the DE) or modifying its LSB. To confirm a certain recovery of the initial image, we'll to boot engraft the initial values of those modified LSBS. In brief, the date-embedding DE rule consists of six steps: conniving the excellence values, partitioning distinction values into four sets, creating a location map, assortment original LSB values, info embedding by replacement, and eventually associate inverse number make over.

Reversible info embedding has drawn numerous interest recently. Being reversible, the initial digital content is also completely restored. Jun Tian [3], we tend to tend to gift a very distinctive reversible info embedding technique for digital footage. We tend to tend to explore the redundancy in digital footage to appreciate really high embedding capability, and keep the distortion low. Throughout this paper, we've bestowed a simple and economical reversible date-embedding technique for digital footage. We tend to tend to explored the redundancy at intervals the digital content to appreciate quality. every the payload capability limit and thus the visual quality of embedded footage unit of measurement among the foremost effective at intervals the literature.

Fig. 1. Reversibly embedded "Lena," with a 39 566 bits payload[3].

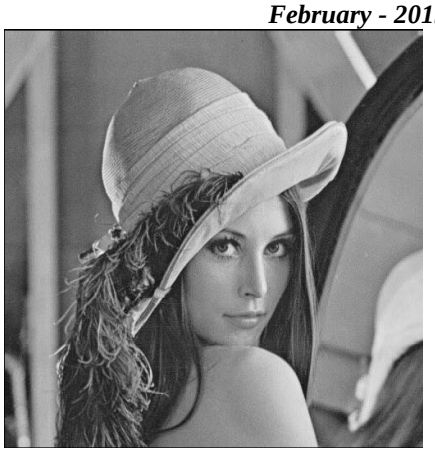

Fig. 2. Reversibly embedded "Lena," with a 141 493 bits payload[3].

Fig. 3. Reversibly embedded "Lena," with a 516 794 bits payload. [3].

The performance of a reversible data-embedding rule are often measured by the subsequent.

1) Payload capability limit: what\'s the supreme quantity of data are often embedded?
2) Visual quality: however is that the visual quality on the embedded image?
3) Complexity: what\'s the rule complexity?

The motivation of reversible knowledge embedding is distortion-free data embedding. Though unobservable, embedding some data can inevitably modification the initial content. Even a awfully slight modification in constituent values might not be fascinating, particularly in sensitive representational process, like military knowledge and medical knowledge. In such a state of affairs, as of data is very important. Any modification can have an effect on the intelligence of the image, and therefore the access to the initial, information is usually needed.

Algorithm flow:

1). Reversible knowledge embedding
   I) Reversible whole number rework
   Ii) Expandable and Changeable distinction Values
   Iii) Data-Embedding rule
2) Expandable distinction value selection
3) Multiple-Layer Embedding:
4) True Fidelity at half Resolution

Our methodology are often applied to digital audio and video furthermore. We tend to calculate the variations of neighbor constituent values, and choose some distinction values for the distinction enlargement (DE). The initial content restoration information, a message authentication code, and extra knowledge (which can be any knowledge, like date/time information, auxiliary knowledge, etc.) Can all be embedded into the distinction values. During this paper we are going to take into account grayscale pictures solely. For color pictures, there area unit many choices. One will de-correlate the dependence among completely different color parts by a reversible color conversion rework, then reversibly insert the info within the de-correlated parts. Or one will reversibly insert every color part one by one.

A. Reversible data Embedding using histogram modification

This rule utilizes the zero or the minimum points of the bar graph of a picture and slightly modifies the constituent grayscale values to insert data into the image. It will insert additional data than several of the prevailing reversible knowledge concealment algorithms. It's proved analytically and shown by experimentation that the height signal-to-

noise (PSNR) of the marked image generated by this methodology versus the initial image is bound to be higher than 48db. This edge of PSNR is far over that of all reversible data concealment techniques according within the literature. The computational complexity of our proposed technique is low and the execution time is short. The algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in coreldraw database. Experimental results and performance comparison with other reversible data hiding schemes are presented to demonstrate the validity of the proposed algorithm.

Algorithm[4]

We first use the "Lena" image as an example to illustrate our algorithm. Then the dada embedding and extracting of the proposed algorithm are presented in terms of pseudo code. Finally, some important issues including data embedding capacity are addressed. For a given grayscale image, say, the Lena image 512× 512× 8 , we first generate its histogram as shown in Fig. 1.

Illustration of Embedding Algorithm Using an Example With One Zero Point and One Peak Point[4]

1) In the histogram, we first find a *zero point*, and then a *peak point*. A zero point corresponds to the grayscale value which no pixel in the given image assumes, e.g., as shown in Fig.4. A peak point corresponds to the grayscale value which the maximum number of pixels in the given image assumes, e.g., as shown in Fig. 4. For the sake of notational simplicity, only one zero point and one peak point are used in this example to illustrate the principle of the algorithm. The objective of finding the peak point is to increase the embedding capacity as large as possible since in this algorithm, as shown below, the number of bits that can be embedded into an image equals to the number of pixels which are associated with the peak point. The implementation of the proposed algorithm with two and more pairs of zero and peak points is further discussed later in this section.

2) The whole image is scanned in a sequential order, say, row-by-row, from top to bottom, or, column-by-column, from left to right. The grayscale value of pixels between 155 (including 155) and 254 (including 254) is incremented by "1." This step is equivalent to shifting the range of the histogram, [155 254], to the right-hand side by 1 unit, leaving the grayscale value 155 empty. 3) The whole image is scanned once again in the same sequential order. Once a pixel with grayscale value of 154 is encountered, we check the to-be-embedded data sequence. If the corresponding to-be-embedded bit in the sequence is binary "1," the pixel value is incremented by 1. Otherwise, the pixel value remains intact. (Note this step may be included into Step 2, described above.

(a) (b)

Fig.4. lena image (a) original and (b) marked (PSNR =48.2) [4]

III. DISCUSSION AND ANALYSIS

Now a days the protection of image data from unauthorized access is important. Image encryption plays a significant role in field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. Reversible data hiding in encrypted image is most commonly method used for better security of data. To maintain the quality of image and to reduce the noise we use Discrete cosine transform (DCT). Data hiding is one of the major field which improves several parameters day by day, researchers continually exploring new algorithms to enhance the quality of image even after hiding a major amount of data in it, here is to hide data in images using reversible data hiding algorithm with the use of DCT to match the closest data hiding pixel for every symbol to be hide. There are two methods: Closest element approach and random sequence approach. With the help of these two approaches the closest data hiding is to be match. Basically the purpose of this method is to find out the noisy pixels and then hide the data in it and recover it by decryption process and calculate the error rate to compare the decrypted data with original one

IV. CONCLUSIONS

This paper presented the recent research work in the field of steganography deployed in spatial, transform, and compression domains of digital images. In this paper, we have presented a simple and efficient reversible date embedding method for digital images. We explored the redundancy in the digital content to achieve reversibility. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature. The p second

reversible data hiding algorithm has been applied to many different types of images, including some commonly used images, medical images, and all of the 1096 images in the CorelDraw database, and has always achieved satisfactory results, thus demonstrating its general applicability. Here, the results of different kinds of images with different typical histogram distribution are presented. In all experiments, two pairs of maximum and minimum points are used in data embedding and extraction. Transform domain techniques make changes in the frequency coefficients instead of manipulating the image pixels directly, thus distortion is kept at minimum level and that's why they are preferred over spatial domain techniques. But when it comes to embedding capacity, spatial domain techniques give better results. However, there exists a trade-off between the image quality and the embedding capacity. Hiding more data results directly into more distortion of the image. In recent years, some researchers have concentrated on embedding secret data into the compression codes of images. Such need arises keeping in mind the bandwidth requirements. For instance terrorists may use this technique for their secret secure communication or antivirus systems can be fooled if viruses are transmitted in this way. However, it is evident that steganography has numerous useful applications and will remain the point of attraction for researchers.

REFERENCES

[1] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[2] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in Proc 13th Information Hiding (IH'2011), *LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.

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

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

[5] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[6] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.

[7] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.

[8] L. Luo *et al.*, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.

