A Framework for Multimedia Data Hiding (Security)

Owoade A. Akeem[†], **Onifade O. F. W**[††], **Okesola J. Olatunji**[†], **Abimbola B. Latifat**[†]

[†] Tai Solarin University of Education, Ijebu Ode, Department of Computer Science
[††]University of Ibadan, Department of Computer Science

Abstract
With the proliferation of multimedia data such as images, audio, and video, robust digital watermarking and data hiding techniques are needed for copyright protection, copy control, annotation, and authentication. While many techniques have been proposed for digital color and grayscale images, not all of them can be directly applied to binary document images. The difficulty lies in the fact that changing pixel values in a binary document could introduce Irregularities that is very visually noticeable. We have seen but limited number of papers proposing new techniques and ideas for document image watermarking and data hiding. In this paper, we present an overview and summary of recent developments on this important topic, and discuss important issues such as robustness and data hiding capacity of the different techniques.

Keywords:
Data hiding; watermarking; binary images; document images; authentication; copyright control

1. Introduction

The digital information revolution has brought about profound changes in our society and our lives. The many advantages of digital information have also generated new challenges and new opportunities for innovation. Along with powerful software, new devices, such as digital camera and camcorder, high quality scanners and printers, digital voice recorder, MP3 player and PDA, have reached consumers worldwide to create, manipulate, and enjoy the multimedia data. Internet and wireless network offer ubiquitous channels to deliver and to exchange information. The security and fair use of the multimedia data, as well as the fast delivery of the multimedia content to a variety of end users/devices with guaranteed QoS are important yet challenging topics. The solutions to these problems will not only contribute to our understanding of this fast moving complex technology, but also offer new economic opportunities to be explored [1]. With the ease of editing and perfect reproduction in digital domain, the protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) become important concerns. Digital watermarking and data hiding, schemes to embed secondary data in digital media, have made considerable progress in recent years and attracted attention from both academia and industry. Techniques are proposed for a variety of applications, including ownership protection, authentication, access control, and annotation. Data hiding is also found useful as a general tool to send side information in multimedia communication for achieving additional functionalities or enhancing performance. Imperceptibility, robustness against moderate processing such a compression, and the ability to hide many bits are the basic but rather conflicting requirements for many data hiding applications. In addition, a few other important problems encountered in practice, such as the uneven embedding capacity for image/video and the perceptual models for binary images, have received little attention in literature. The work included in this paper intend to contribute towards the understanding of multimedia data hiding, addressing both theoretical and practical aspects and tackling both design and attack problems. Practical imaging applications range from famous works of art, to bank checks, and medical images. Reliable methods for copyright protection, copy control, annotation, and authentication are therefore needed. A variety of digital watermarking and data hiding techniques have been proposed for such purposes. However, most of the methods developed today are for grayscale and color images [2], where the gray level or color value of a selected group of pixels is changed by a small amount without causing visually noticeable artifacts. These techniques cannot be directly applied to binary document images where the pixels have either a 0 or a 1 value. Arbitrarily changing pixels on a binary image causes very noticeable artifacts (see Figure 1 for an example). A different class of embedding techniques must therefore be developed. These would have important applications in a wide variety of document images that are represented as binary foreground and background; e.g. bank checks, financial instruments, legal documents, driver licenses, birth certificates, digital books, engineering maps, architectural drawings, road maps. Until recently, there has been little work on watermarking and data hiding techniques for binary document images.

Manuscript received December 5, 2011
Manuscript revised December 20, 2011

Figure 1. Effect of Arbitrarily Changing Pixel Values on a Binary Image

2. Related Work/Literature

The ideas of information hiding can be traced back to a few thousand years ago; simply obscuring the content of a message by encryption is not always adequate in practice. For the last two decades, digital data hiding has received a great deal of attention from the scientific community. Remarkable research efforts have been invested in recent years, trying to export novel and applied real world engineering applications. Data hiding embeds information into digital media for the purpose of identification, authentication, and copyright protection. Data hiding represents a class of processes used to embed data, such as copyright information, into various forms of media e.g. video, image, audio, and text with a minimum amount of perceivable degradation to the "host" signal; i.e., the hidden data should be invisible and inaudible to an observer.

This proposal is intended to bring together a diversity of international researchers, experts and practitioners who are currently working in the area of digital data hiding and its applications:

Liu et al, [6] presents an adaptive DE-based reversible steganographic scheme with bilinear interpolation and simplified location map. Authors apply kernel of bilinear interpolation to effectively improve the number of the embeddable location. Also, it is used for the existing adaptive embedding rule to improve the embedding payload control capability in single layer embedding. Their proposed scheme presents better visual quality of the stego-image and carries larger embedding payload than some other DE schemes published in the current literature.

Zhao et al, [7] confirms the truth that the current reversible data hiding algorithms are detectable. Authors show that the horizontal difference histogram of natural image is significantly altered after being embedded secret message. Furthermore, the difference between the horizontal and the vertical difference histogram of natural image is much less than that of the watermarked image. Experimental analysis demonstrates that the approach of Zhao et al. is effective and more efficient than the already published schemes.

Another paper by Yan et al [Jan, 2011] . presents a MPEG-1 Layer 111 (MP3) audio CODEC based steganographic method to embed secret message during encoding. Their method is designed under the restrictions of the MP3 compression standard without any modifications or additions to the existing standard. The author experimentally show that their method can provide much higher capacity than other approaches, while satisfying the low distortion and security requirements for steganography on MP3 audios.

Vivekananda et al, [10] proposes a new audio watermarking algorithm based on singular value decomposition and modulation quantization. The watermarks produced by this algorithm are highly imperceptible that can be blindly extracted and have low error probability rates. The results show its robustness against attacks like adaptive white Gaussian noise, MP3 compression, resampling, etc.

Fallahpour and Megias ,2011 present an audio watermarking algorithm by incorporating the high frequency band of the wavelet decomposition. In their work, the high frequency band is divided into frames to alter the wavelet samples. The results of their study show that their technique has a very high capacity and is robust against common audio signal processing methods.

Lien and Lin proposes a reversible data hiding method for ordered dithered halftone images. In this method, the data hiding is obtained by sub image swapping operation and by decomposing ordered dithered halftone into a maximal number of sub images. The major advantage of this scheme is that it preserves good visual quality and offers a high capacity. The authors also propose a reversible authentication watermarking system based on reversible watermarking method. Their work shows better visual quality compared to an existing method.

He et al, [12] proposes a neighborhood characteristic based detection model for statistical fragile watermarking to lift the constraints of the tampered area from 4% to 14% of the host image. He et al demonstrate experimentally and analytically that the neighborhood characteristic based detection model effectively reduces the total number of false decisions and detects the tampered pixels with high probability.

Tan et al, [13] proposes a lexicographic-structured framework to generate image hashes. Their system consists of two parts: dictionary construction and maintenance, and hash generation. The authors implement a hashing scheme using discrete cosine transform (DCT) and non-negative matrix factorization (NMF). They also show that their scheme is resistant to normal content preserving manipulations, and has a very low collision probability.

Min-Jen Tsai, [14] presents application chaotic systems to strengthen the security of wavelet tree quantization (WTQ) technique for digital watermarking, especially against cryptanalysis attack. This enhancement in robustness of WTQ is achieved by dividing the digital

image into various blocks and that are scrambled using chaotic system technique and then WTQ is implemented. According to the results, this enhancement is not only for WTQ but also for other advanced wavelet tree based algorithms like wavelet tree group modulation (WTGM) and dynamic energy enabled differentiation (called DEED) watermarking techniques.

Min-Jen Tsai presents a new non-blind watermarking algorithm based on the wavelet tree classification and human visual system (HVS) - dynamic energy enabled differentiation (DEED). The algorithm works by dividing the wavelet coefficients of the image into disjoint trees and embeds one watermark bit into one wavelet tree along with contrast sensitive function (CSF) of human visual system. Author further proposes that this may be enhanced to truly blind watermarking technique by introducing a random direction differentiator that he calls DEEDR. The results show that DEED not only has low complexity but it performs better than other tree energy differentiation based techniques like WTGM and WTQ in terms of robustness and imperceptibility of watermarking.

Luo et al, [15] proposes a secure steganography technique based on a content adaptive scheme where a cover image is divided into small squares, which are rotated by a random multiple of 90 degree to produce a new image that is divided into non overlapping embedding units with three consecutive pixels. The data is embedded in the middle pixel based on the difference among the three pixels such that their sort order is not changed so as to preserve the local statistical features. Experimental results show that their scheme performs better than the existing Pixel-value differencing (PVD) based methods.

Liu et al, [4] proposes a low complexity coding scheme named Minority codes for improving watermarking embedding efficiency for large payloads. By exploiting the property that the positions of the minority bit in two complementing sequences are the same, where the minority bit is the bit with least number of occurrences in an odd number long binary sequence. Minority codes are generated. Using the codebook based on minority codes composed of a pair of complementing sequences combined with the watermarking algorithm such code words are identified that causes fewer embedding changes according to the host image and the watermarking method, thus providing a better efficiency for large payloads.

Xu et al, [16] describes a copy image detection technique that can resist various kinds of image attacks. In the first phase, large sized circular patches are constructed by using Scale Invariant Feature Transform (SIFT) detector and then a Multi-resolution Histogram Descriptor (MHD) is deployed to produce the discriminative attributes. The proposed scheme is compared to global and local feature extraction techniques. An experimental evaluation from benchmark attacks has been performed and the better performance of the proposed technique to the existing methodologies is reported.

Zeng et al, [17] propose a lossless drift compensation scheme to restrain the distortion issues in reversible video data hiding. In their work, the drift compensation signals are merged in the quantized DCT (Discrete Cosine Transform) coefficients P-frames and the corresponding recovery mechanism is presented. The scheme solves the spreading and accumulation problem of traditional reversible schemes. Experimental results show that their propose method improves the video quality and the original data can be recovered by removing the hidden data.

Su et al, [18] combines the methodologies of selective encryption and fingerprinting for effective DRM of H.264/AVC streaming videos. A selective encryption is first presented and then a fingerprinting scheme is introduced to provide further protection. The feasibility of the solution is also studied through the experimental results.

Ling et al, [19] attempt to propose a fine-search scheme to further refine results from rough query set. A local affine-invariant descriptor based on polar mapping and discrete Fourier transform is used as the first step. Second and final step is to propose a spatial dependent matching method. Robustness, distinction and suitability parameters are used as performance metrics in the paper by Ling et al.

Natthawut et al, [5] design a scheme to covertly sent secret message to multiple receivers via a stream of running short text messages. Thai language is used as case study but it can applied to many other languages. Authenticity and privacy against active attacks is also discussed in the paper.

This paper by Hsieh et al, [20] special issue is contributed, in which they develop a solution to identify the source and to detect the image tampering. They present an image authentication scheme that can verify the origin of the received image and detect if the has been tampered with. Their experimental results prove that using different strength values increases the robustness of the watermark with little sacrifice in image quality.

3. ALGORITHM AND SYSTEM DESIGN

DATA HIDING IN BINARY IMAGES

An increasingly large number of digital binary images have been used in everyday life. Handwritten signatures captured by electronic signing pads are digitally stored and are being used as the records for credit card payment by many department stores and for parcel delivery by

major courier services. Word processing software like Microsoft word allows a user to store his /her signature in a binary image file for inclusion at specified locations of a document. The documents signed in such a way can be sent directly to a fax machine or be distributed across a network. The unauthorized use of a signature, such as copying it onto an unauthorized payment, is becoming a big concern. In addition, a variety of important documents, such as social security records, insurance information, and financial documents, have also been digitized and stored. Because it is easy to copy and edit digital images via software tools, the annotation and authentication of binary images as well as detection of tampering are very important. This necessitated the studying of watermarking and data hiding techniques for binary document images which can be classified according to one of the following embedding methods: text line, word, or character shifting, boundary modifications, fixed partitioning of the image into blocks, modification of character features, modification of run-length patterns, or modifications of half-tone images. In the rest of this section we describe representative techniques for each of these methods.

3.1 PROPOSED SCHEME

There are two basic ways to manipulate binary images for the purpose of data hiding, namely, by changing the values of individual pixels and by changing a group of pixels. The first approach flips a black pixel to white or vice versa. The second approach modifies such feature as the thickness of strokes, curvature, and relative positions, which generally depends more on the types of images (e.g. text, ske tches, signatures, etc.). Since the number of parameters that can be changed by the second approach is limited, especially under the requirements of blind detection (i.e. , without using the original detection) and invisibility, the amount of data that can be hidden is usually limited except for special types of images.

In this paper we focus on first approach. An image is partitioned into blocks and several bits are embedded in each block by changing some pixels in that block. For simplicity, we shall show to embed one bit in each block. Three issues will be discussed:

i. How to select pixels for modification so as to introduce as little visual artifacts as possible.

ii. Specific means to embed data in each block using these flappable pixels and

iii. Why to embed the same number of bits in each block and how to enhance the efficiency.

3.1.1 Fixed Partitioning of Images

This class of methods partitions an image into fixed blocks of size m x n, and computes some pixel statistics or invariants from the blocks for embedding data. They can be applied to binary document images in general; e.g. documents with formatted text or engineering drawings. In [21], the input binary image is divided into 3 x 3 (or larger) blocks. The flipping priorities of pixels in a 3 x 3 block are then computed and those with the lowest scores can be changed to embed data. The flipping priority of a pixel is indicative of the estimated visual distortion that would be caused by flipping the value of a pixel from 0 to 1 or from 1 to 0. It is computed by considering the change in smoothness and connectivity in a 3 x 3 window centered at the pixel. Smoothness is measured by the horizontal, vertical, and diagonal transitions, and connectivity is measured by the number of black and white clusters in the 3 x 3 window. Data is embedded in a block by modifying the total number of black pixels to be either odd or even, representing data bits 1 and 0, respectively. Shuffling is used to equalize the uneven embedding capacity over the image. It is done by random permutation of all pixels in the image after identifying the flappable pixels. In [22], an input binary image is divided into blocks of 8 x 8 pixels. The numbers of black and white pixels in each block are then altered to embed data bits 1 and 0. A data bit 1 is embedded if the percentage of white pixels is greater than a given threshold, and a data bit 0 is embedded if the percentage of white pixels is less than another threshold. A group of contiguous or distributed blocks is modified by switching white pixels to black or vice versa until such thresholds are reached. For ordinary binary images, modifications are carried out at the boundary of black and white pixels, by reversing the bits that have the most neighbors with the opposite pixel value. For dithered images, modifications are distributed throughout the whole block by reversing bits that have the most neighbors with the same pixel value. This method has some robustness against noise if the difference between the thresholds for data bits 1 and 0 is sufficiently large, but this also decreases the quality of the marked document. In [23], a data hiding scheme using a secret key matrix K and a weight matrix W is used to protect the hidden data in a host binary image. A host image F is first divided into blocks of size m x n. For each block Fi data bits b1 b2 ...br 1 2 are embedded by ensuring the invariant SUM ((F ⊕K) ⊕W)≡b1 b2… br (mod 2r,)

where ⊕ represents the bit-wise exclusive OR operation,⊕ represents pair-wise multiplication, and SUM is the sum of all elements in a matrix. Embedded data can be easy extracted by computing. The scheme can hide as many as log2[mn +1] bits of data in each image block by changing at most 2 bits in the image block. It provides high security, as long as the block size (m x n) is reasonably large. In a 256 x 256 test image

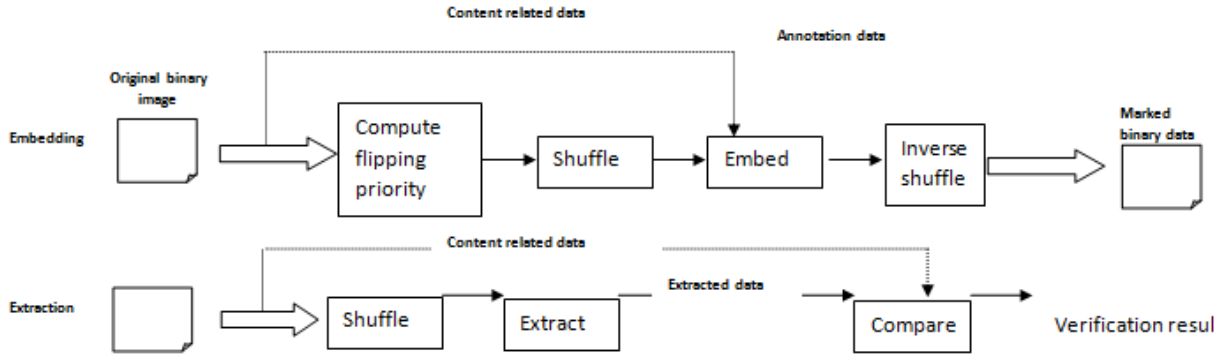
divided into blocks of size 4 x 4, 16,384 bits of information was embedded. This method does not provide any measure to ensure good visual quality in the marked document.

In [24], an enhancement was made to the method proposed in [23] by imposing the constraint that every bit that is to be modified in a block is adjacent to another bit that has the opposite value. This improves the visual quality of the marked image by making the inserted bits less visible, at the expense of sacrificing some data hiding capacity. The new scheme can hide up to log2[mn +1]-1 bits of data in an m x n image by changing at most 2 bits in the image block.

3.1.2 Boundary Modifications

In [25], the data is embedded in the 8-connected boundary of a character. A fixed set of pairs of five-pixel long boundary patterns were used for embedding data. One of the patterns in a pair requires deletion of the center foreground pixel, whereas the other requires the addition of a foreground pixel. A unique property of the proposed method is that the two patterns in each pair are dual of each other changing the pixel value of one pattern at the center position would result in the other. This property allows easy detection of the embedded data without referring to the

original document, and without using any special enforcing techniques for detecting embedded data. Experimental results showed that the method is capable of embedding about 5.69 bits of data per character (or connected component) in a full page of text digitized at 300 dpi. The method can be applied to general document images with connected components; e.g. text documents or engineering drawings.



Block diagram of the embedding and extraction process in binary images for authentication and / or annotation

4. CONCLUSION

This paper addresses the problem of data hiding for binary image. The fixed partitioning of image data hiding method for authentication and annotation of binary images was proposed. The method manipulates “flippable” pixels to enforce a specific block-based relationship to embed a significant amount of data without causing noticeable artifacts. Shuffling is applied before embedding to equalize the uneven embedding capacity. The hidden data can be extracted without using the original image. With the help of a few registration marks, they can also be accurately extracted after high quality printing and scanning. The algorithm can be applied to detect unauthorized use of signatures in binary image format, to detect alterations on documents, and to annotate signatures and drawings. Some directions for future investigation include the further refinement of flippability model for different types of binary images such as texts, drawings, and dithered images, as well as the recovery of binary image from high quality printing and scanning using fewer or no visible registration marks.

REFERENCE

[1] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn: “ Information hiding – A Survey”, Proc. Of IEEE, pp 1062-1078, July, 1999.

[2] M. Swanson, M. Kobayashi, and A. Tewfik, “Multimedia data embedding and watermarking technologies,” IEEE Proceedings, vol. 86, No. 6, pp 1064-1087, June 1998.

[3] N.F. Maxemchuk, S. Low. “ Copyright protection for the electronic distribution of text document”, 1999.

[4] Y. Liu, J. Mant, E. Wong and S. H. Low, “Marking and detection of text documents using 5th int’l. Conf. on document analysis and recognition, 1999, pp. 91-94.

[5] Muhammad K. K; “ Research advances in data hiding for multimedia security”, Jan 28, 2011.

[6] Liu et al. “Adaptive DE-based reversible steganographic technique using bilinear interpolation and simplified location map” April, 2011.

[7] Zhao et al. “Multimedia data embedding and watermarking technologies”, 2011.

[8] Yan et al. “MPEG-1 Layer III (MP3) audio CODEC based steganographic method”, Jan 2011.

[9] Lien and Lin “A reversible data hiding method for ordered dithered halftone images”, April 2011.

[10] Vivekananda et al. “Audio water marking scheme using singular value decomposition”, 2010.

[11] Fallahpour and Megias. “High capacity FFT-Based Audio Watermarking “ 2011.

[12] He et al. “A neighborhood- characteristics – based detection model for statistical fragile watermarking with localization”. Multimedia tools and applications. Vol. 52, No. 2-3, pp307-324, 2011.

[13] Zhenjun Tang et al. “ Lexicographical framework for image hashing with implementation based on DCT and NMF”. Multime Tools Applications, 2010.

[14] Min-Jen Tsai et al. “Wavelet tree based digital image watermarking by adopting the chaotic system for security enhancement”. Multimedia Tools and Applications, Vol. 52, issue 2-3, April, 2011.

[15] Luo et al. “A more secure steganography based on adaptive pixel-value differencing scheme”. Multimed Tools Applications, 2009.

[16] Xu et al. “Robust image copy detection using multi – resolution histogram”. Proceedings of the international conference on multimedia information retrieval, 2010.

[17] Zeng et al. “Issues and solution on distortion drift in reversible video data hiding”. Multimedia Tools and Applications, Volume 52, Number 2-3, 2010.

[18] Su et al. “Selective encryption H.264/AVC Digital watermark-fingerprint”. Multimedia Tools and Applications, 2011.

[19] Ling et al.” Fine search for image copy detection based on local affine-invariant descriptor and spatial dependent matching”. Research Advances in Data hiding for Multimedia Security, Volume 52, Number 2-3, 2011.

[20] Hsieh et al. “An image authentication scheme based on digital watermarking and image secret sharing”. Multimedia Tools and Applications, Page 823-828, 2010.

[21]

[22] M. Wu, E. Tang, and B. Liu, “Data hiding in digital images,” Proc. IEEE Int’l Conf.

[23] on Multimedia and Expo, Jul 31-Aug 2, 2000, New York, NY.

[24] E. Koch, J. Zhao, "Embedding robust labels into images for copyright protection", Proc.

[25] International Congress on Intellectual Property Rights for Specialized Information,Knowledge & New Technologies, Vienna, Aug. 1995.

[26] H-K Pan, Y-Y Chen, Y-C Tseng, “A secure data hiding scheme for two-color images”, IEEE Symposium on Computers and Communications, 2000

[27] Y. Tseng, and H. Pan, “Secure and invisible data hiding in 2-color images,” IEEE Symposiumon Computers and Communications, 2000.

[28] Q. Mei, E. K. Wong, and N. Memon, “Data hiding in binary text documents” SPIE Proc Security and Watermarking of Multimedia Contents III, San Jose, CA., Jan. 2001.

Owoade Ayoade Akeem is working as an assistant lecturer in the department of Computer Science, Tai Solarin University of Education, Ijebu Ode. He received his first degree in Mathematical Sciences/Computer science from University of Agriculture, Abeokuta, Nigeria in 1998 and master degree in Computer science from University of Ibadan, Nigeria in 2005. He had industrial experience in network monitoring on base station subsystem(BSS) and mobile switching centre(MSC) on ZTE platform at Nigerian mobile Telecommunications limited which took him to ZTE University, China where he attended Advance level course in BSS (2005). He is having total 8 years of industrial and teaching experience. His areas of interests are Multimedia data security, Multimedia data mining and data communications.