International Journal of Security and Its Applications
Vol. 1, No. 1, July, 2007

Handwritten Signature Watermarking and Extraction Technique Inspired by Principle of Segregation

Debnath Bhattacharyya
Heritage Institute of Technology, Computer Science and Engineering Department, Anandapur,
Kolkata-700107, INDIA
debnathb@gmail.com

Samir Kumar Bandyopadhyay
Department of Computer Science and Engineering, University of Calcutta, Senate House, 87/1 College Street, Kolkata – 700073, INDIA
skb1@vsnl.com

Poulami Das
Heritage Institute of Technology, Computer Science and Engineering Department, Anandapur, Kolkata-700107, INDIA
dippoulami@yahoo.com

Abstract

In this paper, we propose a technique for embedding handwritten signature image data into color images and extracting embedded image data from color images. For the sake of security, two watermarked images will be transmitted in different times from the sender's end to the receiver's end, in due course, from two transmitted images, at the receiver's end, original handwritten signature image data will be extracted; a new way of data hiding. From 1994 onward, the use and popularity of Internet in business particular has explored the area of Intellectual Property protection techniques.

This paper presents a technique for watermarking Handwritten Signature that achieves robustness by responding to complexity of copy detection, vulnerability to mark removal after revelation for ownership verification and mark integrity issues due to partial mark removal; these three weaknesses.

1. Introduction

Watermarking is the process that embeds data called a watermark, tag or label into an object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an image or audio or video. It may also be text only.

Digital watermarking is the process of conveying information by imperceptibly embedding it into the digital media. The purpose of embedding such information depends on the application and the needs of the owner/user of the digital media. Current main applications of watermarking include the following:

A) Copyright protection: The objective is to embed information about the source/owner of the digital media in order to prevent other parties from claiming the ownership of the media.

B) Fingerprinting: The objective of fingerprinting is to convey information about the recipient of the digital media (rather than the owner) in order to identify every single distributed copy of the media. This concept is very similar to serial numbers of software products.

C) Copy protection: Watermarking can be used to control data copying devices and prevent them from copying the digital media in case the watermark embedded in the media indicates that media is copy-protected.

D) Image authentication: The objective is to check the authenticity of the digital media. This requires the detection of modifications to the data. This project does not specifically focus on a single application of watermarking. Rather, it implements several different watermarking algorithms, which may or may not be desirable for a variety of applications. However, we only focus on watermarking of images as our work.

Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications. Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection.

In our work, Watermarking that embeds data called a watermark into an image object such that watermark can be detected or extracted later to make an assertion about the object. Handwritten Signature Mark can be thought as a visible “seal” placed over an image for authentication. In this research, watermarking scheme (algorithm) consists of two parts:

- Handwritten Signature Insertion
- Handwritten Signature Extraction

Computer scientists Samir Kumar Bandyopadhyay (University of Calcutta), Debnath Bhattacharyya (Heritage Institute of Technology) and A. J. Pal (Heritage Institute of Technology) examine digital watermarking, the process that embeds data called a watermark into an object such that the watermark can be detected and extracted later to make an assertion about the object. Watermarking is either “visible” or “invisible”. Although visible and invisible are visual terms watermarking is not limited to images, it can also be used to protect other types of multimedia objects. They said that the key techniques involve using secure functions to generate and embed image marks that is more detectable, verifiable, and secure than existing protection and detection techniques [8].

2. Previous Works

Many current Intellectual Property (IP) protection techniques are based on encrypted source files. For example, encrypted modules disguise the form and structure from Intellectual Property (IP) users. This allows the Intellectual Property (IP) users the ability to incorporate soft modules and high performance simulation models into their design using a Computer Aided Design (CAD) tool provided with the decryption key, without exposing the IP to theft. However, this approach has been routinely and successfully attacked, often by directly attacking the Computer Aided Design (CAD) tool. Therefore, there is no foreseeable

Intellectual Property (IP) protection technique based on encrypted source files, despite stronger forms of encryption and more thorough systems engineering.

Signature hiding techniques for image, video, and audio signals have recently received a great deal of attention. Digital image steganography has been especially well explored in 1998 by R.J. Anderson and Fabien A.P. Petitcolas [1].

Min Wu, 2004, proposed a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates “flippable” pixels to enforce specific blockbased relationship in order to embed a significant amount of data without causing noticeable artifacts. Shuffling is applied before embedding to equalize the uneven embedding capacity from region to region. The hidden data can be extracted without using the original image, and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks [2].

N.F.Johnson and Sushil Jajodia, 1998, and M. Kankanahalli, et al., 1999, proposed techniques for general intellectual property protection through watermarking. Marks are embedded at the behavioral level down to the physical layout by imposing design constraints [6,3]. A different set of synthesis and optimization issues arises when applying marks at different design phases. Addressing the design at a lower level of abstraction provides the advantage of a larger design space and greater flexibility, making it possible to embed signatures that are significantly more difficult to detect and remove.

M. Kankanhalli, et al. [7] has developed a visible watermarking technique. They divide the host image into different blocks; then they classify the blocks into six different classes in the increasing order of noise sensitivity, such as edge block, uniform with moderate intensity, uniform with high or low intensity, moderate busy, busy and very busy.

W.Zhu, et al. [4, 5] proposes an invisible watermarking technique, where watermark is inserted to wavelet coefficients. The watermark is added to the every high-pass wavelet coefficients.

I.Pitas, et al. uses an approach that allows slightly more information to be embedded. A binary signature that consists of equal number of zeros and ones is embedded in an image by assigning pixels into one of the two sets. The intensity levels of pixels in one of the sets are altered. The intensity levels are not changed in the other set. Signature detection is done by comparing mean intensity value of the marked pixels against that of the not marked pixels. Statistical hypothesis testing is used for this purpose. The signature can be designed in such a way that it is resistant to JPEG compression and low pass filtering. According to the authors, the degree of certainty can be as low as 84% and as high as 92%, which would likely not stand up as evidence in a court of law for copyright protection. But, the algorithm has the advantage that it doesn’t need the original image for watermark detection.

A. Ammar, A. S. S. El-Kabbany M. I. Youssef and A. Emam have developed a new data hiding technique based on residue number system is introduced in digital imagery system. This technique is used to encode two digital image signals or one text with one image signal which are quantized with 8 bits using residue number system (RNS) technique and multiplexed together. This technique will lead to unreadable two image signals, which are hidden and embedded in multiplexed image signal. Also the demultiplexing technique to separate the original image signals is simply performed successfully [9].

Yongjian Hu and Byeungwoo Jeon have proposed a reversible visible watermarking algorithm to satisfy a new application scenario where the visible watermark serves as a tag or ownership identifier, but can be completely removed to resume the original image data [10]. It includes two procedures: data hiding and visible watermark embedding. In order to losslessly recover both the watermark-covered and nonwatermark- covered image contents at the receiver end, the payload consists of two reconstruction data packets, one for recovering the watermark covered region, and the other for the nonwatermark- covered region. The data hiding technique reversibly hides the payload in the image region not covered by the visible watermark.

Mark A. Masry, 2005, proposed a novel blind watermarking algorithm designed for map and chart images. The algorithm segments the image into homogeneous regions and adds multiple watermark signals to the locations of the pixels on the boundary of several regions. The presence of these signals in the watermarked image is determined using a correlation based detector. The watermarks can be detected in the presence of synchronization errors such as those incurred by cropping the image, or shifting by several columns or rows, and in the presence of noise. The algorithm is designed to efficiently process typical map images, which can have resolutions on the order of several 100 million pixels [11].

F. Bartolini, A. Tefas, M. Barni and I. Pitas discussed the problem of authenticating video surveillance image. After an introduction motivating the need for a watermarking-based authentication of VS (video surveillance) sequences, a brief survey of the main watermarking-based authentication techniques is presented and the requirements that an authentication algorithm should satisfy for VS applications are discussed. A novel algorithm which is suitable for VS visual data authentication has proposed [12].

Wen Chung Kuo, Chin Chih Lin and Jiin Chiou Cheng proposed a robust data hiding scheme which combines shuffling method based on RSA and embedding the hidden message in spatial domain [13].

Chang-Lung Tsai, Kuo-Chin Fan, Char-Dir Chung and Thomas Chiang Chuang have proposed a novel data hiding mechanism by hiding data based on pair-wise logical computation. The proposed mechanism can achieve the benefits of reversible and lossless reconstruction of hidden data and host image without utilizing any information from the original host image. It will not degrade the visual quality of the recovered host image after extracting the hidden data. Moreover, satisfactory data hiding capacity can be obtained simultaneously [14].

3. Our Work

We have designed a new Double Crossover Algorithm (DCA). This DCA has some rules, known as DCA Master Rules, those rules are illustrated below:-

Step1: Select two individuals: A, B

Step2: Get chromosome from both the individuals (each chromosome with 3 characteristics in both the individuals). A single byte (with 8 bits) is responsible for a character each chromosome made up of 3 bytes, i.e., with 3 characters chromosome from individual A designated as ‘x y z’ chromosome from individual B designated as ‘p q r’ two points Crossover taken place between ‘x y z’ and ‘p q r’.

Recombination : ½ A with characteristic ‘x q z’ (where A Dominant and B recessive) and ½ B with characteristic ‘p y r’ (where B Dominant and A recessive).

Step3: First Generation (F1), heterozygous individuals are taken for self-fertilization.

Step4: Heterozygous parent gives equal portions of gametes.

Step5: Segregation occurs in production of gametes.

Step6: The progeny are then equally divided between the dominant phenotype and the recessive phenotype. Characteristic with original individuals will be derived (F2).

Rules are implemented and tested using 2 different pseudocodes, for security purpose.

3.1. Pseudocode-1

Watermarking Using Monohybrid Genetic Crossover:-

```
1. Open files in1, in2 in input mode
2. Open files out1, out2 in output mode
3. Read bytes one by one from both the
   input files until EOF
4.    increase the count by one
5.    if count > 54 then {
6.      if RGBCount = 1 then
7.         write byte of in1 to out1
           write byte of in2 to out2
8.      if RGBCount = 2 then
9.         write byte of in2 to out1
           write byte of in1 to out2
10.     if RGBCount = 3 then
11.        write byte of in1 to out1
           write byte of in2 to out2
12.     increase RGBCount by 1
13.     if RGBCount > 2 then
14.       assign 0 to RGBCount
      }
15.   Else
16.     write byte of in1 to out1
        write byte of in2 to out2
```

17. Close in1, in2, out1, out2

3.1. Pseudocode-2

Watermark Detection Using Self Crossover:-

1. Open files in1, in2 in input mode
2. Open files out1 in output mode
3. Read bytes one by one from
   both the input files until EOF
4. increase the count by one
5. if count > 54 then {
6. if RGBCount = 1 then
7. write byte of in2 to out1
8. if RGBCount = 2 then
9. write byte of in1 to out1
10. if RGBCount = 3 then
11. write byte of in2 to out1
12. increase RGBCount by 1
13. if RGBCount > 2 then
14. assign 0 to RGBCount
    }
15. Else
16. write byte of in1 to out1
17. Close in1, in2, out1

4. Result and Illustration with Statistical Analysis

There were two innovations to the science of genetics:

- developed pure lines
- counted those results and kept statistical notes

Pure Line - a population that breeds true for a particular trait [this was an important innovation because any non-pure (segregating) generation would and did confuse the results of genetic experiments] F1 Generation possesses the information needed to produce both parental phenotypes in the following generation. The F2 generation always produced a genotype ratio (1:2:1) and phenotype ration (3:1) where the dominant trait is present three times as often as the recessive trait.

Dominant - the allele that expresses itself at the expense of an alternate allele; the phenotype that is expressed in the F1 generation from the cross of two pure lines.

Recessive - an allele whose expression is suppressed in the presence of a dominant allele; the phenotype that disappears in the F1 generation from the cross of two pure lines and reappears in the F2 generation.

Thus the following points are important in our work:

- The hereditary determinants are of a particulate nature. These determinants are called genes.
- Each parent has a gene pair in each cell for each trait studied. The F1 from a cross of two pure lines contains one allele for the dominant phenotype and one for the recessive phenotype. These two alleles comprise the gene pair.
- One member of the gene pair segregates into a gamete, thus each gamete only carries one member of the gene pair.
- Gametes unite at random and irrespective of the other gene pairs involved.

Using symbols we can depict the cross of Image (where the signature will be marked) and Handwritten Signature Image, these are Parental Generation, in the following manner:

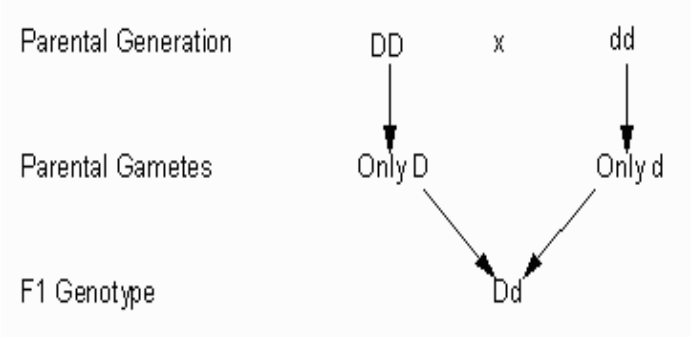

Figure-1

DD : Image (where the signature will be marked).

dd : Handwritten Signature Image.

Dd : Watermarked Image(s).

For self crossover, Dd x Dd, has to be taken, The F2 generation was created by selfing the F1 Images. This can be depicted graphically in a Punnett square.

Union of Gametes At Random		***D***	***d***	Punnett Square
	D	*DD*	*Dd*	
	d	*Dd*	*dd*	

Table-1

The Punnett Square allows us to determine specific genetic ratios. Genotypic ratio of F2, 1 DD : 2 Dd : 1 dd (or phenotype ratio, 3 D_ : 1 dd), (consider Table-1).

So, our intension is to get, dd (Pure line homozygote recessive) : Handwritten Signature Image.

½DD (Pure line homozygote dominant) : Image (where the signature is marked), not required in our case.

Heterozygous F1 generation, from 2-points crossover of Parental Chromosomes, illustrated in Figure-2.

4.1. Solution

Final output of Selfing from F1 Generation:-

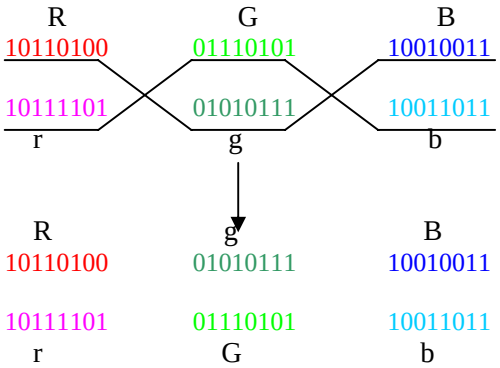

Figure-2

From the product of F2 Generation we have got our desired output, Pure line homozygote recessive, with combination as follow:

½DD (Pure line homozygote dominant) : Image (where Handwritten Signature will be marked).

¼Dd (Heterozygotes) : Watermarked Images.

½dd (Pure line homozygote recessive): Handwritten Signature Image.

4.1. Presentation

Figure-3, is the illustration of our entire work, started from Parental to F2 Generation desired offspring.

5. Conclusion

Technique about watermarking is that are more efficient for detection, more convincing for ownership and recipient verification, and more secure and robust against mark removal than

existing techniques. Both Heterozygous images are used for mark removal. This technique is evolved as result of extensive study of genetical behavior of living organisms.

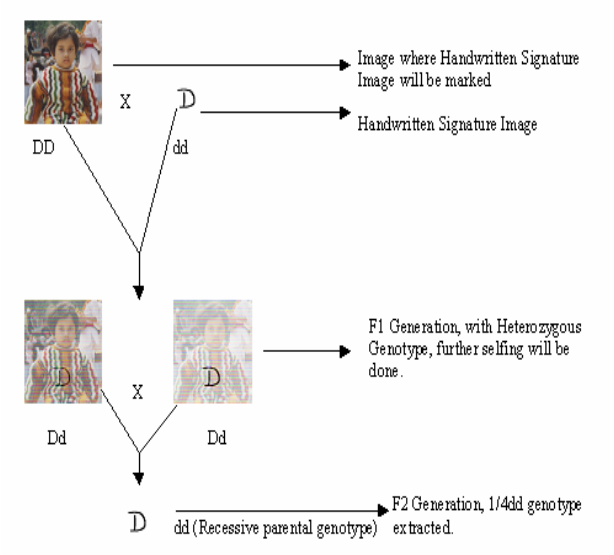

Figure-3

6. References

[1] R.J. Anderson and Fabien A.P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Comm., Vol.16, No.4, May' 98, pp.474-481.

[2] Min Wu, Data Hiding in Binary Image for Authentication and Annotation, IEEE Transactions On Multimedia, Vol. 6, No. 4, August 2004.

[3] N.F.Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol.31, No.2, pp.26-34, feb.1998.

[4] W. Zhu, et al., "Multiresolution Watermarking for Images and Video", IEEE Tran. On Circuits & Systems for Video Technology, Vol.9, No.4, June 1999, pp.545-550.

[5] W. Zhu, et al., "Multiresolution Watermarking for Images and Video : A Unified Approach", Proc. IEEE International Conf. on Image Processing, ICIP-98, Vol.1, pp.465-468.

[6] M. Kankanahalli, et. al., "Adaptive Visible Watermarking of Images", Proc. of IEEE Int. Conf. On Multimedia Computing Systems, ICMCS-99, Cento Affari, Florence, Italy, June 1999.

[7] M. Kankanahalli, et. al., "Adaptive Visible Watermarking of Images", Proc. of IEEE Int. Conf. On Multimedia Computing Systems, ICMCS-99, Cento Affari, Florence, Italy, June 1999.

[8] Samir K Bandyopadhyay, Debnath Bhattacharyya and A. J. Pal, "Secure Delivery of Handwritten Signature", ACM Ubiquity, Vol. 7 Issue. 40 October 16, 2006.

[9] A. Ammar, A. S. S. El-Kabbany M. I. Youssef and A. Emam, "A Novel Data Hiding Technique Using Residue Number System", NRSC 2003, Proceedings of the Twentieth National Radio Science Conference, 18-20 March 2003, Cairo, Egypt, Page(s):C15 - 1-12.

[10] Yongjian Hu and Byeungwoo Jeon, "Reversible Visible Watermarking and Lossless Recovery of Original Images", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, No. 11, November, 2006.

[11] Mark A. Masry, "A Watermarking Algorithm for Map and Chart Images", Proceedings of the SPIE Conference on Security, Steganography and Watermarking of Multimedia Contents VII, January 2005.

[12] F. Bartolini, A. Tefas, M. Barni and I. Pitas, "Image Authentication Techniques for Surveillance Applications", IEEE Proceedings, Vol. 89, No. 10, October 2001.

[13] Wen Chung Kuo, Chin Chih Lin and Jiin Chiou Cheng, "Design a Data Hiding Scheme using RSA", IEEE Int. Workshop VLSI Design & Video Tech. Suzhou, China, May 28-30, 2005.

[14] Chang-Lung Tsai, Kuo-Chin Fan, Char-Dir Chung and Thomas Chiang Chuang, "Reversible and lossless data hiding with application in digital library", ICME '04. 2004 IEEE International Conference, 11-14 Oct. 2004 Page(s):226 – 232.

Authors

Debnath Bhattacharyya

Lecturer, Computer Science and Engineering Department, Heritage Institute of Technology, Kolkata. Received his M.Sc.(IT) Degree, from Allahabad Agricultural Institute, in 2004. He was an Education Officer in Computer Society of India, Kolkata Chapter for 10 years. His research interests include Image Processing and Bio-Informatics. He has 12 Years of experience in the line of Teaching and Projects. He is working towards his research, since, middle of 2006 under the guidance of Prof. Samir Kumar Bandyopadhyay. He has published eleven Research Papers in International Journals and Conferences.

Dr. Samir Kumar Bandyopadhyay

B.E., M.Tech., Ph. D (Computer Science & Engg.)., C.Engg.,D.Engg., FIE, FIETE, currently, Professor of Computer Science & Engineering and Registrar, University of Calcutta, visiting Faculty Dept. of Comp. Sc., Southern Illinois University, USA, MIT, California Institute of Technology, etc. His research interests include Bio-medical Engg, Mobile Computing, Pattern Recognition, Graph Theory, Software Engg.,etc. He has 25 Years of experience at the Post-graduate and under-graduate Teaching & Research experience in the University of Calcutta. He has already got several Academic Distinctions in Degree level/Recognition/Awards from various prestigious Institutes and Organizations. He has published 300 Research papers in International & Indian Journals and 5 leading text books for Computer Science and Engineering. He has visited USA, Finland, Sri Lanka.

Poulami Das

Did her M.Tech in Computer Science and Engineering from the University of Calcutta. She is currently a Lecturer with the Computer Science and Engineering Department at Heritage Institute of Technology, Kolkata. Her research interest includes Bio-Informatics and Image Processing. She has 3 Years of experience in the line of Teaching. She is working towards his research, since, middle of 2006 under the guidance of Prof. Samir Kumar Bandyopadhyay. He has published seven Research Papers in International Journals and Conferences.