

Secure Delivery of Handwritten Signature

by

Samir Kumar Bandyopadhyay^Ψ

Department of Computer Science and Engineering,
University of Calcutta,
Senate House, 87 /1 College Street, Kolkata - 700073,
skb1@vsnl.com, skb1@sify.com

Debnath Bhattacharyya^Φ

Heritage Institute of Technology,
Computer Science and Engineering Department,
Anandapur, Chowbaga, Kolkata - 700107,
debnathb@gmail.com, debnath_s77@hotmail.com

Anindya Jyoti Pal[@]

Heritage Institute of Technology,
Computer Science and Engineering Department,
Anandapur, Chowbaga, Kolkata - 700107,
anindyajp@yahoo.com

A number of researchers have proposed using digital marks to provide ownership (watermarking) identification for the property. One way of data hiding is digital signature, copyright label or digital watermark that completely characterizes the person who applies it and, therefore, marks it as being his property. Digital Watermarking is the process that embeds data called a watermark into an object such that 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 object. Our research work is on watermarking techniques in particular.

Many of these proposed techniques share three specific weaknesses: complexity of copy detection, vulnerability to mark removal after revelation for ownership verification, and mark integrity issues due to partial mark removal. This paper presents a method for watermarking Handwritten Signature that achieves robustness by responding to these three weaknesses. 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.

Keywords : HSIA, HSEA, Encoder, Decoder, Formatter and Comparator.

1. Introduction

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Iliad [1]. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history [2]. Few other examples of steganography can be found in [3,4,5]. Watermarking technique has evolved from steganography. The use of watermarks is almost as old as paper manufacturing [6]. 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 other. Digital watermarking technology is used with cryptography, signal processing and communications. Digital Watermarking is providing value added protection on top of data encryption and scrambling for content protection.

In our research, Watermarking process 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 our research, watermarking scheme (algorithm) consists of three parts:

- The Watermark
- Handwritten Signature Insertion
Algorithm (HSIA) or The encoder.
- Handwritten Signature Extraction Algorithm (HSEA) or The decoder.

HSIA (marking algorithm) incorporates the Handwritten Signature as watermark into an Image. HSEA (extraction / detection algorithm) extracts the Handwritten Signature from the Watermarked image.

2. Related Work

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 [8, 9]. Although many mark security and verification issues have been raised [10], several image-watermarking techniques do exist that have been shown to be robust against all known attacks [11]. Digital audio protection has proven to be even more difficult, but many different techniques have nevertheless been proposed [12,13,7]. Video stream protection techniques have also been developed [1,14].

Techniques have arisen that provide general intellectual property protection through watermarking. Marks are embedded at the behavioral level down to the physical layout by imposing design constraints [15,2,16,17]. 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.

Another area of related work is in string matching, which has received a great deal of attention since the early 1970s [18]. Several exceptionally effective algorithms have been proposed for rapid string matching in text [7, 19, 20]. A number of copy detection techniques have been developed in biotechnology [15] and image processing [21].

M.Kankanhalli, et al. [22] 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. [23, 24, 25] proposes an invisible watermarking technique, which is very much similar to that of, but the watermark is inserted to 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.

3. Our Research and Experiments:

We have used BMP File format because of its simplicity, highly standardized and popular. The BMP File Header has exactly fourteen bytes in it. Windows Image Header is 40 bytes long. In the 24-bit format, each pixel is represented by three consecutive bytes of data that specify the RGB component values respectively. We are considering the above Windows BMP file format in our experiment.

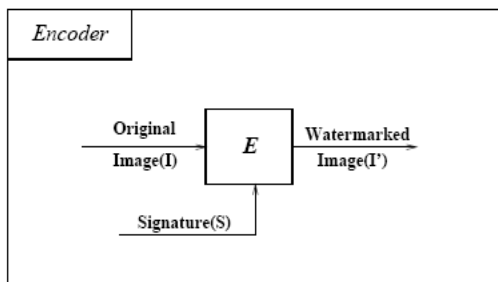
3.1 Handwritten Signature Insertion Algorithm (HSIA), The Encoder:

Let us denote an Image by I , a Handwritten Signature by S and the Watermarked Image by \hat{I} . E is an encoder function, it takes an image I and a Handwritten Signature S and it generates a new image which is called watermarked image \hat{I} . Mathematically,

$$E(I, S) = \hat{I} \quad (1)$$

It should be noted that the signature S may be dependent on image I .

Following figure illustrates the encoding process:



HSIA : The Encoder

3.1.1 Handwritten Signature Image Formatter Pseudocode:

1. Open handwritten signature bitmap file in Input mode
2. Open formatter bitmap file in output mode
3. Set an integer I to 1
4. While input bitmap file is not end

5. Loop
6. Read byte
7. I is increased by 1
8. If integer I is greater than 54 Then
9. Start byte count increased 1 by 1
10. If byte count is equal to 3
11. Write every third byte to formatter file
12. Else
13. Write modified byte to formatter file
14. make byte count to 0, when it reached 3
15. Else
16. Write byte to formatter file
17. End loop
18. Close all files

3.1.2 HSIA, The Encoder, Pseudocode:

1. Open image file in input mode
2. Open formatted signature file in input mode
3. Open resultant file in output mode
4. Set an integer 'I' and 'x' to 0
5. while both the input files not end
6. loop
7. Read byte from both the input files 1 by 1
8. I is increased by 1
9. If integer I is greater than 54 Then
10. If x is equal to 2 Then

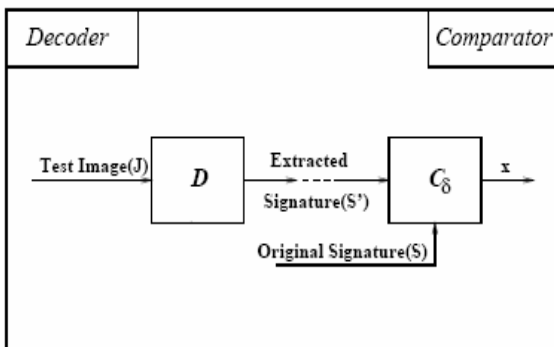
11. Write byte of formatted file to output file
12. Else
13. Write image file byte to output file
14. x is increased by 1
15. if x is greater than 2 Then Set 0 to x
16. Else
17. Write image file byte to output file
18. Refresh byte stream
19. End loop
20. Close all files

3.2 Handwritten Signature Extraction Algorithm (HSEA), The Decoder:

A decoder function D takes an image J (Watermarked) whose ownership is to be determined and recovers the handwritten signature S' from the image. Mathematically,

$$D(J) = S' \quad (2)$$

Following figure illustrates the decoding process:



HSEA : The Decoder

3.2.1 HSEA, The Decoder, Pseudocode:

1. Open resultant file generated by HSIA in input mode
2. Open extracted signature file in output
3. While input bitmap file is not end
5. Loop
6. Read byte
7. Depending on byte count, process the byte
8. Write the processed byte to output file
9. End Loop
10. Close all files

4. Result and Illustration:

The Formatter pseudo code is tested under P-4 Machine with the platform independent language, Java. The original signature is a 24-bit BMP File (Figure : OUTPUT). The BMP Image is Scaled and Thinned. The Formatter (3.1.1) algorithm (Stage-I) convert the image in such a way that only the last data byte will be changed, that can also be identified and modified by the 3.2.1, the Decoder Algorithm.

Now the Formatted Signature (BMP) File and the other Image (BMP) File are taken and HSIA (3.1.2) Algorithm will encode the Formatted Signature on the other Image (BMP) File, marked as Stage-II on Figure : OUTPUT.

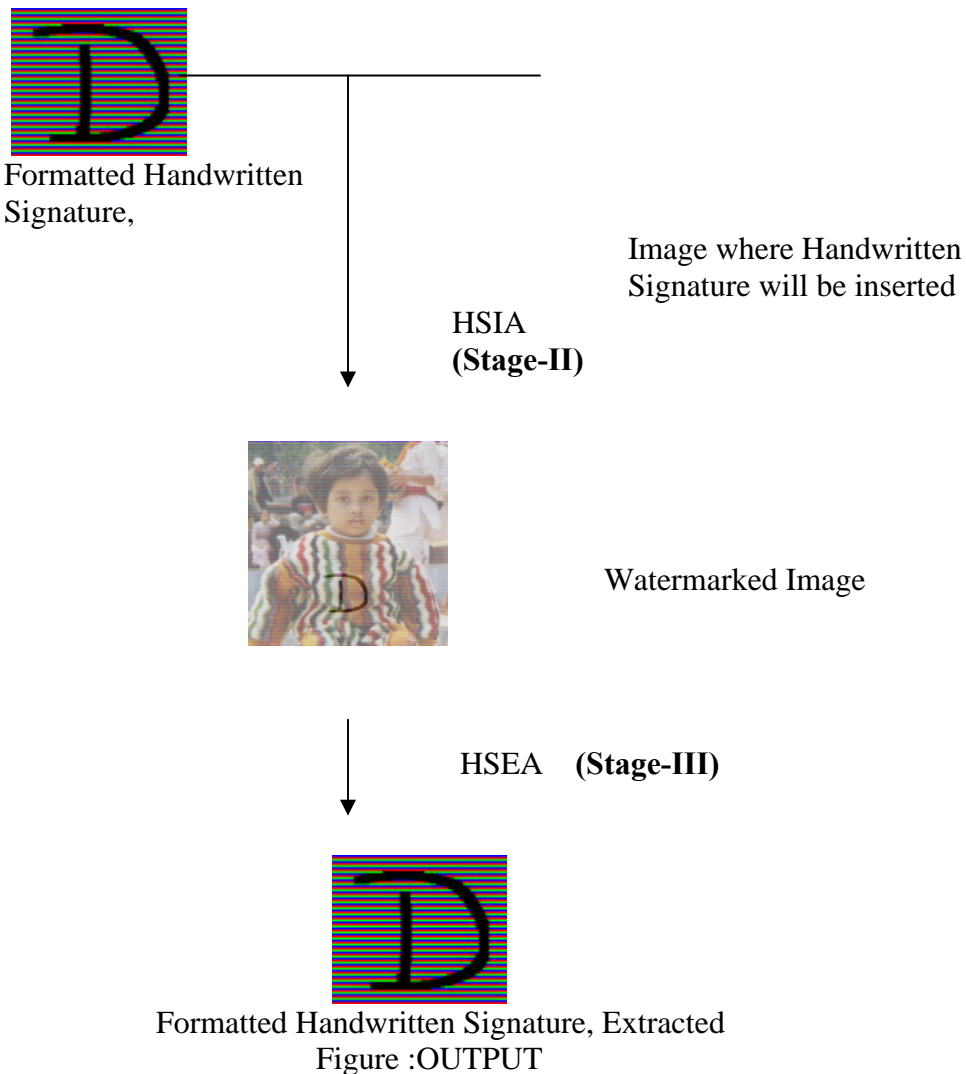
In Stage-III, Algorithm HSEA (3.2.1) will be executed and encoded image will be extracted.



Original Handwritten
Signature, for example.

Handwritten Signature
Formatter (**Stage-I**)





5. Conclusion

We have proposed a new HSIA and HSEA design techniques for Watermarking that are more efficient for detection, more convincing for ownership and recipient verification, and more secure and robust against mark removal than existing techniques. These improvements are achieved without increasing user design effort, CAD tool effort, or area and timing overhead. Hopefully, this work will open a new side of secure data transaction over open Network.

We have also started our future work for Comparator technique.

References

- [1] Homer, "The Iliad" (trans. R. Fragels), Middlesex, England: Penguin 1972.
- [2] Herodotus, "The Histories" (trans. R. Selincourt), Middlesex, England: Penguin 1972.

- [3] David Kahn, "Codebreakers : Story of Secret Writing", Macmillan 1967.
- [4] David Kahn, "The History of Steganography", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30 June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7.
- [5] F.A.P.Petitcolas, et al., "Information Hiding - A Survey", *Proceedings of the IEEE*, Vol.87, No.7, July 1999, pp.1062-1078.
- [6] Hal Berghel, "Watermarking Cyberspace", *Communications of the ACM*, Nov.1997, Vol.40, No.11, pp.19-24.
- [7] Neal Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag.
- [8] R.J. Anderson, "Stretching the Limits of Steganography", *Proc. of First Int. Workshop on Information Hiding*, Cambridge, UK, May30 June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.).
- [9] N.F.Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, Vol.31, No.2, pp.26-34, feb.1998.
- [10] V. K. Rohatgi, "An Introduction to Probability Theory and Mathematical Statistics", Wiley Eastern Ltd., 1993.
- [11] E. Franz, et. al., "Computer Based Steganography", *Proc. First Intl. Workshop on Information Hiding*, Cambridge, UK, May 30 - June 1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.).
- [12] A.Papoulis, "Probability, Random Variables and Stochastic Processes", McGraw Hill Inc., 3rd Edn., 1991.
- [13] R.C.Gonzalez and R.E.Woods, "Digital Image Processing", Addison-Wesley Publishing company, Inc., 1993.
- [14] 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 1998, pp.474-481.

- [15] A.K.Jain, "Fundamentals of Digital Image Processing", Prentice-Hall of India Pvt. Ltd., 1995
- [16] J. G. Proakis, "Digital Communications", McGrawhill 1995, 3rd ed.
- [17] A. J. Viterbi, "CDMA Principles of Spread Spectrum Communications", Addison-Wesley Inc., 1995.
- [18] A.Papoulis, "Probability, Random Variables and Stochastic Processes", McGraw Hill Inc., 3rd Edn., 1991.
- [19] W. Bender, et. al., "Techniques for Data Hiding", *IBM Systems Journal*, Vol.35, No.3 and 4, pp. 313-336, 1996.
- [20] B.M.Macq and J.J.Quisquater, "Cryptography for Digital TV Broadcasting", *Proc. of the IEEE*, Vol.83, No.6, June 1995, pp. 944-957.
- [21] R. G. Gallager, "Information Theory and Reliable Communication", Wiley, 1968.
- [22] 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.
- [23] 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.
- [24] 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.
- [25] I.J.Cox et. al., "Secure Spread Spectrum Watermarking of Images, Audio and Video", *Proc IEEE International Conf on Image Processing, ICIP-96*, Vol.3, pp 243-246, <http://www.neci.nj.nec.com/tr/neci tr 95 10.ps>

Author's Profiles:

^ψ **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 250 Research papers in International & Indian Journals and 5 leading text books for Computer Science and Engineering. He has visited USA, Finland, Sri Lanka, Singapore, Australia, South Africa, UK, Austria, Germany, etc., for different academic purpose.

^φ**Debnath Bhattacharyya**, Lecturer, Department of Information Technology, Heritage Institute of Technology, Kolkata. He did his M.Sc. in Information Technology, 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, Projects and Research. He has published 1(one) Research Paper in International Journal.

@Anindya Jyoti Pal did his M.Tech in Computer Science and Engineering from the University of Calcutta. He is currently an Assistant Professor with the Computer Science and Engineering Department at Heritage Institute of Technology, Kolkata. His research interests include Graph Coloring, Algorithm and Image Processing. He has 7 Years of experience in the line of Teaching and Research. He has published more than 4 research papers in the international conferences and several books as well.

Source: Ubiquity -- Volume 7, Issue 40 (October 17, 2006 - October 23, 2006)

<<http://www.acm.org/ubiquity/>>