Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-1, February 10, 2012

Hand Written Signature Embedding in Photographs - an Authentication Mechanism for Internet Based Transactions

Rajkumar S
M.Sc (Computer Technology)
Coimbatore Institute of Technology
E-mail:rajkumarmessenger@gmail.com

Manikandan K M
Dept of MCA
K.S.Rangasamy College of Technology
E-mail:kmmanikandanmca@gmail.com

Abstract - The photograph-signature scheme is widely used in many day-to-day transactions, such as in passport application and others. This paper proposes to embed the handwritten signature into passport size photograph using watermarking technique. The signature is embedded in the photograph, and thus protected from all attempts to copy it. The watermarking methods used guarantee that the photograph is not altered in any disturbing manner and signature is extracted efficiently and exactly later. The embedded photograph can then be used as authentication document. An algorithm for signature embedding and extraction has been developed and implemented. The system has been verified using several images and satisfactory results have been observed.

Keywords: *Internet Security, Digital Watermarking*

I. INTRODUCTION

The rise of information economy, borne along by proliferating computers, sprawling telecommunications, and the Internet, has radically transformed how people do business and communication. The private documents that in the past had been committed to paper and hand delivery or stowed under lock and keys are now routinely created, sent, and stored electronically. However, the very things that allow such speed and ease of communication have also made it far more difficult to ensure one’s authenticity. In an electronic age, an interloper can intercept and alter messages far more easily now than when face-to-face exchanges were the norm. Passwords and encryption methods are widely popular, but they are complex and cumbersome to many in remembering long strings. Despite their complexity, they are often broken. Biometric techniques like fingerprinting, eye scanning, etc are increasingly used for offline transactions. Online transactions defy such usage and though feasible, they are costlier to implement and to maintain.

The other viable and cost effective means is to use handwritten signature verification system. But owing to the ease and swiftness, with which duplication of information can be achieved in the digital world, the human signature as such cannot be used on the Net. Does this mean an end to handwritten signature based verification, which has been long used as the primary source of identification of a person? Not so, as this paper proposes a digital watermarking based approach to protect the signature on the Internet. This proposed scheme is called photograph-signature authentication scheme.

II. SIGNATURE EMBEDDING AND EXTRACTION

The system proposes to provide an alternative scheme to the photograph-signature combined approach used in the present paper based authentication system. The photograph-signature approach uses the photograph for visual identification of the person and the signature endorses it.

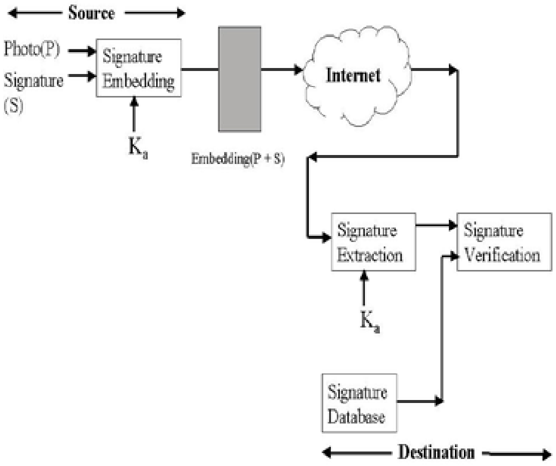


Fig 2.1: Schematic Block of a Generic Signature Embedding Based Authentication System

In order to be effective, Signature Embedding should meet a set of requirements:

- **Unobtrusive:** It should be statistically and perceptually invisible so as not to degrade data quality and to prevent attackers from finding and changing it.
- **Readily extractable:** The data owner or an independent control authority should easily extract it.
- **Loss less:** It should imply no loss of relevant information.
- **Robust:** It should be difficult to remove by attackers trying to counterfeit copyright of the data. If only partial knowledge of the signature is available, then attempts by an outsider to remove or destroy it should produce a remarkable degradation in the data quality before the watermark is lost. In particular, the signature embedding should be resistant to common signal processing techniques, to distortion and to collision and forgery attacks.
- **Unambiguous:** Its retrieval should unambiguously prove the identity of the data owner.
- **Dynamic:** Embedding should be dynamic, exploiting unique features of the photograph. In other words, it should provide robustness and unpredictability to the embedding process.
- **Coupling with Cryptographic methods:** The embedding can be coupled with other cryptographic methods to provide extra layer of security.

The image embedding process can be viewed as a task consisting of two main steps.

1. The first step in embedding is signature casting in which the signature is embedded into the original image and transmitted over the channel as the embedded image.
2. The second step is the signature detection, in which the signal is received and signature is extracted from the embedded image. The original image can also be used to provide extra robustness against several attacks.

The System Diagram of Signature Embedding and Extraction is as Below.

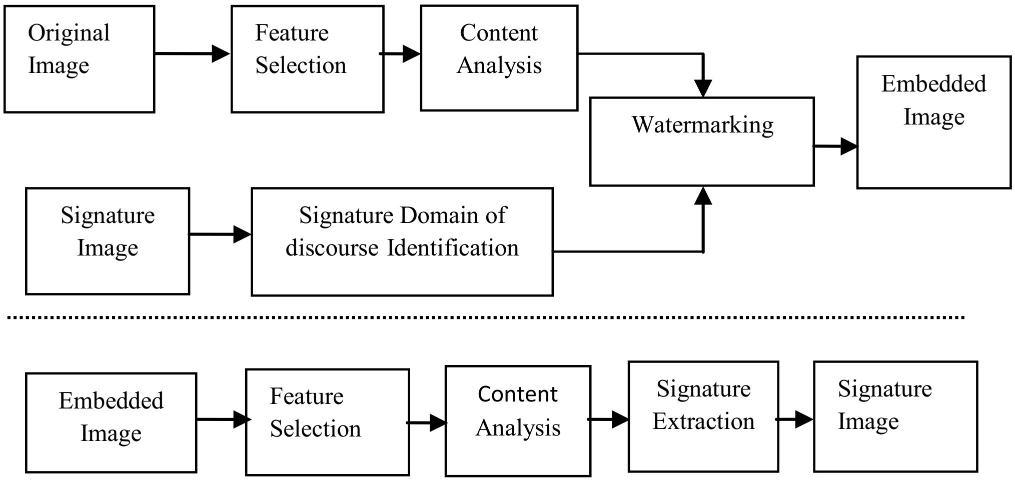


Figure 2.2: System Diagram of Signature Embedding and Extraction

2.1 Feature Selection

The authentication system needs that; original photograph should not be altered in a way that would tamper the quality of the photograph. Hence, there is a need to identify particular features of the photograph, which are insignificant in person identification process. The passport type photos, which are known to contain background, though of different varieties, can be altered without troubling the other processes in signature verification.

2.2 Content Analysis

Authentication system demands that signature embedding be robust and dynamic, exploiting unique features of the image. Histogram analysis is done on the feature-selected area of the image, determining the dynamic range of pixels that should contain signature. Traditionally as in [5] and [1], blue component of the image had been exploited owing to its low luminosity. However, that will make tampering easy. Therefore, the colour and range of pixels should be dynamically determined for each image.

2.3 Signature domain of discourse identification

Generally, it is observed that the signature image contains redundant space, around the signature. This invalidates any future attempts to provide robustness using less space. To overcome this, the signature's domain of discourse is identified and stored in the host image. The domain of discourse includes all area of the signature image that contains vital information needed during signature identification.

III. PROPOSED METHOD

Signature Embedding

The algorithm for signature embedding is as follows:

a) Convert the signature to 1-bit image and identify signature's Domain of discourse.
b) Convert photograph into gray colour image and perform edge detection.
c) Identify the background area and perform histogram analysis on its colour counterpart.
d) Embed signature bits into pixels with values in the above-determined range in the step c.

a. Convert the signature to 1-bit image and identify signature's Domain of discourse.

The discourse identification involves:

1. Convert the image pixels of signature to black (0) and white (1) values. In other words, only one bit is stored for each signature pixel. This action is asserted by the fact that every pixel contributes to the signature by mere presence. Hence, it will be unnecessary to store all bits for every pixel. This is valid for almost all signature based authentication systems.
2. The area of the signature is constricted from all the 4 sides of the image, until a black pixel pertaining to the signature is obtained.

b. Convert photographs into gray colour image and perform edge detection.

The pixels of the photograph image are grabbed and RGB values are extracted. The gray scale equivalent is determined as

$$K = (R + G + B)/3$$

The edge highlighting the border between background and the person is determined by performing convolution of the image with Sobel's masks.

c. Identify the background area and perform histogram analysis on its colour counterpart.

The background pixels are isolated. To perform histogram analysis, the pixels in all the three colour components red,

R1	R2	R3	…	R10
G1	G2	G3	…	G10
B1	B2	B3	…	B10
6 – 30	31-55	56 – 80	…	231 – 255

green and blue are divided based on their pixel values and regrouped into sets of 25 consecutive pixel values as in [3].

Each Ri, Gi or Bi is the cumulative histogram values over their corresponding range.
The colour component is first chosen as

Colour component, $C = \max (\Sigma Ri + \Sigma Gi + \Sigma Bi)$, where $1 \leq i \leq 255$.

The range of pixels that are to contain signature, is determined as

1. Sort the colour range on their cumulative histogram values as S_{CR}.
2. Pick all S_{CRi} such that $\Sigma S_{CRi} \geq T$,

   Where $1 \leq i \leq N$ and N is minimum, and

   T= threshold number of pixels required for embedding signatures.

d. Embed signature bits into pixels with values in predetermined range using watermarking.

The watermarking method employed will determine robustness, security and integrity of the signature. The spatial domain based watermarking methods are more suitable for this type of application as they provide large space for embedding. The embedding is tested with different methods viz. Least Significant Bit (LSB) insertion method and Amplitude modulation (AM) method. In the AM method, modifying the selected colour channel C of the pixel (i, j) embeds the bit s by a fraction of the luminance L as:

$$L_{ij} = 0.3R_{ij} + 0.6G_{ij} + 0.1 B_{ij}$$

$$C_{ij} = C_{ij} + (2s - 1) L_{ij}\, q$$

Where q is a constant, determining the signature strength. The value q is selected for best trade-off between invisibility and robustness.

Signature Extraction

The signature extraction extracts the signature bits from the embedded image and reconstructs the signature. The extraction algorithm is similar to the embedding algorithm, but for the final step.

The algorithm is as follows:

1. Convert photograph into gray colour image and perform edge detection.
2. Identify the background area and perform histogram analysis on its colour counterpart.
3. Extract signature bits from pixels with values in above determined range.

Extract signature bits from pixels with values in above determined range.

In amplitude modulation, to recover the embedded bit a prediction of the original value of the pixel containing the information is needed. This prediction is based on a linear combination of pixel values in a neighborhood around the pixel. The prediction C'ij is thus computed as:

$$C'_{ij} = \frac{(C\,i-1,j + C\,i+1,j)}{2}$$

To retrieve the embedded bit the difference δ between predicted value and actual value of the pixel is taken: δ = C ij – C' ij
The sign of the difference δ determines the value of the embedded bit.

IV. IMPLEMENTATION

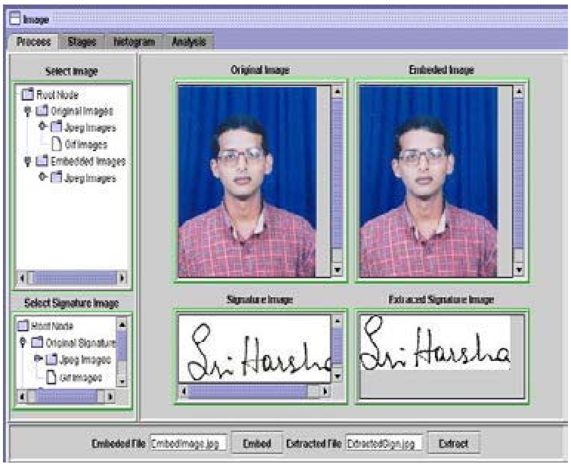
A prototype has been implemented for signature embedding and extraction using watermarking methods. Photographs of size 250 x 250 with different set of background and other features are selected. Signature Images are reduced to a fixed area of 100 x 50 and preprocessed with threshold and contrast enhancements. The value of signature strength parameter q was kept at 0.1. An algorithm to adaptively compare the original and extracted signatures has been developed.

The new feature selection approach is compared with the classical approach for efficiency of signature embedding. The robustness of traditional method, which exploited only the blue component, and the newly proposed method, which dynamically selects the colour component based on the colour dominance, is also compared. The new proposed approach is tested with different methods for watermarking viz. Least Significant Bit (LSB) insertion method and Amplitude modulation method.

V. EXPERIMENTS AND RESULTS

The algorithms have been implemented in JAVA. Experiments have been carried out with a widely varied image set of 500 photographs of size 250 x 250 and 500 signatures. The photographs were categorized based on their background's colour dominance, and tested with methods, classical method of watermarking and amplitude modulation method of watermarking.

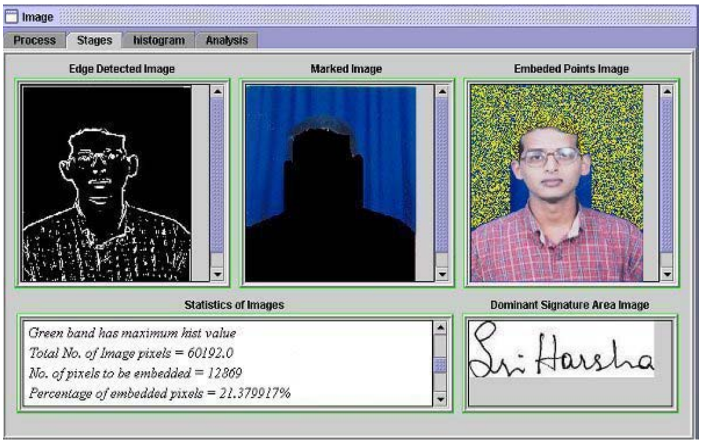
The histogram analysis of the original and embedded images shows the embedding in the colour band selected. The results of the intermediate stages shown below are used for verification of the method proposed.



Embeded File: EmbedImage.jpg

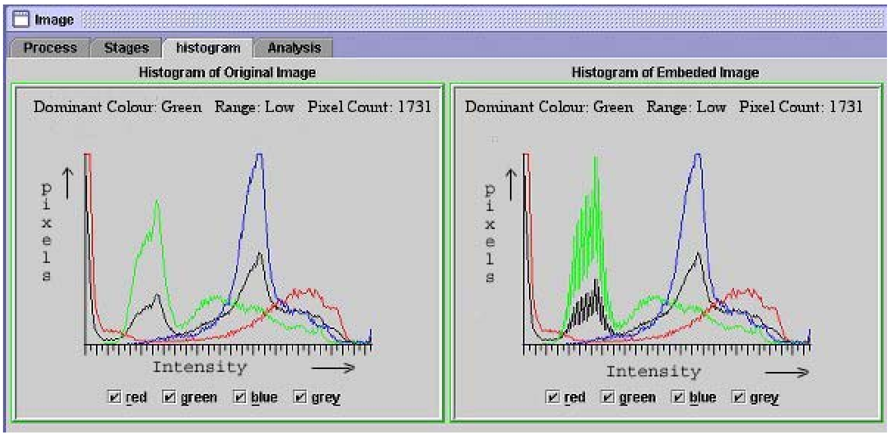
Extracted File: ExtractedSign.jpg

Figure 5.1: Front interface to the Signature Embedding



Green band has maximum hist value
Total No. of Image pixels = 60192.0
No. of pixels to be embedded = 12869
Percentage of embedded pixels = 21.379917%

Figure 5.2: Intermediate Stages During Signature Embedding



Dominant Colour: Green Range: Low Pixel Count: 1731

Dominant Colour: Green Range: Low Pixel Count: 1731

Figure 5.3 Comparison of Histogram of Original and Embedded Images

An Analysis engine has also been developed to study the results of the experiment on a variety of photograph-signature sets. A sample analysis snapshot has been shown below:

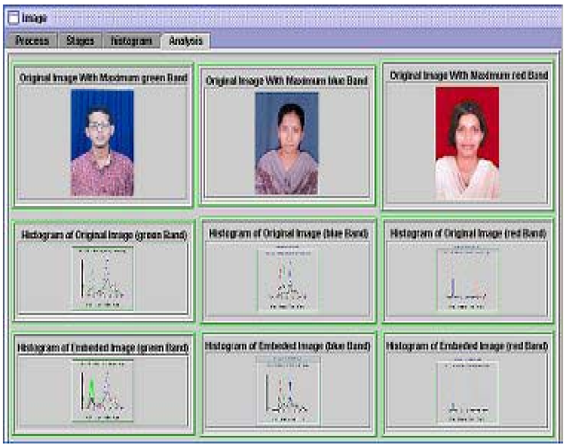


Image
Process
Stages
Histogram
Analysis
Original Image With Maximum green Band
Original Image With Maximum blue Band
Original Image With Maximum red Band
Histogram of Original Image (green Band)
Histogram of Original Image (blue Band)
Histogram of Original Image (red Band)
Histogram of Embeded Image (green Band)
Histogram of Embeded Image (blue Band)
Histogram of Embeded Image (red Band)

Figure 5.4 :Analysis Engine Snapshot of Photographs with Different Colour

The results are also tabulated for the above experiments.

Dominant Colour	Percentage comparison between original and extracted signatures
Red	95%
Green	95%
Blue	98%

Table 5.1: Efficiency of Signature Extraction

	Traditional Approach	New Feature Selection approach
Percentage of image pixels modified in the foreground of the photograph	35%	03% ***

Table 5.2: Comparison of image pixels modified in the foreground area of the photograph

*** 97% of pixels in the photograph's foreground remain unaffected.

VI. CONCLUSION

An authentication mechanism for business transactions on the Internet using human signatures has been discussed. The least significant bit insertion method and amplitude modulation method of watermarking was used to embed the signature pixels into the significant features of the photograph. The mechanism supports signatures that can be either handwritten or a thumbprint in support of both literate and illiterate persons. This system is particularly useful role in e-governance where the audience is large and diverse including literate and illiterates. The new concept has been verified and found to produce satisfactorily results.

The proposed algorithm could be improved in several ways. The strength of the signature in each of the selected color channel can be made proportional to the sensitivity of the human eye to it. More powerful histogram specification methods can be adopted to select pixels to contain signature. Also, robustness could be improved with the use of optimal error correcting codes.

REFERENCE

1. W. Bender, D. Gruhl, and N. Mormoto. Techniques for data hiding. In SPIE, volume 2420, February 1995.
2. Watermarking digital images for copyright, J.J.K.O Runaidh, W.J. Dowling and F.M. Boland, I.E.E. Proceedings on Vision, Signal and Image Processing, vol.43 no.4pp.250–256, Aug.1996, http://cuiwww.unige.ch/˜oruanaid/ieejnl.ps.gz.
3. K. C. Ravishankar, B. G. Prasad, S. K. Gupta and K.K. Biswas, “Dominant Color Region Based Indexing for CBIR”, IEEE, ICIAP proceedings, 0040, PP: 887-892,1999.
4. Information Hiding – An annotated bibliography. Ross J Anderson and Fabien A.P. Petitcolas. The electronic version of this document is available at: http: // www . iss e. gmu . edu /~njohnson/Security/sbib00.htm
5. Digital signature of colour images using Amplitude Modulation, Martin Kutter, and F.Johnson (1997).
6. Can Invisible watermarks resolve rightful ownership, an IBM Research report? Scott Craver, Nasir Memon, Boon-Lock Yeo, Minerva-Yeung. RC 20509 (July 25, 1996)
7. Digital Image processing, Rafael C Gonzalez, Richard E Woods. Addison-Wesley publications.