OPEN ACCESS
ISSN: 2249-6645

International
Journal
Of Modern Engineering Research (IJMER)

Providing Protection and Validation of Manual Signature image by using Embedding Approach

Niranjan Babu T [1], Balachandra Reddy K [2]
[,12]*Lecturer, CSE Department, JNTUA College of Engineering, Pulivendula, India*
tniranjanbabu@gmail.com [1] kakarla505@gmail.com [2]

ABSTRACT: In previous days data hiding had many conditions that affected the technique of data accessing by a mediator in an authorized network. It will become insecure if the mediator knows the procedure used by the sender. Hiding of manual signature is examined by using the embedding approach. The manual signature which we are using will be embedded in the host image and also the initial point of the embedded image is encrypted by using public key to form a complex image. The complex image will be later obtained at the receiver's end by using private key.
The principle which we follow here is that the size of manual signature image which the sender calculates is less when compared to the size of host image. The manual signature's initial point embedded in the host image will be positioned in a byte block and encrypted using a public key. The receiver receives the above block in a encoded format and decrypts it using a private key to get the initial point of the image and thus obtaining the manual signature. This technique provides a high amount of security thus enhancing the quality of manual signature and also prevents the optical deterioration of the host image.
The specific target is to provide protection and validation of the manual signature in an entrusted network.

Keywords: Digital watermarking, steganography, RSA, encryption, decryption, hybrid-embedding technique.

I. INTRODUCTION

Overview

The process of embedding information into another object or signal is known as watermarking. Embedding information into a digital signal is known as digital watermarking. In visible watermarking, the information which is embedded is visible in the picture or video. Information is added as digital data to audio, picture or video, but it cannot be seen in invisible watermarking. One important application of invisible watermarking is copyright protection systems, which is to prevent or find unauthorized copying of digital data.
Digital watermarking is a process where a low-energy signal is embedded in another signal. The signal in which the watermark is embedded is known as the cover signal. A challenging work here is to embed bytes without causing visual degradation to the host image. This requires embedding data in such a way that adapts with the local characteristics of an image. Then we require a hybrid digital embedding technique to hide an image into another image so that the quality of the recovered image can be improved.

II. Existing System

Bi-Color Nonlinear Data Embedding and Extraction of Handwritten Signature, IEEE Electro Information Technology Conference, EIT-2007, May 17-20, 2007, Illinois Institute of Technology, Marriott O'Hare Chicago, Illinois, U.S.A.Debnath Bhattacharyya and Deepsikha Choudhury and Samir Kumar Bandyopadhyay have proposed a data hiding method where the size of the carrier image must be double (or more) the size of source image. If necessary then additional bytes or noise has to be injected into carrier image to attain the required size. They said that the key techniques involve using secure functions to generate and embed image marks that are more detectable, verifiable, and secure than existing protection.

Demerits of existing system

- This System is vulnerable to attacks as tampering of the image is possible.
- The Data can be extracted if the attacker knows the Extraction Algorithm.

Proposed System

In this project, we propose a technique for embedding watermark bi-color image into color image. At the source, the handwritten signature image (bi-color image) is encoded at the end of the color image. Double folded security of handwritten signature can be achieved (over the entrusted network) by firstly, the starting point of encoding the image data is depended on the size of the images; secondly, the starting point (byte location) of bi-color image encoding in the color image is stored within a four-byte block in encoded form. This four-byte location encoding is done by public key. At the target, firstly, the starting point of encoding bi-color image data (location) is decoded by private key and then, secondly, starts extracting the encoded bi-color image data from the color image. This technique requires knowledge of the color image for the recovery of the handwritten signature image. At the receiver, the algorithm reconstructs the original handwritten signature image. Embedding high volume of information into images without causing perceptual distortion has been quite challenging. We here consider the problem of image-in image hiding, in which an image, called the handwritten signature image, is to be embedded into another image, called the host image, to get a composite image. We are using here hybrid data-hiding technique resulting into invisible watermarking.

In this project, two algorithms for encoding and decoding purposes are used. They are

- Hybrid digital-embedding Algorithm at source.
- Handwritten Signature Extraction Algorithm from Hybrid Composite Image files at target.
-

Merits of proposed system

- Double folded security for the handwritten signature.
- At source, the embedding is done and then the starting point is encrypted using the key concept.
- At the target, the starting point of encoding bi-color image (location) is decoded by key and then, extraction of image using the Algorithm.

The discrete cosine transform (DCT)

To separate the image into parts (or spectral sub-bands) the discrete cosine transform (DCT) has major role of differing importance (with respect to the image's visual quality). The DCT and discrete Fourier transform are same: a signal or image is transformed from the spatial domain to the frequency domain.

The following are the basic operations of DCT:

- N by M is an input image.
- Row i and column j are the intensity of the pixel f (i, j).
- Row k1 and column k2 is the DCT coefficient of F (u, v) in the DCT matrix.
- At low frequencies, much of the signal energy lies for most images; it appear in the upper left corner of the DCT.
- The lower right values represent higher frequencies and compression is achieved through these are often small.
- The input of DCT is an 8 by 8 array of integers. Each gray scale level pixels is contained by an array. An 8 point DCT can be considered as: where

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & \text{for} \xi = 0 \\ 1 & \text{otherwise} \end{cases}$$

To remove the unwanted pixels, we use DCT methodology in the host image that does not cause any visual degradation to the image in this project.

III. RSA Algorithm

Algorithm for generating key:

1. Generate two large random primes, p and q, of equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Calculate n = pq and (φ) phi = (p-1) (q-1).
3. Choose an integer e, 1 < e < phi, such that GCD (e, phi) = 1.
4. Calculate the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.
   - n is the modulus.
   - e is the public encryption exponent or just the exponent.
   - d is the secret exponent or decryption exponent.

Encryption

Processes done by sender A:

1. Obtains the recipient B's public key (n, e).
2. The plaintext message is represented as a positive integer m.
3. Calculate the cipher text $c = m^e \bmod n$.
4. The cipher text c is sent to B.

Decryption

1. Uses private key (n, d) to compute $m = c^d \bmod n$.
2. The plaintext from the message representative m is extracted.

Digital signature

Processes by sender A

1. A message digest of the information to be sent is created.
2. The message digest is represented as an integer m between 0 and n-1.
3. Uses her private key (n, d) to compute the signature $s = m^d \bmod n$.
4. The signature s is sent to the recipient B.

Signature verification

Processes by recipient B

1. Uses sender A's public key (n, e) to compute integer $v = s^e \bmod n$.
2. The message digest from this integer is represented.
3. The message digest of the information that has been signed independently and computed.
4. If both message digests are identical, the signature is valid.

Key length

When we talk about the key length of RSA key, we are referring to the length of the modulus, n in bits. The minimum key length for a secure RSA transmission is 1024 bits. One convention in defining key length is the position of the most significant bit in n has the value 1, where the least significant bit is at position 1. Similarly, key length = ceiling ($\log_2$ (n+1)). The other convention used is the key length which is the number of bytes needed to store n multiplied by eight, i.e. ceiling ($\log_{256}$(n+1)).

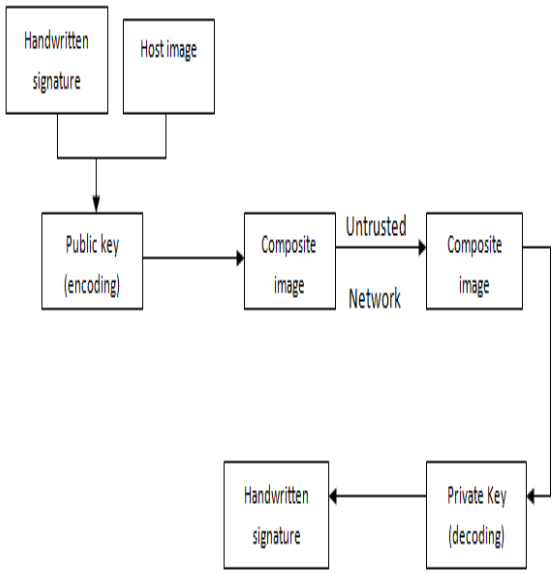

Fig: System Architecture

IV. Module Description:

Embedding of image

In this module host image and handwritten image are used. Host image is the multicolored, high pixel image whereas the handwritten signature image is bicolor. First the host image is subjected to Discrete Cosine Transform (DCT). The DCT is used to remove the bits that do not cause any visual degradation to the host image. It also helps to find the highest pixel area in the picture to embed the handwritten signature image. The appropriate point in the host image obtained is secure to embed the handwritten signature image.

The handwritten signature image is embedded using the Handwritten Signature Insertion Algorithm (HSIA). The HSIA is used mainly for inserting handwritten signature images. HSIA checks the host image and the handwritten signature image such that the size of the host image is greater than that of the size of the handwritten signature image. If this criteria satisfies then the signature image is embed into the host image at the particular point obtained by the DCT.

Encoding

The composite image is then encoded by obtaining the starting point of the embedded bicolor handwritten signature image in the Host Image. The DCT obtains the staring point in the composite image. Inverse DCT is done here to get the originality of the host image with default pixel. The address value of the starting point of the image is encoded using RSA cryptography concept. As it is difficult for the user to enter a big integer and obtain the keying values, I implement the technique of entering a secured keying in character format. After entering the character value, the encoding process of the starting point is done in the composite image.

The encoding process converts the composite image into encrypted image format which cannot be extracted by anyone except the desired party. A key is automatically generated using the encrypted image and it is been stored. The generated key is verified at the time of decoding process. Finally the obtained image appears to be an ordinary image but it contains the handwritten signature image which has the encrypted starting point.

Embedding and Encoding
Flow diagram

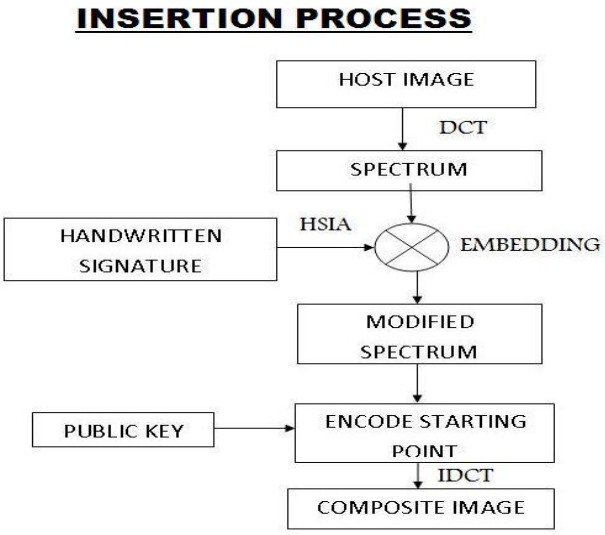

Fig: insertion process

Decoding

The decoding process is done by decrypting the starting point of the handwritten signature image in the composite image. First the character key value is entered to start the decryption process. A new key value is generated by the RSA Cryptography technique for the encrypted image.

Then the obtained encrypted image is subjected to decryption process. The key is verified with the already generated key. If the key value matches then the starting point is decoded. If mismatch of key is entered then it displays an error message to enter the correct key. Unauthorized users or hackers cannot obtain this encrypted key format as it used the big integer value and character keying concept. Verification is done twice to start the decryption process.

Extraction of image

The handwritten signature image is extracted using the Handwritten Signature extraction Algorithm (HSIA). The HSEA is used mainly for extracting handwritten signature images. The handwritten signature is retrieved from the composite image without any visual degradation. The handwritten signature image is obtained with original quality. The extracted handwritten image now can be used by the authorised party. Unauthorised hackers cannot extract the signature image at any cost.

Decoding and Extraction

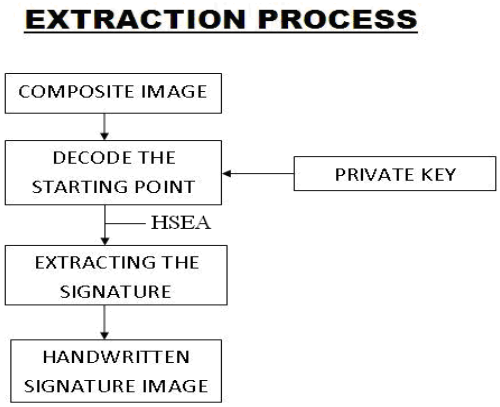

Fig: extraction process

Applications

Digital watermarking techniques have wide ranging applications. Some of the applications are enlisted below.
Copyright Protection

- Copy Protection
- Tracking
- Tamper Proofing
- Broadcast Monitoring
- Concealed Communication

V. Conclusion

This paper is mainly concentrates on the extraction of handwritten signature from the composite image. The visual quality of the handwritten signature image is maintained after the extraction has been done. The key generation is used, which increases the security of the bicolor image and provides authentication.

References

[1.] Hybrid Digital Embedding Using Invisible Watermarking- IEEE 2008.
[2.] N.F.Johnson and Sushil Jajodia,"Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol.31, No.2, pp.26-34, feb.1998.
[3.] D. Kundur and D. Hatzinakos, "Towards a Telltale Watermarking Technique for Tamper Proofing", Proc. ICIP, Chicago, Illinois, Oct 4–7, 1998, vol 2.
[4.] R. B. Wolfgang and E. J. Delp, "A Watermark for Digital Images", Proc. IEEE Int. Conf. on Image Processing, vol. 3, pp. 219–222, 1996.