International Journal of Computer Techniques -– Volume 2 Issue 1, 2015

RESEARCH ARTICLE OPEN ACCESS

Fusion of Digital Signature & Fingerprint Watermarking using Bit plane slicing

Sonali V.Satonkar, Dr.seema Kawathekar

Dept. of Computer Science &Information Tehnology

Dr.Babasaheb Ambedkar Marathwada University, Aurangabad

Abstract

In recent years, internet revolution resulted in an explosive growth in multimedia applications. The rapid advancement of internet has made it easier to send the data/image accurate and faster to the destination. Besides this, it is easier to modify and misuse the valuable information through hacking at the same time. Digital watermarking is one of the proposed solutions for copyright protection of multimedia data.[2] Digital image watermarking provides copyright protection, by hiding appropriate ownership information in digital images. This ownership information may be in the form of logo called as 'watermark'. The image formed after hiding 'watermark' in original image is called 'watermarked image'.[3]

Keyword :- **Least Significant Bit (LSB) , pixel**

Introduction:-

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics.

Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are anticipated to pervade nearly all aspects of the economy and our daily lives.[1]

1.2 Technique of watermarking

1 Spatial Domain Techniques

The watermark can be detected by correlating the expected pattern with the received

signal. Spatial domain watermarking is performed by modifying values of pixel.

2 Frequency Domain Watermarking

These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture.

3 Spread Spectrum

This technique can be used for both spatial domain and frequency domain. The spread spectrum method has the advantage that the watermark extraction is possible without using the original unmarked image [4].

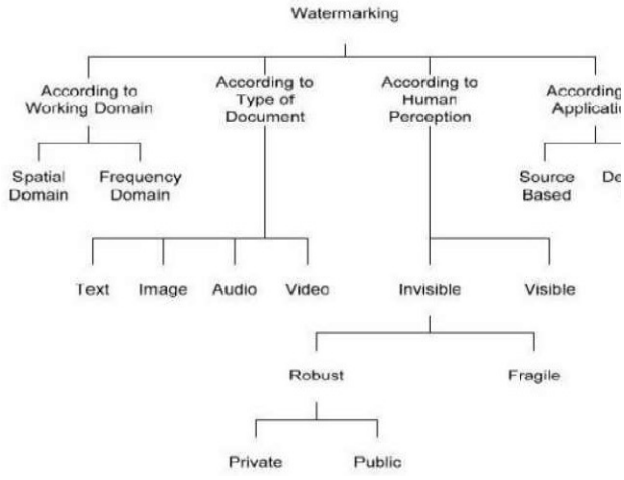
In other way, the digital watermarks can be divided into three different types as follows:

i. Visible watermark

ii. Invisible-Robust watermark

iii. Invisible-Fragile watermark

1.3 There are different sorts of watermarking as shown in figure 4



2 Objective:

Watermarking biometric data is a still a relatively new issue, but it is of growing importance as more robust methods of verification and identification are being used. Biometric provide the necessary unique characteristic but their validity must be ensured. This can be guaranteed to an extent by watermarks. In our Research , Image Watermarking using Least Significant Bit (LSB) algorithm is used. Proposed algorithm performs pre-processing operation on fingerprint & digital signature images. Often by isolating particular bits of pixel value in an image, I have highlight interesting aspects of that image.Higher order bits usually contain most of the significant visual images & lower order bits contain subtle details. This work has been implemented through MATLAB.

4. Methodology

4.1 Spatial Domain

In this work I have used image enhancement in spatial domain. The word spatial domain implies working with the pixel values or working directly with available raw data. Let g(x,y)be the original image where g is the gray level value and (x,y) are the image coordinate for 8 bit image , g an take values from 0 -255 where 0 represents black,255 represents white and all the intermediate values represents shades of gray. In an image of size 256 X 256 , x and y can take values from (0,0)to (255,255) the modified image can be expressed as under f (x,y)= T [g (x,y)] g (x,y) is the original image and T is the transformation applied to it to get a new modified image f(x,y). For all spatial domain technique it is simply T that changes. The general equation remains the same.

Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during watermark embedding.

- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

Spatial Domain enhancement may be carried out in following two different ways.

- point processing
- neighborhood processing

some of the important example of point processing are digital negative ,constant stretching thresholding gray level slicing, bit plane slicing, dynamic range compression.

4.2 Bit plane slicing: An image is defined as say 256 x 256 x 8 image. In this 256 x 256 is the number of pixel present in the image and 8 is the number of bits required to represent each pixel. 8 –bits simply mean 28 or 256 gray levels. Now each pixel will be represented by 8 bits. For example, black is represented 00000000 and white is represented as 11111111 and between them , 254 gray levels are accommodated. In bit plane slicing the importance of each bit in the final image this can be done as follows.

Consider the LSB value of each pixel and plot the image using only the LSBs. continue doing this for each bit till come to the MSB. Now getting 8 different images and all the 8 images will be binary. The

higher order bits contain majority of the visually sufficient data , while the lower bits contain the suitable details in the image.

5. Pre-processing

Preprocessing is done by following ways.

1) Firstly Read the fingerprint image & signature image.

2) Resize that two images.

3) Add that two images.

4) Then gray thresh image & gray thresh image to binary

5) Binary image to double precision.

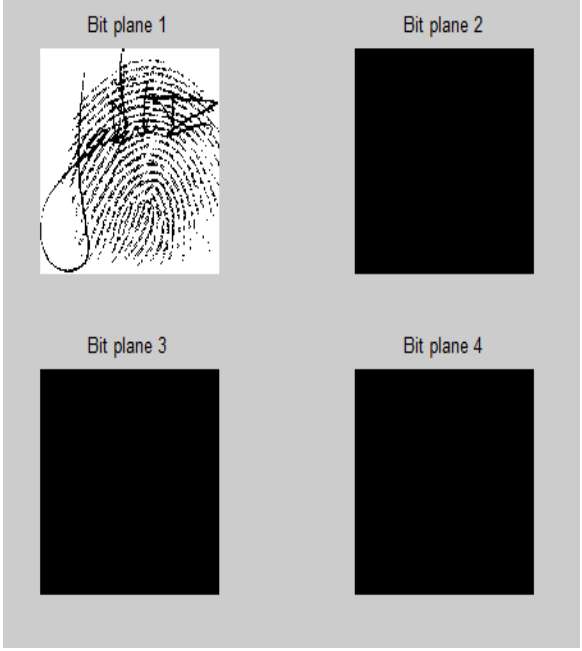
5.1 Least significant bit

LSB watermarking describes a straightforward and basic way to integrate watermark information in digital documents. Considering a basic grayscale image, the pixel and its values can be sliced up into significant and irrelevant levels. Because the significant levels merely represent a digital noise pattern, it could be easily used for digital watermarking. In changing selected pixel values of the noise pattern using a special, the watermarking information can be easily integrated.

There are many algorithms available for invisible digital watermarking. The simplest algorithm is Least Significant Bit (LSB) Insertion ,4 in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark. [6] Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times.[6].In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image .Two techniques were presented to hide data in the spatial domain of images by them. These methods were based on the pixel value's Least Significant Bit (LSB) modification

For the sake of this example only the least significant bit of each pixel will be used for embedding information. If the pixel value is 138 which is the

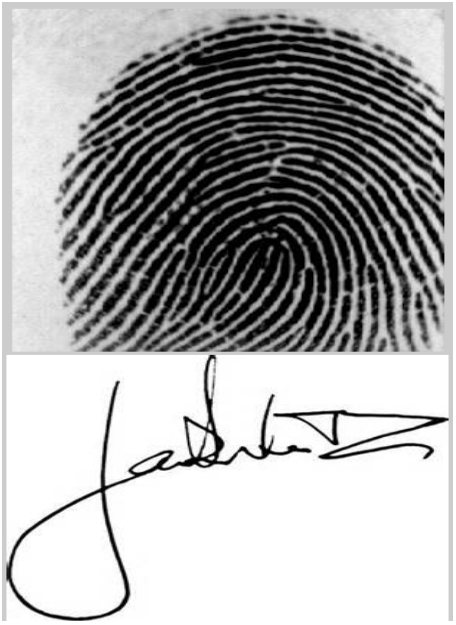
value 10000110 in binary and the watermark bit is 1, the value of the pixel will be 10000111 in binary which is 139 in decimal. In this example we change the underline pixel. [7].



5.2 Algorithm for least significant bit.

- Convert RGB image to gray scale image.
- Make double precision for image.
- Shift most significant bits to low significant bits of watermark image.
- Make least significant bits of host image to zero
- Add shifted version of watermarked image to modified host image.

6.Experimental Results:



7.Results :

- The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality.
- This ratio is often used as a quality measurement between the original and a watermarked image.

	PSNR	**MSE**
Fingerprint image	19.3725	751.3239
Signature image	30.3470	61.4306
combined fingerprint&signature	55.3509	0.1897
combined fp &sign watermark	51.6110	0.4487
Bit0 substitution	51.3626	0.4751
Bit 1 substitution	51.3166	0.4802
Bit 2 substitution	51.2266	0.4903
Bit3 substitution	51.0544	0.5101
Bit 4 substitution	50.7599	0.5459
Bit 5substitution	50.8499	0.5347
Bit 6substitution	51.2254	0.4904
Bit 7 substitution	51.6110	0.4487

:

Conclusion : The increasing amount of digital exchangeable data generates new information security needs. After performing the experimental work &statistical analysis of result the good quality image watermarking technique is robust. The robust solutions will ensure copyright protection and also guarantee the authenticity of multimedia documents. For security of images spatial domain watermarking technique is used.

10.Reference:

[1] Fernando L. Podio1 and Jeffrey S. Dunn", Biometric Authentication Technology: From the Movies to Your Desktop"

[2]Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C., Anil Gupta," Lsb Based Digital Image Watermarking For Gray Scale Image *IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. 2012), PP 36-41*

[3] Baisa L Gunjal and Dr. Suresh N Mali,"Article "Handling Various Attacks in Image Watermarking"

[4] Gurpreet Kaur Kamaljeet Kaur**,"** Image Watermarking Using LSB (Least Significant Bit)"

[5] Dipanjan Bhowmik DISSERTATION On Analysis of Digital Watermarking Methods towards Development of an Adaptive Watermarking Algorithm Based On DCT And an Approach to Steganography Using LSB

[6]Max Sobell"LSB Digital Watermarking",CPE 462

[7] R.AARTHI, 2V. JAGANYA, &3S.POONKUNTRAN "Modified Lsb Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 –7449 Vol-3, Iss-3, 2012

[8] Anil K. Jain "Biometric System Security" Department of Computer Science and Engineering Michigan State University, http://biometrics.cse.msu.edu.

[9] A.Ross, K.Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer-Verlag edition, 2006.