Efficient Analysis And Secure Client Side Image Using Fingerprint Embedding

A. Sudha, K. Vanitha, A. NooralShaba

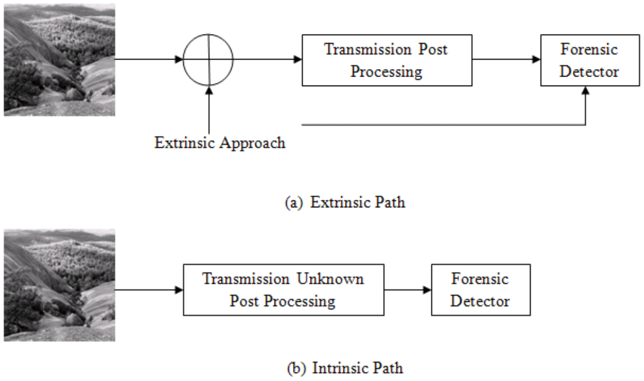
Abstract: In Secure embedding, the data sent to the client in encrypted form along with a client specific decryption key. The decryption process and watermarking process are securely interwined, so that decryption result in a different uniquely watermarked content copy personalized for the client. The main objective of the project is to introduce the audition to identify whether the received image is original or not. To do that it maintains the authorized users fingerprint. For sending the image, the sender has to encode the finger print with the original image. While encoding, the senders fingerprint will be embedded behind the original image. After receiving the fingerprint images the receiver has to decode the image. While decoding the image the receiver can extract the fingerprint which is embedded in the image. Then the forensics detector checks the extracted finger print with the collected fingerprints. If the fingerprints are matched then the received image is original image otherwise the received image has been modified by the hackers.

Index Terms: Finger print embedding, Decryption, Encoding, Decoding, Encryption, Decryption.

1 INTRODUCTION

Now a day's transferring the data in multimedia processing and network technologies has facilitated the distribution and sharing of multimedia through networks, and increased the security demands of multimedia contents. Hacking the data from the router and modifying the original data send by source and retransmit the modified data to the destination has now increased in network technology. To avoid those problems an algorithm has to be developed to detect and classify original image from the network transmission. [1] Motivation of the process is image validation, security of image transmission. By using the tool the algorithm can identify the received image is original or forgery image. Within the past decades, the explosive combination of multimedia signal processing, communications and networking technologies has facilitated the sharing of digital multimedia data and enabled pervasive digital media distribution. Digital images, in particular, have been widely used in news reporting, insurance claim investigation, criminal investigation, and many other applications. The digital nature of information also allows individuals to access, duplicate, or manipulate information. Conventional forensic technologies use proactive and additive means to protect multimedia content by hiding additional information in the original signal. For example, the idea of the trustworthy camera was used to make the trustworthiness of digital images accountable, where a digital watermark was embedded into the image at the instance of its acquisition. Secure Embedding, the content is sent to the client in encrypted form along with a client specific decryption key. The decryption process and watermarking process are securely interwined, so that decryption result in a different uniquely watermarked content copy personalized for the client. [1] Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and documents. Such a message is a group of bits describing information pertaining to the signal or to the author of the signal. Any later tampering of the image can be detected based on the changes on the digital watermark. Similarly, in traitor-tracing digital fingerprinting, user identification information is embedded in each distributed copy to identify the corresponding user and trace the source of the illicit copies. However, it requires that all camera manufacturers agree upon a common standard, and for some real applications, it may be too expensive and impractical to implement such extrinsic protection mechanisms. Often it is not possible to enforce content protection through any extrinsic means. However, for each copy of multimedia data, its acquisition, processing, and transmission process constitutes a unique data path. To ensure that [7] multimedia data are processed by the appropriate entities for intended purposes only, its data path must be validated by identifying each of its steps: acquisition, source coding, channel coding, transmission, and other possible processing at the user's side. Each operation leaves its unique artifact in the image. Such intrinsic fingerprints are naturally and inherently generated throughout the chain of content acquisition and processing, and it provides evidence to help identify the origin and detect the alterations of multimedia content. Thus in the scenarios where extrinsic content protection techniques are not applicable, image forensics via intrinsic fingerprints offers technologies to detect alterations and identify the source of the image without any proactive protection mechanisms Figure.1.1 illustrates the difference between the methodologies that rely on extrinsic operations to protect multimedia content versus those that employ intrinsic fingerprint analysis.

- *Sudha, M.E Working as Asst.Professor Al-Ameen Engineering College, Erode, India, vitsudha@gmail.com*
- *K. Vanitha, Ph.D Working as Asst.Professor Al-Ameen Engineering College, Erode, India, kvanithacse@gmail.com*
- *NooralShaba, M.E Working as Asst.Professor Al-Ameen Engineering College Erode, India, shaba64@gmail.com*


Transmission Post Processing
Forensic Detector
Extrinsic Approach
Transmission Unknown Post Processing
Forensic Detector

(a) Extrinsic Path

(b) Intrinsic Path

Figure.1.1 Multimedia security using extrinsic and intrinsic information.

With extrinsic protection of multimedia, an additive signal is embedded into the image before distribution and is available to the forensic detector, while with intrinsic-fingerprint forensics, the only input to the forensic detector is the received image in a raw format. Image forensics via intrinsic fingerprints can be applied to identify many types of image processing. [6, 7]For instance, it is often useful to determine the source of image acquisition: a digital camera or a post editing software. Since most image acquisition devices reduce the data size by applying lossy encoders to the images, there are prior arts in the literature which identify the camera model based on the JPEG quantization table. Forensics on other steps in image compression such as block size estimation via the intrinsic fingerprints has also been studied in the literature. It builds a framework to integrate the image source encoding forensics that provides a general methodology and fundamental research of image source coding identification. Unfortunately, the compression algorithm and settings may not be immediately obvious, especially if performed automatically as a result of the acquisition device (e.g., compression in digital cameras). Visible watermark is a secondary translucent overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedding in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism.

2 A DCT-Based Secure JPEG Image Authentication Scheme

In [4] an image authentication system that is tolerant to JPEG lossy compression operations. An encrypted feature vector extracted from the image DCT coefficients is embedded redundantly and invisibly in the marked image. On the receiver side, the feature vector from the received image is derived again and compared against the extracted watermark to verify the image authenticity. Two approaches have been suggested for achieving the authenticity of digital images: 1) the digital signature-based method and 2) the digital watermark-based method a digital signature is based on the method of Public Key Encryption. A private key is used to encrypt a hashed version (digest) of the image. This encrypted digest of the image is called the signature of the image; it provides a way to ensure that it cannot be forged. This signature then accompanies the image. The authentication process of the image needs an associated public key to decrypt the signature. The image received for authentication is hashed and the resulting digest is compared to the decrypted signature. If it matches then the received image is authenticated. It is based on the observation that discovered a mathematical invariant relationship between two discrete cosine transform (DCT) coefficients in a block pair before and after JPEG compression. for adding security, the derived feature vector is XOR-ed with a secret key known to sender and receiver. It could be possibly incorporated in the camera and downloaded in the authentication system upon system initialization. In this scheme it will consider only grey scale JPEG compressed images. The extension to color images is reasonably straightforward. A block diagram for the embedding of data is given in Figure. 2.1 EM/EX is the embed and extract control. MV is the proprietary mapping vector, and the feature vector is derived from the DC components of the quantized image blocks.

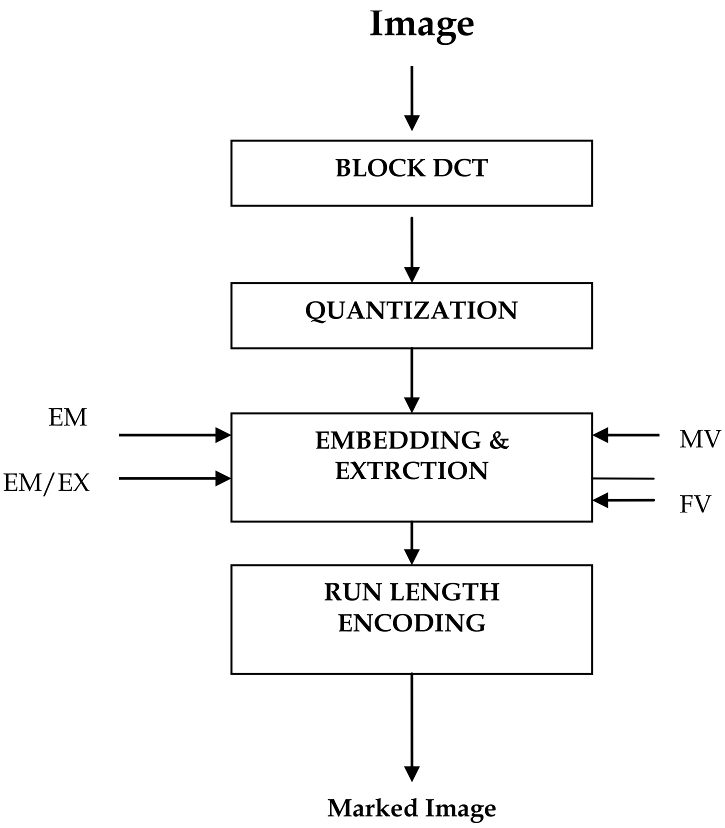


Figure 2.1 JPEG Embedding and Extraction Process

The embedding process is as follows: Assuming it need to embed a "1" into a block, then it examine the first AC component and it's corresponding MV bit, from a table such as in table 1, if it is a "1" then it leaves the AC unchanged, if it is a "0", then it find the nearest value in the table that has its MV bit "1", either to the left or right. In this case the AC value is changed to the value corresponding to the "1" in the table. The same process is carried out for all the first five AC components

AC	..	9	8	7	6	5	4	3	2	1	..
MV	..	1	0	0	1	0	1	1	0	1	..

Image authentication, requires that the verification method be able to resist incidental distortions while being sensitive to malicious manipulations. An image authentication scheme for verifying the authenticity of JPEG images is presented; it is based on a secret key and a secret mapping vector that is used in embedding the digital signature of a feature vector derived from the frequency domain of the image.

3 RELATED WORK

In earlier days, for transferring image through the network they used the visible watermarking approach. In that the security image is embedded behind the original image which is visible to the outside world. The watermark appears visible to a casual viewer on a careful inspection. For more robustness watermark should not be publicly available, the watermark should be used in different sizes and should be put in different portions for different images. Due to its visibility it cannot provide enough security to the image. Hence this approach is not recommended for providing more security. To overcome the problems in the watermarking approach I used the forensics detector which contains the collection of authentified fingerprint images. Draw backs in existing system watermarking approach was used. Due to its visibility every one can read the copy right information. Due to its visibility hackers can try to attack the image or chance to modify the image.

3.1 Drawbacks

In existing system watermarking approach was used. Due to its visibility every one can read the copy right information. Due to its visibility hackers can try to attack the image or chance to modify the image.

3.2 PROPOSED SYSTEM

Invisible watermarking techniques aim at producing watermarked data that suffer no or little quality degradation and perceptually identical to the original versions. The most common utility of a watermarked image is for image viewing and display and for extracting the embedded watermark in subsequent copy protection applications. To increase the security demands of multimedia contents, the secret information will be shared between the sender and receiver. Watermarking is most popularly used approach for providing security on images. Under many circumstance watermarking approach is not possible for providing the security. Because of the visibility of the security message, the hackers can create the watermarking on the original image as like the sender sent and then send the modified image to the receiver. Everyone can read the copyright information. To solve the problems in watermarking approach the unique intrinsic fingerprint of the image source coders are taken as the evidence for security. Based on the intrinsic fingerprint of image source encoders, forensic detector is developed. This detector identifies which source encoder is applied, what the coding parameters are along with confidence measures of the result. The main objective of the project is to introduce the Forensics Detector that identify whether the received image is original or not. To do that it maintains the authentified users fingerprint. For sending the image, the sender has to encode the finger print with the original image. While encoding, the senders fingerprint will be embedded behind the original image. After receiving the fingerprint images the receiver has to decode the image. While decoding the image the receiver can extract the fingerprint which is embedded in the image. Then the forensics detector checks the extracted finger print with the collected fingerprints. If the fingerprints are matched then the received image is original image otherwise the received image has been modified by the hackers Invisible robust watermarks find application in following cases.1.Invisible watermarking to detect misappropriated images.2. Invisible Watermarking as evidence of ownership.

4 CLIENT SIDE IMAGE USING FINGERPRINT EMBEDDING

To increase the security of multimedia contents, a protection scheme uses some security approaches between sender and receiver such as extrinsic approaches and watermarking. Secure Embedding, the content is sent to the client in encrypted form along with a client specific decryption key. The decryption process and watermarking process are securely interwined, so that decryption result in a different uniquely watermarked content copy personalized for the client. To overcome the problems in watermarking approach, Forensics Detectors via Intrinsic Fingerprints are used. The unique intrinsic fingerprint of the image source coders are taken as the evidence for security. Based on the intrinsic fingerprint of the sender, forensic detector is developed. Hence only original image will be received by the receiver. To start with working this project, JAVA software is used to communicate with a client side image using fingerprint embedding security mechanisms to protect us against malicious code that might try to invade image. Now a day's transferring the data in multimedia processing and network technologies has facilitated the distribution and sharing of multimedia through networks, and increased the security demands of multimedia contents. Hacking the data from the router and modifying the original data send by source and retransmit the modified to the destination is increase in network technology. So this process is to detect and classify original image from the network transmission.

4.1 REQUIREMENTS OF IMAGE WATERMARKING

An image watermarking system needs to have at least the following two components:

1. A watermark embedding system.
2. A watermark extraction

In this proposed approach, the embedded binary watermark image must be invisible to human eyes and robust to most image processing operations. To meet these requirements, each binary watermark pixel value (0 or 1) is embedded in one block of the host image

4.2 MODULE DESCRIPTION

Image has to transfer from source to destination with security. For providing the security this system consists of the following modules with diagrammatic representations in fig 4.2.

1. Compressing original image with finger print
2. Transfer the compressed file from source to destination
3. Decompressing the Image
4. Identifying modified part in the image.

4.2.1 COMPRESSING ORIGINAL IMAGE WITH FINGER PRINT

In this process the source image with finger print images are compressed. To compress the image DCT algorithm is used.

This algorithm is used for split the image into number of blocks. DCT helps to separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality).The input image is taken as a matrix form (N by M). By using the matrix, intensity of the pixel is arranged in row and column. The DCT coefficients in row and column will be taken. For most images, much of the signal energy lies at low frequencies. These frequencies appear in the upper left corner of the DCT. Compression is achieved since the lower right values represent higher frequencies, and are often small - small enough to be neglected with little visible distortion. The DCT input is an 8 X 8 array of integers. This array contains each pixel's gray scale level; 8 bit pixels have levels from 0 to 255.

$$T= \begin{cases} i/\sqrt{N} & \text{if } i=0 \\ \sqrt{2/N}\ \cos((2j+1)i\prod/2N) & \text{if } i>0 \end{cases} \qquad (4.2.1)$$

By using above step split the original image into 8 X 8 block pixel. With in this block the finger print images will be compressed.

$$D = T\ M\ T' \qquad (4.2.1)$$

The popular block-based DCT transform segments image non-overlapping blocks and applies DCT to each block. This result in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT based watermarking is based on two facts.

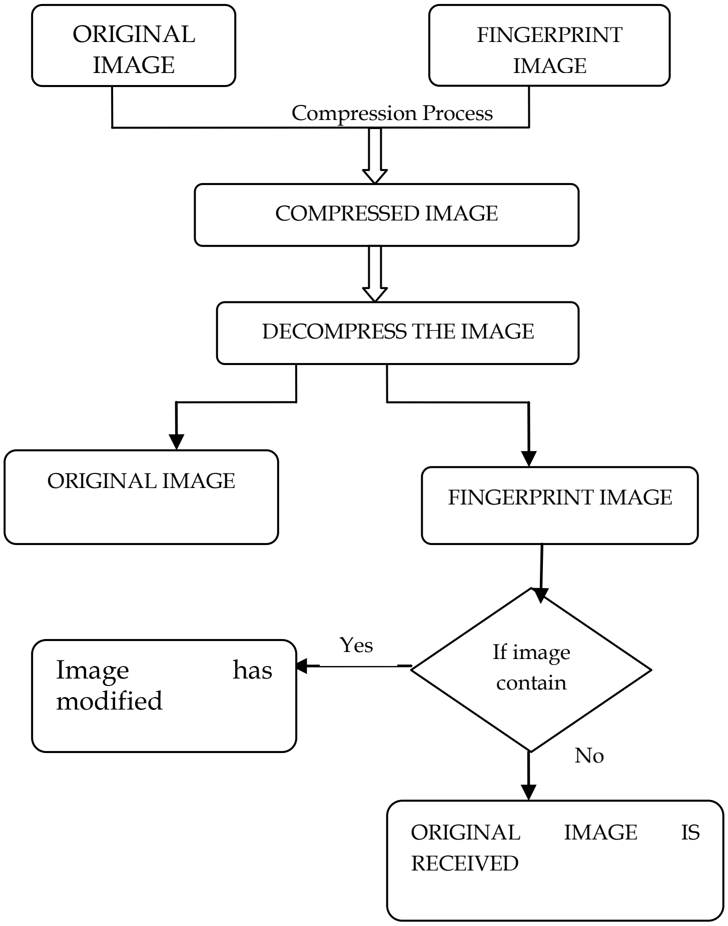


Fig 4.2 Compressing and De compressing the original image

- The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image.
- The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

To compress the image invisible water marking approach is used. In invisible watermarking, information is added as digital data or audio, picture or video, but it cannot seem. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or determine unauthorized copying of digital media. The original image and the finger print images are compressed. The compressed images form a one new image. The Watermark Embedding Process are

1. Load the image to be watermarked (original image). The size of the original image 512 × 512.
2. Load the watermark image. The size of the watermark is 64×64.

3. The host image is divided into a number of blocks; the size of each block is 8×8
4. Guarantee that the number of host image blocks is equal to or greater than the number of watermark pixels.
5. Calculate the variance of each block in the host image in spatial domain.
6. For each host image block compute the DCT transform coefficients.
7. Select the DC component of blocks which has highest variance, and each watermark pixel Wq (0 or 1) is embedded in the DC component Xdc in order as follow:

   $$X'dc = Xdc + M \text{ if } Wq = 1 \qquad (5.3)$$

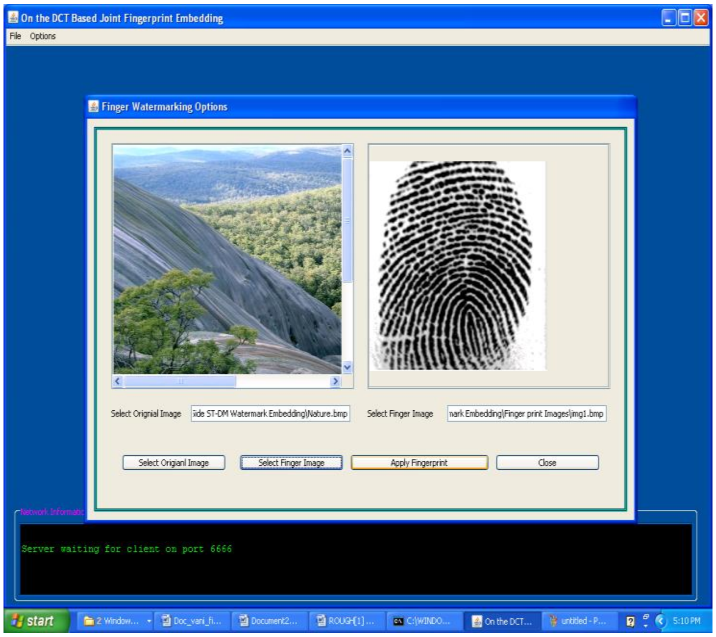
   $$X'dc = Xdc - M \text{ if } Wq = 0 \qquad (5.4)$$

   Where, q =1,2,3,………..rc,

   rc = size of the watermarked image ,

   M = embedding Watermark strength.

8. After embedding the watermark, IDCTtransform is applied for each block, then the Watermarked image is reconstructed



Select Orignial Image: ide ST-DM Watermark Embedding\Nature.bmp

Select Finger Image: nark Embedding\Finger print Images\img1.bmp

```
Server waiting for client on port 6666
```

Fig: 4.2.1 Compressing the Original Image with Fingerprint Image

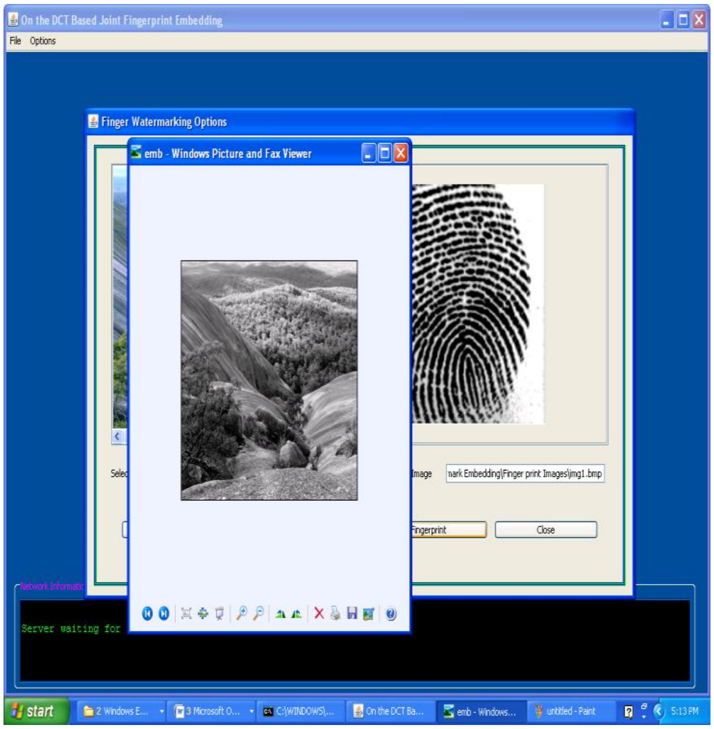


Image: nark Embedding\Finger print Images\img1.bmp

```
Server waiting for
```

Fig: 4.2.1 Embedded Image

4.2.2 TRANSFER THE COMPRESSED FILE FROM SOURCE TO DESTINATION

After embedded a finger print image into the original image file we transfer the compressed image file from source system to destination system. To transfer the file we using the TCP/IP protocol within LAN systems. TCP is one of the core protocols of the Internet protocol suite. The protocol guarantees reliable and in-order (correct order of packets) delivery of data from sender to receiver. To put it simply, it's reliable. The second aspect of TCP is that it is connection oriented. That means TCP requires that a connection be made between the sender and receiver before data is sent. The socket associated with TCP is known as the Stream Socket. The java.net package contains all the classes required to create network enabled applications. Server Socket and Socket are also part of this package. Apart from these classes, it also contains classes to connect to the web server, create secured sockets, and so forth. The Server Socket class provides server sockets or sockets at server side. Such sockets wait for requests over the network. Once such requests arrive, a server socket performs operations based on the request and may return a result. The Server Socket class wraps most of the options required to create server-side sockets. The Socket class provides client-side sockets or simply sockets. They are at the client side connecting to the server, sending the request to the server and accepting the returned result. Server Socket exposes only the compulsory parameters required to create a server-side socket, similarly, Socket asks the user to provide only those parameters that are most necessary.

4.2.3 DECOMPRESSING THE IMAGE

After compressing the original image with finger print image, transmit the compressed image from the source to destination. In the receiver side verification is done using the inverse DCT algorithm on the received image. To verify the image, decompress the received image. While decompressing the image, the original image and the compressed finger print image are separated. While decompression the fingerprint image and the original image will be separated. After getting the finger print image pixel, the modified images can be identified during transmission. Watermark Extraction Process To obtain the extracted watermark from watermarked image, the following procedure was performed:

1. Original image is used for watermark retrieval, as in the embedding process, original
   image and watermarked image are divided into a number of 4×4 blocks.
2. Calculate the DCT transform coefficients for each block in both original image and watermarked image.
3. Watermark extraction process is done by comparing the DC coefficient of each two

Corresponding blocks with the same embedding order as follow:

$W'q = 1$ if $Xw – Xo \geq 0$

$W'q = 0$ if $Xw – Xo \leq 0$

Where Xw = DC coefficient of the watermarked image.

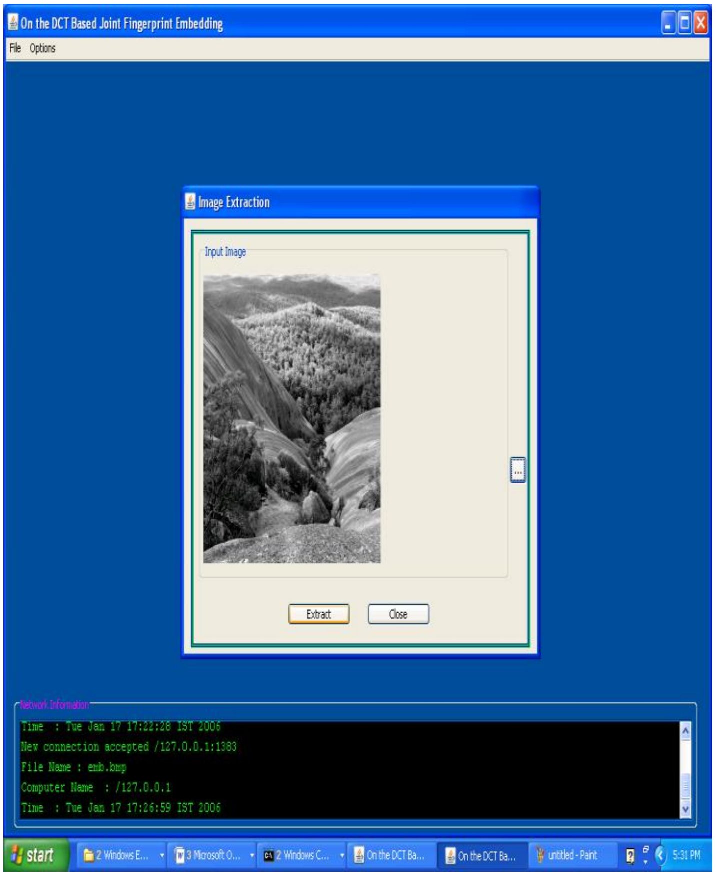
Xo = DC coefficient of t he original image

W'q = extracted watermark pixel.

Then the extracted watermark will be as follow: After extracting the watermark, the normalized cross-correlation (NCC) is calculated to evaluate the effectiveness of our scheme. The normalized cross-correlation is calculated between the original watermark W (i, j), and the extracted W' (i, j).

4.2.4 IDENTIFYING MODIFIED PART IN THE IMAGE

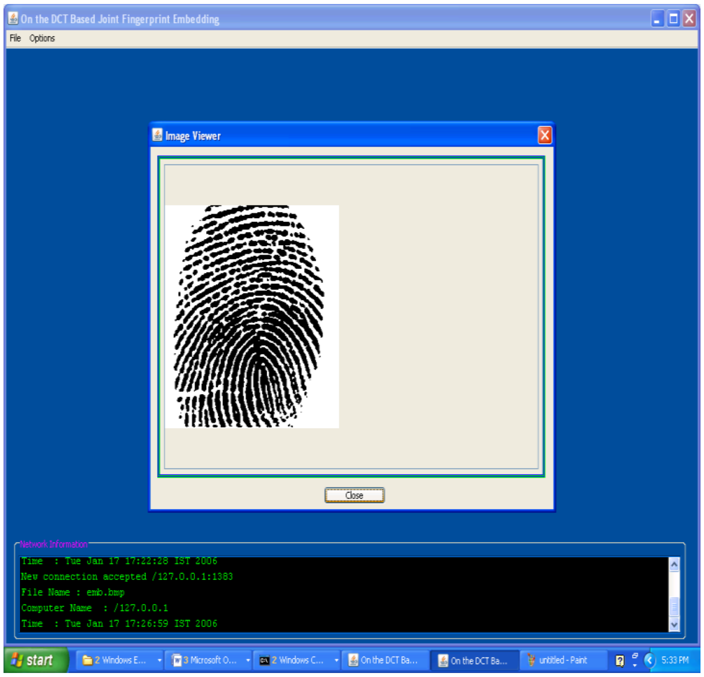
In this module the modified part of the original image will identified. For identifying that, the receiver checks each pixels of the fingerprint image. If any of the blocks has different pixel rate as compared with the finger print image that particular block has modified by the hacker. From this the receiver can easily identify which part of the image has been modified by the hacker.



```
Time  : Tue Jan 17 17:22:28 IST 2006
New connection accepted /127.0.0.1:1383
File Name : emb.bmp
Computer Name  : /127.0.0.1
Time  : Tue Jan 17 17:26:59 IST 2006
```

Fig 4.2.4 Identifying modified part in image.

Intrinsic fingerprint forensic on image coding, which enable us to follow the trace hides in the image and what processes has been applied to the multimedia content which is an important issue in the multimedia forensics and security.



```
Time  : Tue Jan 17 17:22:28 IST 2006
New connection accepted /127.0.0.1:1383
File Name : emb.bmp
Computer Name  : /127.0.0.1
Time  : Tue Jan 17 17:26:59 IST 2006
```

Fig:4.2.4 Retrievinbg the original image.

5. CONCLUSION

Thus the project identifies whether the received image is original or not. The forensic detector does not need any information other than the decoded image at the receiver. Because the unique intrinsic fingerprint of image source encoder embedded in the received image. This approach provides more security than the extrinsic approach such as watermarking. This can be used in military, criminal identification, theft identification. By using the intrinsic fingerprint of each source code, the digital image has more security than the watermarking approach.

6. FUTURE ENHANCEMENT

Watermarking is most popularly used approach for providing security on images. Under many circumstance watermarking approach is not possible for providing the security. Because of the visibility of the security message, the hackers can create the watermarking on the original image as like the sender sent and then send the modified image to the receiver. Everyone can read the copyright information. To solve the problems in watermarking approach the unique intrinsic fingerprint of the image source coders are taken as the evidence for security. Based on the intrinsic fingerprint of image source encoders, forensic detector is developed. This detector identifies which source encoder is applied, what the coding parameters are along with confidence measures of the result. In future, multiple images can also send through the network by using the finger print of the sender.

REFERENCES

[1]. A. K. Jain, A. A. Ross,K.Nandakumar, Introduction to Biometrics, Springer, 2011, 311 p.

[2]. Alessandro Piva., Alessia De Rosa., and Tiziano Bianchi.(2010) 'Secure Client-Side ST-DM Watermark Embedding', IEEE Trans. On Information Forensics and Security,Vol.5,No.1,March.

[3]. Avcibas, I.,Bayram, S., Memon, N., and Sankur, B (2006) 'Image manipulation detection," Journal of ElectronicImaging, Volume 15, Issue4, 041102 (17 pages), vol.15(4).

[4]. Buccigrossi, R.W. and Simoncelli, E.P. (1999) 'Image compression via joint statistical characterization in the wavelet domain', IEEE Transactions on Image Processing, 8(12):1688.1701.

[5]. Christopoulos, C., and Nister, D. (1997) 'An embedded DCT-based still image coding algorithm', ISO/IEC JTC1/SC29/WG1 N610, November 10-14, Sydney, Australia.

[6]. Christopoulos, C., and Nister, D. (1997) 'An embedded DCT-based still image coding algorithm', ISO/IEC JTC1/SC29/WG1 N610, November 10-14, Sydney, Australia.

[7]. Farid, H., and Popescu, A.C. (2005) 'Exposing digital forgeries by detecting traces of resampling', IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767.

[8]. Fridrich, F., Lukas, J., and Soukal, D. (2003) 'Detection of Copy-Move Forgery in Digital Images', Digital Forensic Research Workshop, Cleveland, USA, Aug.

[9]. Friedman, G. L. (1993) 'The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image', IEEE Trans. Consumer Electron. Vol. 39, pp. 905-910.

[10]. Kirovski, D., Potkonjak, M., and Wong, J. L.(2004) 'Computational forensic techniques for intellectual property protection', IEEE Trans. On Computer-Aided Design of Integrated Circuits and Systems, vol. 23, no.6, pp. 987–994, Jun.

[11]. Ray Liu, K.J.,Sabrina Lin, W., Tjoa, K., and Vicky Zhao, H. (2009) 'Digital Image Source Coder Forensics via Intrinsic Fingerprints', IEEE Transactions On Information Forensics And Security, Vol. 4, No. 3, September.