International Conference on Advances in Materials, Computing and Communication Technologies
In Association withInternational Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

Secure Data Transmission Using Water Marking and Encryption Technique

J. Jeejo Vetharaj[1], S. Nandhini[2], C. Anjali[2]

[1]Assistant Professor, Department of CSE, Marthandam College of Engineering & Technology, Tamil Nadu, India

[2]Final Year Student, Department of CSE, Marthandam College of Engineering & Technology, Tamil Nadu, India

ABSTRACT

Data security is a main concern in everyday data transmissions in the internet. A possible solution to guarantee secure and legitimate transaction is via hiding a piece of tractable information into the multimedia signal., i.e, watermarking. To ensure the security of information various security concepts our project proposes a group of two algorithms such as, DCT and RSA algorithms to provide copy right protection to the digital data. The main framework of our proposed method securely hides binary information in color image media, and securely extracts and authenticates it using a secret key. Experimental results prove that our proposed invisible watermarking techniques is resilient to 90% of the well-known benchmark attacks and hence a failsafe method providing constant protection to the ownership rights.

Index Terms—Multimedia security, Discrete cosine transform technique, Rivets Shamir alderman technique, copyright protection

I. INTRODUCTION

An image may be defined as two-dimensional function, f(x, y), where x and y are spatial coordinates, and the amplitude of any pair of coordinates (x, y) is called the intensity or gray level of the image at that point .When x, y and the amplitude values of f are all fine, discrete quantities, we call the image as digital image. The field of digital image processing refers to the processing of digital image by means of a digital computer. Note that a digital image is composed of a finite number of elements, each of which has a particular location and value. These elements are referred to as picture elements, image elements and pixels. Pixel is the term most widely used to denote the elements of a digital image.

II. DIGITAL WATERMARKING

Digital watermark is an invisible mark embedded in a digital image which may be used for a number of different purposes including image captioning and copyright protection. With the rapid development of modern communication networks, information is transmitted with speeds never seen before. At the same time, illegally manipulated copies of digital media can be easily transmitted and distributed. As a result, copyright protection has become a major issue

worldwide. Digital watermarking is a promising technique to tackle this problem.

This project focuses on image watermarking. A good image- watermarking method should be imperceptible, robust, and secure. Imperceptibility means that watermarks should be perceptually unobtrusive watermarks after undergoing different kinds of attacks. There are two types of attacks, which are signal processing attacks and geometric attacks. Security refers to the resistance to unauthorized watermark decoding without knowing the secret key. Over the last decade, various image- watermarking methods have been developed. Many of these methods are robust to common signal processing attacks but do not cope well with geometric attacks.

III. COMMUNICATION-BASED MODELS

Communication-based models describe watermarking in a way very similar to the traditional models of communication systems. Watermarking is in fact a process of communicating a message from the watermarking embedded to the watermarking receiver. Therefore, it makes sense to use the models of secure communication to model this process. In a general secure communication model we would have the sender on one side, which would encode a message using some kind of encoding key to prevent eavesdroppers to decode the message if the message was intercepted during transmission. Then the message would be transmitted on a communications channel, which would add some noise to the noise to the encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back. In general, communication-based watermarking models can be further divided into two sub-categories. The first uses side-information to enhance the process of watermarking and the second does not use side-information at all.

The term side information refers to any auxiliary information except the input message itself that can be used to better encode or decode it. The best example encoded message. The resulting noisy message would be received at the other end of the transmission by the receiver, which would try to decode it using a decoding key, to get the original message back. In general, communication-based watermarking models can be further divided into two sub-categories. The first uses side-information to enhance the process of watermarking and the second does not use side-information at all.

The term side information refers to any auxiliary information except the input message itself that can be used to better encode or decode it. The best example of this is the image used to carry the message, which can be used to provide useful information to enhance the correct detection of the message at the receiver.

IV. WATERMARKING PROPERTIES

Every watermarking system has some very important desirable properties. Some of these properties are often conflicting and we are often forced to accept some tradeoffs between these properties depending on the application of the watermarking system. The first and perhaps most important property is effectiveness. This is the probability that the message in a watermarked image will be correctly detected. We ideally need this probability to be 1. Another important property is the image fidelity. Watermarking is a process that alters an original image to add a message to it, therefore it inevitably affects the image's quality. We want to keep this degradation of the image's quality to a minimum, so no obvious difference in the image's fidelity can be noticed. The third property is the payload size. Every watermarked work is used to carry a message. The size of this message is often important as many systems require a relatively big payload to be embedded in a cover work. There are of course

applications that only need a single bit to be embedded.

The false positive rate is also very important to watermarking systems. This is the number of digital works that are identified to have a watermark embedded when in fact they have no watermark embedded. This should be kept very low for watermarking systems.

Lastly, robustness is crucial for most watermarking systems. There are many cases in which a watermarked work is altered during its lifetime, either by transmission over a lossy channel or several malicious attacks that try to remove the watermark or make it undetectable. A robust watermark should be able to withstand additive Gaussian noise, compression, printing and scanning, rotation, scaling, cropping and many other operations.

V. CLASSIFICATION OF DIGITAL WATERMARKING

Image watermarking techniques can be classified from five perspectives as shown below:

Based on Visibility:

Watermarks may be visible or invisible. A visible watermark is easily detected by observation while an invisible watermark is designed to be transparent to observer and detected using signal processing techniques.

Based on Application:

The watermarking techniques are classified based on application such as copyright protection or authentication. Copyright protection is useful for ownership verification. Image authentication systems have applicability in law, commerce and journalism.

Based on Fragility:

Based on fragility, watermarking schemes are classified as fragile, semi fragile. A fragile watermark is designed to detect slight changes to watermarked image with high probability. Fragile watermarking is used for content authentication and tamper detection. Semi schemes are used to discriminate between malicious manipulations.

Based on Extraction:

Image watermarking is classified as blind, semi blind or non blind. In blind watermarking, watermark is extracted without original image thus reducing storage requirements.

Semi blind watermarking does not use original image for detection but answers the question in positive or negative form. Non blind watermarking systems require original image for extraction. This kind of scheme is more robust than others because it requires access to secret material.

Based on Domain of Transformation:

In spatial domain methods, watermark information is embedded directly into image pixels. The images are manipulated by altering one or more number of bits that make up pixels of the image. In frequency domain methods, watermark information is embedded in the transform domain.

VI. EMBEDDING PROCESS

The watermark-embedding process consists of four steps: Gaussian filtering, histogram construction, pixel group selection, and HFCM based watermark embedding.

Gaussian Filtering:

It is known that robustness to common signal processing attacks can be achieved by embedding watermarks into the low-frequency component of an image. Thus, we first pre-process the host gray scale image I by a 2-D Gaussian low- pass filter

$$F(x, y,\sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{-x^2+y^2}{2\sigma^2}}$$

where (x, y) denotes the position of the pixel and σ is the standard deviation of the distribution, which is

usually chosen as σ =1 The filtered image for the high-frequency component removed by the Gaussian filtering from the host image I, it follows the size of the Gaussian mask F is often chosen using expression (2kσ +1)×(2kσ +1), where k is a positive integer.

Since 99.7% energy of the Gaussian distribution is concentrated

within three standard deviations from the mean, we can set k to be 3. Thus, the size of the Gaussian mask F used is 7×7.

Histogram Construction:

Assume that the filtered image has K gray levels, e.g., an 8-bit gray scale image has K = 256 gray levels, ranging from 0 to 255. The histogram of an image illustrates the number of pixels versus the gray level values.

Clearly, the shape of the histogram is related to the image content. To introduce security into our method, a pseudo-used as a security key to randomly select S gray levels from the K available gray levels, where K/2≤ S < K. Each element of p(n) randomly takes an integer from the range [0, K – 1], if i = j. Denoting the S selected gray levels by K1, K2,...,KS, the ith selected gray level Ki is given by Ki = p(i).

Pixel Group Selection:

After constructing the histogram HS, we take each LB neighboring gray levels in HS to form a bin. In total, one can form

$MB = S/LB$

Further, we take each two neighboring bins to form a group, which will yield $MB/2$ groups. Next, we select the pixel groups that are suitable for hiding watermarks. Let NS be the total number of pixels corresponding to the S selected gray levels

$N = \sum S\ h\ (K\ )$

$S \quad i=1\ S \quad i$

To make the selection of pixel groups adaptive to the histogram shape, we propose a pixel group selection criteria based on the ratio between $hG(i)$ and NS , i.e.,

g(i)= $hG(i)$

NS

where i = 1,2,..., $MB/2$

based on which is insensitive to common geometric attacks, including cropping attacks and RBAs, which is essential to tackling geometric attacks. If g(i) is greater than a predetermined threshold TG, the ith pixel group is considered to be suitable for watermark embedding.

The threshold TG balances robustness and embedding rate. The larger TG, the higher robustness due to more pixels in the group but the lower embedding rate as fewer pixel groups will be chosen for watermark embedding. In this paper, TG is empirically chosen as TG= Total number of image pixels $4LB$

noise (PN) sequence p(n)=[p(1), p(2),...,p(K)] of length K is

VII. APPLICATIONS OF WATERMARKING

The main applications of digital watermarking are

- Copyright protection
- Content archiving
- Broadcast monitoring
- Tamper detection

RSA Decomposition:

RSA stands for Rivest, Shamir, Adleman. These are the creators of the RSA Algorithm. It is a public-key encryption technique used for secure data transmission especially over the internet. In RSA, the public key is generated by multiplying two large prime numbers p and q together, and the private key is generated through a different process involving p and q. A user can then distribute his public key pq, and anyone wishing to send the user a message would encrypt their message using public key. For all practical purposes, even computers cannot factor large numbers into the product of two primes, in the same way that factoring a number like 414863 by hand is virtually impossible. However, multiplying two numbers is much less difficult, so a potential factorization can be verified quickly. When the user

receives the encrypted message, they decrypt it using the private key and can read the original text.

VIII. WATERMARK-EMBEDDING PROCESS

The watermark-embedding process of the method is shown in Figure below.

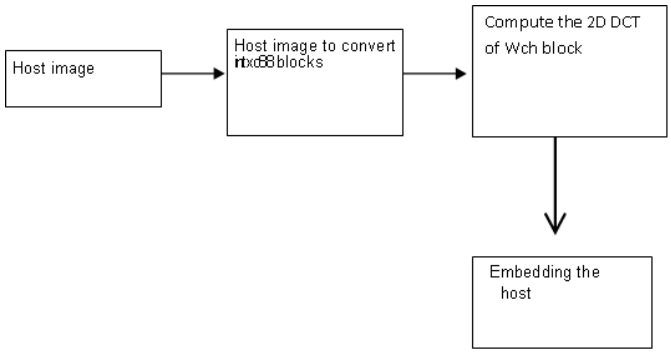

Fig: Block diagram of watermark-embedding process

IX. IMAGE PROCESSING TOOLBOX PRODUCT DESCRIPTION

Image Processing Toolbox provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Many toolbox functions support multi-core processors, GPUs, and C-code generation.

Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and homographic. Visualization functions and apps let you explore images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest (ROIs). The toolbox supports workflows for processing, displaying, and navigating large images.

X. CONCLUSION

Thus working of Combined DCT-RSA Watermarking Technique used for question paper protection. The DCT and RSA provide high robustness and imperceptibility to the question paper image. This software provides security, copyright protection and data authenticity to question paper image. In this paper, it also describes a watermarking algorithm based on combining two transforms; DCT and RSA, Watermarking is done by altering the wavelets coefficients. The robustness of the proposed watermarking scheme against compression, filtering, noise, histogram modification and geometric attacks has also been studied and shown to be more robust than the other existing schemes.

XI. REFERENCES

[1]. J.J.K.O.Ruanaidh, T.Pun et al(2000),'Rotation, scale and translation invariant spread spectrum digital image watermarking'.

[2]. C.Lin, J.A.Bloom, (2001) et al,' Rotation, Scale, and Translation Resilient Watermarking for Images'.

[3]. J.F.Lichtenauer, I.Setyawan, (2002)et al, 'Exhaustive Geometrical Search and the False Positive Watermark'.

[4]. P.Dong, Y.Yang, (2003)et al,'Geometric Robust Watermarking Based on a New Mesh Model Correction Approach'.

[5]. M.Barni, (2005)et al, 'Effectiveness of Exhaustive Search and Template Matching Against Watermark Resynchronization'.

[6]. A.Reddy, B.Chatterji, (2005)et al,' A New Wavelet Based Logo –Watermarking Scheme'.

[7]. J.Zheng, (2008)et al,' A Color Image Watermarking Scheme In The Associated Domain Of DWT-DCT Domains Based On Multi-Channel Watermarking Framework'.

[8]. S.Bedi, Piyush Kapoor , (2009)et al, 'Robust Secure SVD Based DCT- DWT Oriented Watermarking Technique For Image Authentication'.

[9]. M.Lee, K.S.Kim, H.K.Lee, (2010)et al,'Digital Cinema Watermarking for Estimating the Position of the Pirate'.

[10]. N.K.Kalantari, S.M.Ahadi, (2010)et al,'A Robust Image Watermarking in the Ridgelet Domain Using Universally Optimum Decoder'.

[11]. H.Zhang, (2011)et al,'Affine Legendre Moment Invariants for Image Watermarking Robust to Geometric Distortions'.

[12]. E.Nezhadarya, Z.J.Wang, (2011)et al,'Robust Image Watermarking Based on Multi-scale Gradient Direction Quantization'.