Amandeep Kaur, Sukhjeet K. Ranade, Megha Kansal / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.2282-2287

Collusion Resistant Fingerprinting In DCT Domain

Amandeep Kaur[*], Sukhjeet K. Ranade[**], Megha Kansal[***]
[#] CSE Department, Punjabi University Patiala, India

Abstract

Digital fingerprinting is a technique for identifying users who use multimedia content for unintended purposes, such as redistribution. These fingerprints are typically embedded into the content using watermarking techniques that are designed to be robust to a variety of attacks. A cost-effective attack against such digital fingerprints is collusion, where several differently marked copies of the same content are combined to disrupt the underlying fingerprints.

Anti-Collusion Codes (ACCs) are employed to design the fingerprints, which can accommodate more users than orthogonal modulation based fingerprints with the same amount of signals. The selected DCT coefficients of the original image are quantized according to fingerprints; quantization table is employed to improve the ability of anti-compression. Blind fingerprint detection scheme has larger capacity and is more efficient than the existing algorithms.

Keywords— Fingerprinting, Collusion attack, Quantization

I. INTRODUCTION

With the advancement of multimedia technology and internet, a large amount of multimedia content is distributed through networks. In order to protect the sensitive nature of multimedia data that is shared by a group of users, as well as protect the commercial value of content after it has been delivered to subscribers, solutions must be developed to provide the ability to track and identify persons involved in unauthorized redistribution of multimedia content. Digital Fingerprinting is a class of technologies whereby unique labels, known as *digital Fingerprints*, are inserted in different copies of the same content before distribution.

According to the function of digital fingerprint, the digital fingerprint model needs following characteristics: The production being protected can't risk appreciable quality degradation when embedding the digital fingerprint. PSNR is used to measure the transparency of watermark. Digital fingerprint should resist possible disposal, operation and attack so that the information being extracted can trace illegal distributor. It needs adequate information after being attacked by user to trace by distributor. So it needs enough embedded capacity. When users attack together, the distributor should at least find out one illegal distributor after the precondition that has no entanglement innocent purchaser. It needs the generating algorithm and tracing algorithm has very high efficiency. General process of image fingerprinting embeds data into a host image. The ground process of fingerprinting is depicted in figure 1. The process constitutes of three phases; embedding a fingerprint, during transmission it may undergo some possible attacks and tracing the pirate. A unique fingerprint is assigned to each intended recipient, which facilitates the tracing of the culprits who illegally distribute their data. To protect the content, it is difficult to remove the fingerprint from the content. For multimedia content, fingerprints can be embedded using conventional watermarking techniques that are robust against the variety of attacks mounted by an individual. The global nature of the internet has brought adversaries closer to each other. It is now easy for a group of users with differently marked versions of the same data to work together and collectively mount attacks against the fingerprints. These attacks are known as multiuser collusion attacks. These attacks provide a cost-effective method for attenuating each of the colluders' fingerprints.

An improperly designed embedding and identification scheme may be vulnerable in the sense that a small coalition of colluders can produce a new version of the content with no detectable traces. Collusion poses a real threat to protecting media data. So it is desirable to design fingerprints that resist collusion and identify the colluders.

In this Paper, we first provide background on robust data embedding, upon which the multimedia fingerprinting system is built. We also introduce the basic concepts of fingerprinting and collusion and provide a discussion on the various goals associated with fingerprint design and colluder tracing in section 2. In section 3, the fingerprint embedding using quantization theory is illustrated. We also present the fingerprint detection and colluder tracing.

II. THE BACKGROUND

Fingerprinting multimedia requires the use of robust data embedding methods that are capable to resist attacks that adversaries might employ to remove the fingerprint. Collusion-resistant fingerprinting also requires that the fingerprints survive collusion attacks and can identify colluders. The earliest concept of fingerprinting used to identify the users was proposed by Wagner in 1983 [1]. Now with the development of multimedia technologies the current fingerprinting focuses on tracing colluders.

A lot of fingerprinting algorithms has been proposed for code, through which colluders can be traced. The other one studies the performance of orthogonal fingerprinting and embedding methods [5], this technique has been studied extensively. Orthogonal fingerprints are easy to encode and embed, which makes them attractive to identification applications that involve a small group of users.

performance is high when the JPEG compression is moderate,
but it reduces sharply when the JPEG quality factor reduces further. Another problem is that the capacity of fingerprint is limited. So exploring the blind detection method is key research direction [6].Considering all the factors, we propose a

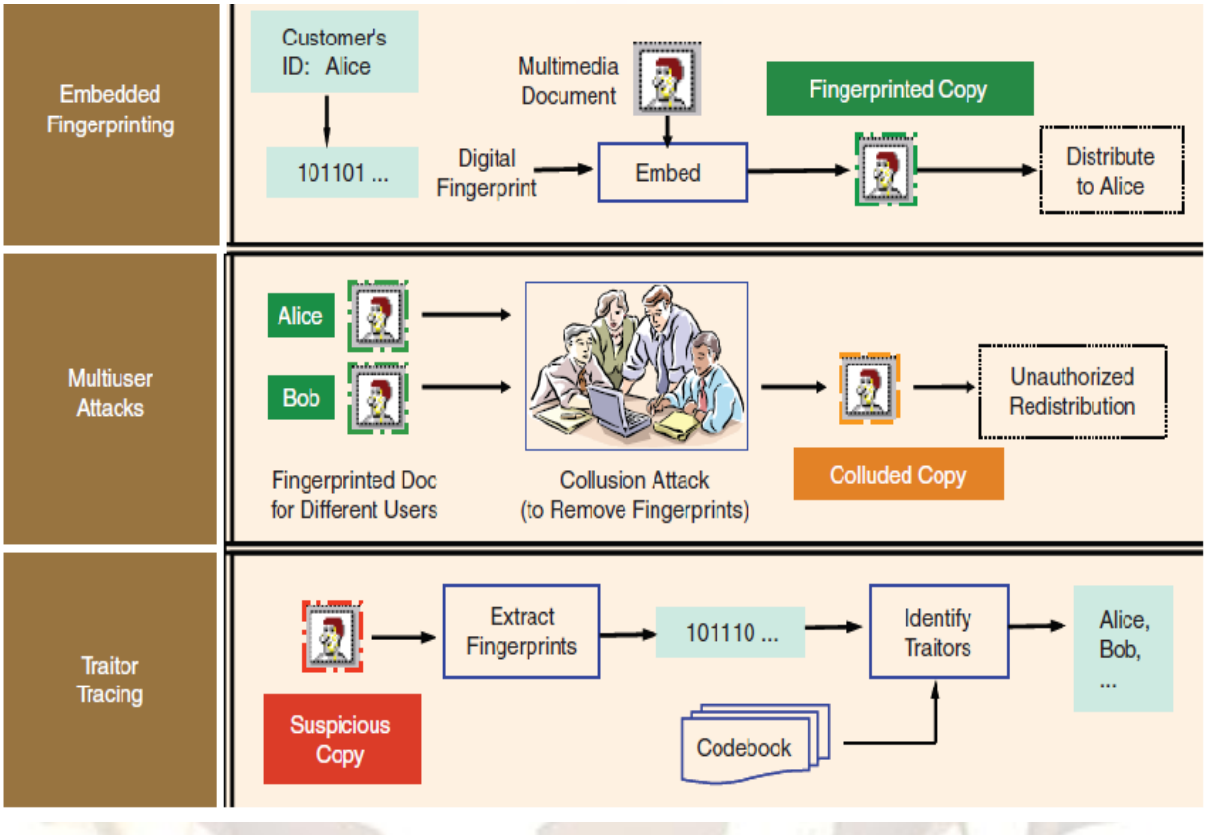

Fig. 1 Using Embedded Fingerprinting for Tracing Users

The problem is that with the increase in number of fingerprints the orthogonal basic vectors will be increased. To overcome this problem Trappe introduced an Anti-Collusion Code (ACC) same length of fingerprint code. The most existing methods are non blind detection means that original signal is required during fingerprints detection. Spread spectrum method is to embed ACC modulated fingerprints, which can detect the fingerprints blindly. However, original fingerprints and the test signals has are very small the correlation based detection statistics when the original signals were not removed and it lead to low probability of right detection and high probability of wrong detection. The performance drops sharply when the colluded version is added some noise. Ashwin proposed a fingerprinting scheme based on Quantization Index Modulation (QIM) [7], where he used the spread transform dither modulation to embed fingerprints. The tracing blind fingerprint detection scheme in this paper. We employ the random vectors modulated with the fingerprints and embed them by quantizing the DCT coefficients of the original images. By using Euclidean distance classification method we can trace the colluder. The proposed scheme can effectively detect fingerprints from the collusion copies without using original images.

A. Collusion attack on fingerprinting

Collusion attacks can be classified as linear collusion attacks and non linear collusion attacks.
Linear collusion is one of the most feasible collusion attacks. When users come together with the total of K differently fingerprinted copies, then they can simply combine the K signals to produce the colluded version. These attacks can be categorised as:
Average Attack*:* The K fingerprinted copies are typically averaged with an equal weight for each user

to produce a pirated image. . As the number of traitors increases, the quality of the pirated image improves exponentially. This fact may elude users to join the traitor group in order to get a high quality copy of an image.

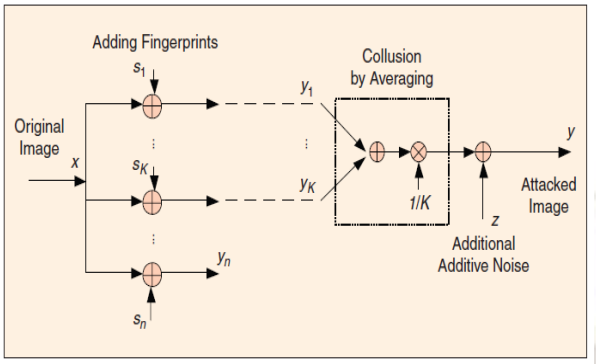

Fig. 2 collusion attack by averaging

2) **Cut and paste attack***:* Copy and paste attack, involves users cutting out portions of each of their media signals and pasting them together to form a new signal

3) **Linear combination collusion attack (LLCA):** This attack is generalization of the average attack model .LLCA generates a pirated image of good quality but prevent traitors from being identified.
Nonlinear attacks are also very useful. Class of nonlinear attacks is based upon operations such as taking the maximum, minimum, and the median of corresponding components of k colluders' independent watermarked copies. Non linear can be classified as following.

*1***) Minimum/maximum/median attack:** Under these three attacks, the colluders create an attacked signal in which each component is the minimum, maximum, and median, respectively, of the corresponding components of the K watermarked signals associated with the colluders.

2) Minmax attack: Each component of the attacked signal is the average of the maximum and minimum of the corresponding components of the K watermarked signals.

*3***) Modified negative attack:** Each component of the attacked signal is the difference between the median and the sum of the maximum and minimum of the corresponding components of the K watermarked signals.

*4***) Randomized negative attack:** Each component of the attacked signal takes the value of the maximum of the corresponding components of the K watermarked signals with probability p, and takes the minimum with probability (1 – p).

B. **Techniques in fingerprinting:**
Fingerprinting techniques can be categorized into spatial domain watermarking and transform domain watermarking.

1) Spatial domain watermarking:
This domain hides the information into the spatial domain. It encodes the extra information into the image by making small modifications into large number of pixels. The simplest example of spatial domain fingerprinting is LSB (least significant modification) method.

2) Transform domain watermarking:
Generally DCT, FFT and wavelet Transform are used as the methods of data transformation. The main strength offered by transform domain technique is that they can take the advantage of special properties of alternate domains to address the limitations of pixel based methods or to support additional features. Designing a fingerprint in DCT domain leads to better implementation compatibility. The frequency domain fingerprinting schemes are more robust than spatial domain watermarking schemes, particularly in lossy compression, noise addition, noise addition, pixel removal, rescaling, rotation and shearing. Generally, the main drawback of Transform domain methods is their higher computational requirement. Fourier transform analyse a signal in the time domain for its frequency content. This Fourier transforms work by translating a function in the time domain into a function in the frequency domain. The signal can then be analysed for its frequency content because the Fourier coefficients of the transformed functions represents the contribution of each sine and cosine function at each frequency.

C. **Applications of fingerprinting**
The various applications of fingerprinting are as following.
1) Copyright Control. Cross-referencing actual usage rights and permissions in a fingerprint database will facilitate monitoring of authorized and unauthorized uses of content. Content producers and distributors will use fingerprints to determine whether a database contains unauthorized content. Stock footage providers will use fingerprints to spot the clips they license in commercial programming.

2) Metadata: Metadata allows content creators to store all sorts of useful tracking information associated with content.

3) Behavioral Modeling Advertising*:* Interest-based or behavioral advertising matches ads to individuals based on a user's past online activities, such as visiting a website or searching for information on a particular subject. It also brings behavioral advertising models to new domains, such as VOD

services and cable television where signals must pass through a set-top box.

4) Copy Protection: Video fingerprints can be used as a copy protection tool. For example, both a video fingerprint and an authenticating signature could be required before a file could be copied or replicated.

5) Forensics: Another promise of video fingerprinting is in the area of information forensics where fingerprints could be used to detect whether video footage has been manipulated. Research is ongoing in this area.

6) Additional Business Opportunities: Digital fingerprints must be matched against extensive content ownership databases to be effective. It stands to reason that maintaining, licensing and managing access to large-scale fingerprint databases is a potential revenue opportunity. Audible Magic, for example, has already established a subscription based business leveraging its extensive ownership database.

III. PROPOSED SCHEME

The implementation process of fingerprinting can be divided into three stages; Pre-processing using Discrete Cosine Transform, Training using Quantization, Classification.

A. Discrete Cosine Transform and its Implementation

The DCT is a technique for converting a signal or image into elementary frequency components. It represents the image as a sum of sinusoids of varying magnitudes and frequencies. It has the property for images without sharp discontinuities; most of the spectral power is in the first few terms, which allows the later one to be ignored without too much information loss. The (0, 0) element is referred as the DC component and the other values are the AC components as shown in fig 3.

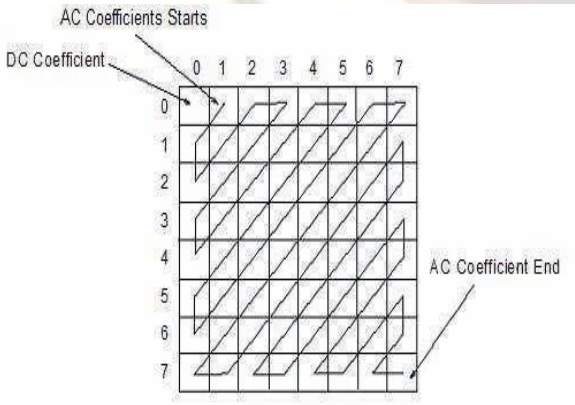

Fig. 3 Zigzag Pattern of DCT components

If we input image f(x, y), the DCT coefficients for the transformed output image F (u, v) of input image N×M pixels are computed using the following equation:

For an M×N image, where each image corresponds to a 2D matrix, DCT coefficients are calculated as follows:

$$F(u,v)\frac{1}{\sqrt{MN}}\alpha(u)\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}f(x,y)\cos\left(\frac{(2x+1)u\pi}{2M}\right)\cos\left(\frac{(2y+1)v\pi}{2N}\right)$$

U=0, 1… M, V=0, 1… N

Where,

$$\alpha(u)=\begin{cases}\frac{1}{\sqrt{M}} & u=0\\ \sqrt{\frac{2}{M}} & u=1,2,\dots,M-1\end{cases}$$

$$\alpha(v)=\begin{cases}\frac{1}{\sqrt{N}} & v=0\\ \sqrt{\frac{2}{N}} & v=1,2,\dots,M-1\end{cases}$$

F (x, y) is the image intensity function and F (u, v) is a 2D matrix of DCT coefficients. Block-based implementation and the entire image are the two implementations of the DCT. The DCT is applied to the entire image to obtain the frequency coefficient matrix of the same dimension. Fig. 4 a and b shows a typical face image and its DCT coefficients image.

In general, the DCT coefficients are divided into three bands (sets), namely low frequencies, middle frequencies and high frequencies. Fig. 4 visualizes these bands. Low frequencies are correlated with the illumination conditions and high frequencies represent noise and small variations (details). Middle frequencies coefficients contain useful information and construct the basic structure of the image. From the above discussion, it seems that the middle frequencies coefficients are more suitable.

Fig. 4 Low Middle High

B. Embedding using quantization

Quantization, involved in image processing, is a lossy compression technique achieved by compressing a range of values to a single quantum value. When the number of discrete symbols in a given stream is reduced, the stream becomes more compressible. For example, reducing the number of colors required to represent a digital image makes it possible to reduce its file size. A typical video codec works by breaking the picture into discrete blocks (8×8 pixels). These blocks can then be subjected

to discrete cosine transform (DCT) to calculate the frequency components, both horizontally and vertically. The resulting block (the same size as the original block) is then pre-multiplied by the quantization scale code and divided element-wise by the quantization matrix, and rounding each resultant element. The quantization matrix is designed to provide more resolution to more perceivable frequency components over less perceivable components (usually lower frequencies over high frequencies) in addition to transforming as many components to 0, which can be encoded with greatest efficiency. Many video encoders and compression standards allow custom matrices to be used. The extent of the reduction may be varied by changing the quantizer scale code, taking up much less bandwidth than a full quantizer matrix. Typically this process will result in matrices with values primarily in the upper left (low frequency) corner. By using a zig-zag ordering to group the non-zero entries and run length encoding, the quantized matrix can be much more efficiently stored than the non-quantized version. This procedure is used to add the finger print in to the image as shown in Fig. 5.

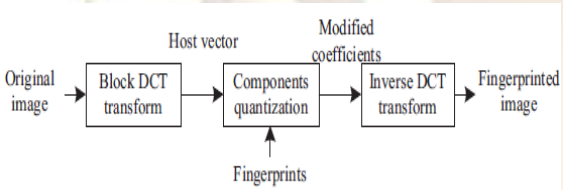

Fig. 5 Diagram of fingerprint embedding

$$d_1' = \left\lfloor \frac{d1 - X}{2} \right\rfloor * \Delta + X$$

$$d_0' = \left\lfloor \frac{d0 - X}{2} \right\rfloor * \Delta + X$$

Where, d0 and d1 are corresponding values of pixel after DCT transform and Δ is quantization step for binary values it will be 2 and X is any random number and bi is bit to be embedded.

$$X = \begin{cases} 0 < X < 1, & if\ bi = 0 \\ 1 < X < 2, & if\ bi = 1 \end{cases}$$

1) Algorithm:

Fingerprint embedding stage includes following steps:

1. Construct the fingerprint database. The size of fingerprint is less than or equal to the size of original image.
2. Calculate the DCT coefficients of samples images as described in previous phase.
3. Calculate the average value d_1' and d_0' of image by using formula given above.
4. Add the resultant values in to the resultant image.
5. Apply Inverse DCT on resultant image to get the watermarked image.

C. **Colluder Tracing**

The classification rule used to trace colluder is the Nearest Neighbor. This is a simple nonparametric classifier where the most likely class of the query face is decided by finding the neighbour with minimum distance between the features of query and all prototypes using Minimum Euclidean distance . It is having two vectors X, Y,

$$d(X,Y) = \sum_{i=1}^{n} (x_i - y_i)^2$$

By using same procedure and Euclidean distance classification method we can trace the colluder as shown in fig. 6.

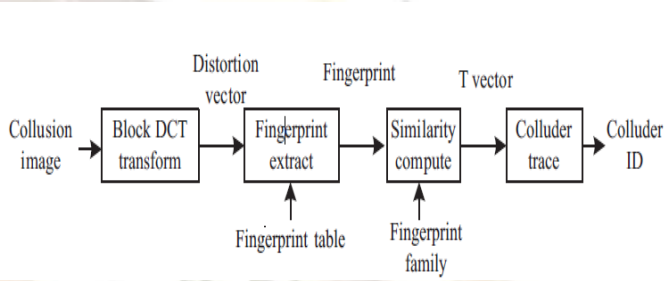

Fig. 6 Diagram of colluder tracing

1) Algorithm:

1. Calculate the Euclidean distance between the training and test classification space projection, Y′ and Y respectively, and prepare the distance matrix.
2. Select the minimal distance from the prepared matrix.
3. Output the class of the image with minimal distance.

The test image is assumed to be in the class whose distance is the minimal among all other class distance.

IV. CONCLUSIONS

This paper will implement capacity improved fingerprinting scheme in DCT domain. Though many fingerprinting schemes have been studied, few of them are blind. Blind fingerprint detection scheme has larger capacity and is more efficient than the existing algorithms but its performance is not good enough as non-blind detection. Studying robust fingerprinting resisting collusion attack with blind detection is an important work in the future.

REFERENCES

[1] N.R. Wagner. "Fingerprinting," In: Proceedings Symposium on Security and Privacy.1983. on Information and Theory, Sep 1998, pp.1897–905.

[2] I. Cox, J. Bloom, and M. Miller, "Digital Watermarking: Principles & Practice.," San Mateo, CA: Morgan Kaufman, 2001.

[3] Dan Boneh and J. Shaw, "Collusion-secure Fingerprinting for digital data," IEEE Trans. on Information Theory, vol.44 , Sep. 1998, pp. 1897-1905.

[4] W. Trappe, M. Wu, and Z.J. Wang," Anti-collusion fingerprinting for multimedia,"IEEE Transactions on Signal Process, April 2003, pp.1069–1087.

[5] Z.J Wang, M. Wu, H.V Zhao, W. Trappe, and K.J.R Liu," Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," IEEE Transactions on Image Processing, June 2005, pp.804–821.

[6] M. Wu, W. Trappe, Z. Wang, and K.J.R. Liu ,"Collusion Resistant Fingerprinting for Multimedia", IEEE Signal Processing Magazine, Special Issue on Digital Rights management, 2004, pp. 16-24.

[7] Swaminathan A, He S, Wu M. "Exploring QIM-based anti-collusion fingerprinting for multimedia," In: Proc. SPIE/IS&T, Security, Steganography, and Watermarking of Multimedia Contents. 2006.

[8] Trappe W, Wu M, Liu KJR, "Anti-collusion fingerprinting for multimedia," IEEE Transactions on Signal Processing April 2003, pp.1069–86.

[9] Zhao HV, Wu M, Wang ZJ, Liu KJR, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," IEEE Transactions on Image Processing , May 2005 pp. 646–61.

[10] Cox I, Kilian J, Leighton F, Shamoon T. "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, December 1997,pp.1673–87.

[11] Podilchuk C, Zeng W. "Image adaptive watermarking using visual models," IEEEJournal of Selected Areas in Communications , May 1998, pp. 525–40.

[12] Chen B, Wornell GW. "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," IEEE Transactions on Information Theory, May 2001, pp. 1423–43.