Global Journal of Computer Science and Technology
Volume 12 Issue 9 Version 1.0 April 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Robust Digital Watermarking for Color Images Using Fuzzy Vault

By Priyanka D. Godase, Snehal B. Kale, Sonika S. Shelke, S.M.Sangve & S.P.Deshmukh

Dnyanganga College of Engineering and Research; Pune, Maharashtra, India

Abstract - The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development. Key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. So we propose a new robust digital watermarking system based on DCT and fuzzy vault techniques.

Keywords : *DCT; color components; color image; fuzzy vault; Digital watermarking.*

GJCST Classification: *I.2.3*

Strictly as per the compliance and regulations of:

Robust Digital Watermarking for Color Images Using Fuzzy Vault

Priyanka D. Godase[α], Snehal B. Kale[σ], Sonika S. Shelke[ρ], S.M.Sangve[ω] & S.P.Deshmukh[¥]

Abstract - The advent of the Internet has resulted in many new opportunities for the creation and delivery of content in digital form. Applications include electronic advertising, real-time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of all participants. It has been recognized for quite some time that current copyright laws are inadequate for dealing with digital data. This has led to an interest towards developing new copy deterrence and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development. Key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. So we propose a new robust digital watermarking system based on DCT and fuzzy vault techniques.

Keywords : DCT; color components; color image; fuzzy vault; Digital watermarking.

I. Introduction

Information hiding can be mainly divided into three processes - cryptography, steganography and watermarks. Cryptography is the process of converting information to an unintelligible form so that only the authorized person with the key can decipher it. As many advances were made in the field of communication it became rather simple to decrypt a cipher text. Hence more sophisticated methods were designed to offer better security than what cryptography could offer. This led to the discovery of stenography and watermarking. Stenography is the process of hiding information over a cover object such that the hidden information cannot be perceived by the user. Thus even the existence of secret information is not known to the attacker. Watermarking is closely related to steganography, but in watermarking the hidden information is usually related to the cover object. Hence it is mainly used for copyright protection and owner authentication.

Digital watermarking is the process of embedding information into digital multimedia content such that the information (the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development. Key research problem that we still face today is the development of truly robust, transparent and secure watermarking technique for different digital media including images, video and audio. So we propose a new robust digital watermarking system based on DCT and fuzzy vault techniques

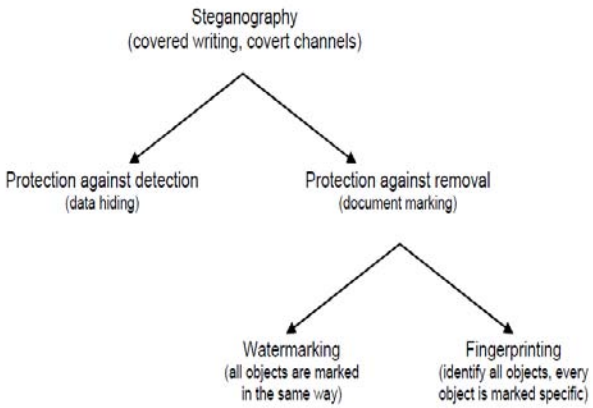

Figure 1: Types of Steganography

II. Principle of Watermarking

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital

Author α σ ρ : UG Student, Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India.
Author ω : Head of the Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India.
Author ¥ : Assistant Professor, Department of Computer, Dnyanganga College of Engineering and Research; Pune, Maharashtra, India.
E-mail α : priyanka.godase@gmail.com
E-mail σ : manusnehal@gmail.com
E-mail ρ : sonika_shelke@yahoo.com
E-mail ω : sunilsangve@gmail.com
E-mail ¥ : sayaleedeshmukh@yahoo.com

data, which means the information is not embedded in the frame around the data, it is carried with the signal itself.

III. Digital Watermarking Technology

As an Emerging Interdisciplinary application Technology, Digital Watermarking Involves the Ideas and Theories of Different Subject Coverage Such as Signal Processing, Cryptography, Probability Theory, Network Theory Algorithm Design, and other techniques.

a) Classfication of Digital Watermarking

i. *Visible*

The watermark is visible which can be a text or a logo used to identify the owner. Any text or logo to verify or hide content.

ii. Invisible

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied.

Invisible watermark can be further divided into three types,

a. *Robust Watermarks*

Invisible watermark cannot be manipulated without disturbing the host signal. This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and unintentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

b. *Fragile Watermarks*

They are designed with very low robustness. They are used to check the integrity of objects.

c. *Public and Private Watermark*

They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.

IV. System Architecture

a) Embedding Watermark

This module is designed to insert the fuzzy vault into the host image. The fuzzy vault is combination of set of genuine points and set of chaff points. Secret data is used to construct the polynomial.

In this module first we extract minutiae features from fingerprint image. And these features are further used to project the polynomial then set of genuine points and chaff points is calculated. And the union of set of genuine points and chaff points is nothing but the fuzzy vault.For inserting the fuzzy vault into an image DCT is applied on that image and to get the watermarked image IDCT is applied.

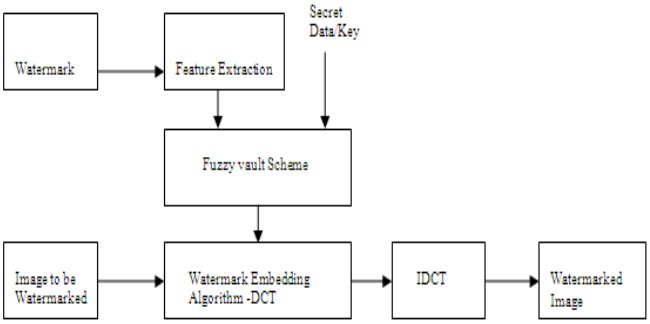

Figure 2: Embedding watermark

b) Extracting Watermark

In this module secret data is extracted by using the watermarked image and fingerprint image to validate the user. Again the DCT is applied on the watermarked image and fuzzy vault is extracted from that image. And minutiae features are extracted from the fingerprint image. By comparing the minutiae features and fuzzy vault candidate points are calculated. And then applying Langrange Interpolation CRC is calculated. If the CRC is correct then we get the secret data that proves that the user is valid user.

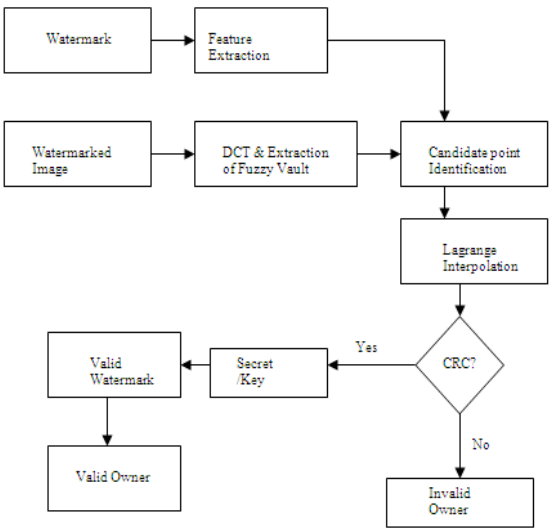

Figure 3: Extracting watermark

c) Main Algorithms

i. *Encoding Algorithm*

1. Choose the secret value or the cryptographic key S
2. Generate the cyclic redundancy check value CRC

3. Construct 144-bits data SC by concatenation of S and CRC
4. Extract k-eigenvectors E to arrive at the 16-bit locking data unit u
5. Construct a polynomial P with SC: SC can be represented as a polynomial with 9 (=144/16) coefficients for the degree D = 8.

$$P(u) = c8u\hat{}8 + c7u\hat{}7 + ...+ c1u + c0$$

6. Generate genuine points set G with ui

$$G = \{(u1, P(u1)), (u2, P(u2)),.., (uN, P(uN))\}$$

$$ui \neq uk ,i = 1,2,...,N$$

7. Generate chaff points set C

$$C = \{(c1, d1), (c2, d2), ..., (cM, dM)\}$$

$$dj \neq p(cj), j = 1, 2,\ldots M$$

8. Generate vault set VS: VS = C U G

$$VS = \{(V1, W1), (V2, W2),.., (VN+M, WN+M)\}$$

ii. *Decoding Algorithm*

1. Confirm the vault set VS

$$VS = \{(V1, WI), (V2, W2),.., (VN+M, WN+M)\}$$

2. Extract N-features u*

$$u*1, u*2, \ldots, u*N$$

3. Find K-candidate points: If any u*i is equal to Vj, the corresponding vault point is added to the list of candidate points, where K< N.
4. Find all possible combinations ofD+1 points among t he list of candidate points, resulting in C (K, D+1) combinations.
5. Reconstruct polynomial p*(u): a specific combination set given as:

$$L= \{(v1, w1), (v2, w2), (v3, w3) ,\ldots ,(vD+1,wD+1)$$

the corresponding interpolating polynomial method is the Lagrange method.

$$p^* (u) = C*8u\hat{}8+C^* 7u\hat{}7 +...+C*1u+C*0$$

6. Check CRC
7. Decode secret value S

iii. *Steps for Getting Watermarked Image*

1. Divide host image in to 8x8 blocks.
2. Calculate DCT for each block from left to right and top to bottom.
3. Compress image using Quantization technique.(Quantization: It is the Process of approximation.)
4. By using IDCT we get original Watermarked image.

V. Application

In this project, an efficient blind digital image watermarking algorithm using mapping technique is presented. The algorithm can embed or hide an entire image or pattern (logo) directly into the original image. The embedding process is based on changing the selected DCT coefficients of the host image to odd or even values depending on the binary bit value of watermark DCT coefficients. The algorithm is tested for fingerprint image embedded with a face watermark. It is demonstrated that the watermarking algorithm offers a significant advantage of providing biometric image compression and authentication without introducing any significant degradation in the image quality. Moreover the watermarking scheme is blind and does not require any additional data for logo extraction.

Applications of image watermarking:

a) Copyright Protection

This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

b) Authentication

Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

c) Broadcast Monitoring

As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

d) Content Labeling

Watermarks can be used to give more information about the cover object. This process is named content labeling.

e) Tamper Detection

Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

f) Digital Fingerprinting

This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

g) Content Protection

In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

VI. Conclusion

With the popularity of the network, the safety communication issue of digital product becomes an important and urgent research topic. The basic principles and algorithms of the digital watermarking technology are discussed, and the DCT algorithm is selected to do the application test of digital image copyright protection.

The experiment proves that DCT-based watermark can well withstand a variety of image processing, and the watermark can survive after compression, cropping, and other attacks.

Digital watermarking technology can provide a new way to protect the copyright of multimedia information and to ensure the safe use of multimedia information. Comparing to the traditional information security technology, digital watermarking technology has its own advantages in the multimedia information security protection. Then it can meet the application need in many aspects and has a bright development prospect.

References Références Referencias

1. David Salomon. Data Compression - The Complete Reference 3rd Edition, Springer, 2004
2. N. Ahmed, T. Natarajan, and K. R. Rao, Discrete cosine transform, IEEE Trans. Comput., vol. C-23, Jan. 1974, 90-93.
3. G. A. Juels and M. Sudan, "A Fuzzy Vault Scheme," *Proceedings of IEEE International Symposium on Information Theory*, 2002.
4. B. D. Tseng and W. C. Miller. On computing the discrete cosine transform, IEEE Trans. Computing, vol.C-27: July 1976, 966-968.
5. U. Uludag and A. K. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in IEEE Workshop on Privacy Research In Vision, June 2006, p. 163.
6. X. Chen, J. Tian, and X. Yang, "A novel algorithm for distorted fingerprint matching based on fuzzy features match," in AVBPA 2005. 2005, vol. LNCS 3546, pp. 665-673, Springer-Verlag.
7. D.P. Mital and E.K. Teoh, "An automated matching technique for fingerprint identification," in KES 1997, May 1997, vol. 1,pp. 142-147.
8. S. Na K.D. Yu and T.Y Choi, "A fingerprint matching algorithm based on radial structure and a structure-rewarding scoring strategy," in AVBPA 2005. 2005, vol. LNCS 3546, pp. 656-664, Springer-Verlag.
9. Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Eurocrypt 2004, 2004.
10. J. Jeffers and A. Arakala, "Minutiae-based structures for a fuzzy vault," in 2006 Biometrics Symposium, 2006.